ISSN : 2229 - 3515

Volume : 10 ,
Special Issue of NCSCCSS 2020
27-28th November 2020

Proceedings of the
3rd National Conference
on
Soft Computing, Communication Systems & Sciences

(NCSCCSS 2K20)

27-28th November 2020

(Virtual Mode)

International Journal of ADVANCES IN SOFT COMPUTING TECHNOLOGY

Editor-in-Chief
Dr.C.Srinivasa Kumar

Organized by

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

Convener
Dr. Kanaka Durga Returi
Dr.A.Praveen Kumar

Published by
BHAVANA RESEARCH CENTER

3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES

(NCSCCSS 2K20)

on

27-28th November 2020

(VIRTUAL MODE)

Conveners

Dr. KANAKA DURGA RETURI

Dr. ARCHEK PRAVEEN KUMAR

Organized by

Department of Computer Science & Engineering
Department of Electronics & Communication Engineering
MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN
Maisammaguda, Medchal, Hyderabad-500100, TS, INDIA

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.

E-Mail: rg.mrcew@gmail.com

EAMCET CODE: MREW

JNTUH CODE: RG

Sri. CH. MALLA REDDY
M.L.A -Medchal
Hon'ble Minister, Govt. of Telangana
Labour & Employment, Factories,
Women and Child Welfare.
Founder Chairman, MRGI

Message

MRCEW, HYDERABAD has always been a front runner to organize such events and this time too we have come up with (VIRTUAL MODE) "3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K20)" in this pandemic **COVID 19 Period**. The objective was to bring the eminent academicians, scientists, researchers, industrialists, technocrats, government representatives, social visionaries and experts from all strata of society, under one roof, to explore the new horizons of innovative technologies to identify opportunities and define the path forward. Finally, I congratulate Principal, HODs, college faculty, student representatives and participant for their efforts in organizing and participating in this conference and wish the conference all the success.

CH. MALLA REDDY

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.

E-Mail: rg.mrcew@gmail.com

EAMCET CODE: MREW

JNTUH CODE: RG

Sri. CH.MAHENDER REDDY

Secretary, MRGI

Message

It gives me immense pleasure to be a part of this hosting team of "3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K19)". The events in the conference are targeted towards researchers, practitioners, professionals, educators and students to share their experience, innovative ideas, issues, recent trends and future directions in field of Engineering and Science and Technology. Finally, I congratulate the team members and participant for their efforts in organizing and participating in this conference and wish the conference all the success.

Sri. CH.MAHENDER REDDY

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.

E-Mail: rg.mrcew@gmail.com

EAMCET CODE: MREW

JNTUH CODE: RG

DR. VAKA MURALI MOHAN
B. Tech., M.Tech (ChE)., Ph.D (AU)
M.Tech (CSE)., Ph.D (GU)
MISTE., MCSI., MSAI., MIEEE., MUACEE
PRINCIPAL & PROFESSOR of CSE
murali_vaka@yahoo.com

Message

I am very glad that the Department of CSE & ECE is organizing (VIRTUAL MODE) "3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K20)" in this pandemic COVID 19 period. This will not only help the students by opening the vistas of opportunities in various fields of engineering, but also promote learning and sharing of ideas for the faculty members. I am confident that this conference will indeed generate a lot of interest among the students to explore and pursue the area of research, thereby bringing laurels to your institute and developing our society as a whole. I praise the all faculty members of CSE & ECE for their collaboration and hard work in making this conference a magnificent success.

DR. VAKA MURALI MOHAN

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.

E-Mail: rg.mrcew@gmail.com

EAMCET CODE: MREW

JNTUH CODE: RG

DR. KANAKA DURGA RETURI

B. Tech., M.Tech., Ph.D

HOD & PROFESSOR of CSE

CONVENER

Message

It is our great honor to welcome you all the delegates from various parts of the Country to (VIRTUAL MODE) "3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K20)" in this pandemic COVID 19 period. The conference particularly encouraged the interaction of research students and developing academics with the more established academic community in an informal setting to present and to discuss new and current work. Their contributions helped to make the conference as outstanding as it has been. These Proceedings will furnish the scientists of the world with an excellent reference book. I trust also that this will be an impetus to stimulate further study and research in all these areas. We thank all authors and participants for their contributions..

.

DR. KANAKA DURGA RETURI

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.

E-Mail: rg.mrcew@gmail.com

EAMCET CODE: MREW

JNTUH CODE: RG

DR. ARCHEK PRAVEEN KUMAR

B. Tech., M.E., Ph.D

HOD & PROFESSOR of ECE

CONVENER

Message

It is our great honour to welcome you all the delegates from various parts of the Country to (VIRTUAL MODE) "3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K20)" in this pandemic COVID 19 period. The conference received 165 submissions, the huge number of submissions provided an excellent opportunity for a high-quality program, but also called for a demanding and laborious paper evaluation process. The Review Committee worked efficiently and responsibly under tight time constraints to produce at least two reviews for each paper that provided the basis for the final paper selection. We had an exciting week of insightful presentations, discussions, and sharing of technical ideas with colleagues from around the world. We thank you for attending the conference.

DR. ARCHEK PRAVEEN KUMAR

INTERNATIONAL JOURNAL OF ADVANCES IN SOFTCOMPUTING TECHNOLOGY

(ISSN NO: 2229-3515)

(Published by **BHAVANA RESEARCH CENTER, HYDERABAD**)

DR. C.SRINIVASA KUMAR

M.Sc., Ph.D (SVU), M.Tech (CSE)., Ph.D (GU)

MISTE, MCSI MISTE., MCSI., MSAI

EDITOR–IN–CHIEF

MESSAGE

I am glad to note that ***"MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN"*** *has taken the initiative to conduct a two day* ***(VIRTUAL MODE)*** *"3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES* ***(NCSCCSS 2K20).*** Advances in Soft Computing & Communication Technologies gives the latest communication promises faster than other facilities, because of the best possible information and communication updates in current trends. I am sure the deliberations during the conference will expose the Staff, Research Scholars and Students to what is new and what is ahead in Soft Computing & Communication Technologies…….

I congratulate the organizers and convey my best wishes for the success of the Conference in the fulfillment of its objectives.

With Regards

(DR. C.SRINIVASA KUMAR)

Editor-In-Chief, IJASCT

3rd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES
(NCSCCSS 2K20)

on

27-28th November 2020

(VIRTUAL MODE)

Chief Patron

Sri. CH. MALLA REDDY	Founder Chairman, MRGI

Patron

Sri. CH. MAHENDER REDDY	Secretary, Malla Reddy Group of Institutions
Dr. CH. BHADRA REDDY	President, Malla Reddy Group of Institutions
Dr. VAKA MURALI MOHAN	Principal, MRCEW

Convener

Dr. Kanka Durga Returi	Professor & HOD, CSED
Dr. Archek Praveen Kumar	Professor & HOD, ECED

International Advisory Committee

Dr. Kun-Lin Hsiesh	NTU, Taiwan
Dr. Ghazali Bin Sulong	UT, Malaysia
Dr. Halis Altun	MU, Turkey
Dr. Ahamad J Rusumdar	KIT, Germany
Dr. V.R.Chirumamilla	EUT, Netherlands
Dr. Silviya Popova	ISER, BAS, Bugaria
Dr. Shaik Feroz	CCE, Oman
Dr. Lean Yu	AMSC, Beijing, China
Dr. Mohen Hayati	RU, Iran

Technical Committee

Dr.A.Vinay Babu	JNTU Hyderabad
Dr.J.A.Chandulal	GU, Visakhapatnam
Dr.P. Premchand	OU, Hyderabad
Dr. G. Hemanth Kumar	UM, Mysore
Dr.M. Srinivasa Rao	SIT, JNTU Hyderabad
Dr.A.Damodaram	SVU Tirupathi
Dr.G.Govardhan	JNTU Hyderabad
Dr.P.R.K.Murti	Rtd, HCU Hyderabad
Dr. Doreswamy	UM, Mangalore
Dr. M. V. Satish Kumar	TCU, Assam
Dr. J.K. Mantri	NOU, Orissa

Advisory Board

Dr. D. Rajya Lakshmi	JNTU Kakinada
Dr. V. Kamakshi Prasad	JNTU Hyderabad
Dr. G. Narasimha	JNTU Jagityal
Dr. P. V.Nageswara Rao	GU, Visakhapatnam
Dr. B. Padmaja Rani	JNTU Hyderabad
Dr.Md.Zafir Ali Khan	IIT Hyderabad
Dr. N. Kalyani	GNITS, Hyderabad
Prof. K. Srujan Raju	CMRTC & CSI Hyderabad

Mr.Anirban Pal	Tech Mahindra, Hyderabad
Mr.Gautham Mahapatra	Sr.Scientist

Editorial Board

Dr. I. Selvamani	MRCEW Hyderabad
Mr. A. Brahma Reddy	MRCEW Hyderabad
Mr. S. SATYA	MRCEW Hyderabad

Co-Conveners

Mr. K. G. N. Kumar	MRCEW Hyderabad
Mr. Ch. V. Krishna Mohan	MRCEW Hyderabad

Organizing Committee

1	Dr. M. JOSEPH PRAKASH	MRCEW Hyderabad
2	Dr CH. JAYAPRAKASH	MRCEW Hyderabad
3	Dr. J. NELSON	MRCEW Hyderabad
4	Dr A. JANARDHAN	MRCEW Hyderabad
5	Mrs. SUJATHA GODAVARTHI	MRCEW Hyderabad
6	Mrs. POTNURU LAVNYA	MRCEW Hyderabad
7	Mrs. SUNITHA NETALA	MRCEW Hyderabad
8	Mrs. VEERNALA SIREESHA	MRCEW Hyderabad
9	Mr. T. SESHU KIRAN	MRCEW Hyderabad
10	Mrs. SHETAL KULKARNI	MRCEW Hyderabad
11	Mrs. N. UMA MAHESWARI	MRCEW Hyderabad
12	Mrs. MANJU PADIDELA	MRCEW Hyderabad
13	Mrs. K. SHIVANI	MRCEW Hyderabad
14	Mrs. Y. SANGEETHA	MRCEW Hyderabad
15	Mr. PITTA SANKARA RAO	MRCEW Hyderabad
16	Drs T. SUDHA	MRCEW Hyderabad
17	Dr. P. GEETA SWARUPA	MRCEW Hyderabad
18	Mrs. Y. SAROJA	MRCEW Hyderabad

****

ISSN: 2229-3515

INTERNATIONAL JOURNAL OF ADVANCES IN SOFT COMPUTING TECHNOLOGY

Subscription

Price Per Volume (2 Issues): Rs. 2000(India), US $. 125(Foreign)

BHAVANA RESEARCH CENTER
#A-905, 2nd Floor, Allwyn Colony, Phase-2,
Kukatpally, Hyderabad – 500 072, TS, India
☎.: 91- 7730883888
✉ :editor@ijasct.in, brchyd_2010@yahoo.com
www.ijasct.in

INTERNATIONAL JOURNAL OF ADVANCES IN SOFT COMPUTING TECHNOLOGY

(VIRTUAL MODE)

Volume: 10 *Special Issue of NCSCCSS-2K20* *27th – 28th November, 2020*

Network Link-Based Energy Consumption With QoS Requirements

Dr M Joseph Prakash[1]., K Susmitha[2]., M Umamaheshwari[3]., Ch Asritha[4]., M Chandana[5]
1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- :- mjosephp7@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0526, 17RG1A0538, 17RG1A05J3, 17RG1A05L2),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***ALR is definitely an Ethernet technology where link rate and power dynamically scale with traffic volume. As a result, even without altering the topology, energy consumption can continue to vary greatly given different routings that lead to different traffic volume around the pathways. We design a eco-friendly Internet routing plan, in which the routing may lead traffic in a manner that is eco-friendly. We vary from previous studies where they switch network components, for example line cards and routers, into sleep mode. We don't prune the web topology. The issue of maximizing the ability saving with trunk links using MPLS-like routing continues to be proven to become NP-hard. We first create a power model, and validate it using real commercial routers. Rather of creating a centralized optimization formula, which requires additional protocols for example MPLS to materialize online, we decide a hop-by-hop approach. It's thus much simpler to integrate our plan in to the current Internet. We study "green" routing where we don't prune the web topology. A vital observation which makes this possible would be that the energy consumption for packet delivery could be different in various traffic volumes. We comprehensively evaluate our algorithms through simulations on synthetic, measured, and real topologies, with synthetic and real traffic traces. We progressively develop three algorithms, that are loop-free, substantially reduce energy consumption, and jointly consider eco-friendly and QoS needs for example path stretch. We further evaluate the ability saving ratio, the routing dynamics, and also the relationship between hop-by-hop eco-friendly routing and QoS needs.***

Keywords— Hop-by-hop routing, routing algebra, NP-hard, green-routing.

1. INTRODUCTION

Online, routers and switches account for almost all energy consumption. Within this paper we study energy conservation online. We realize that different traffic volumes on the link can lead to different energy consumption this really is mainly because of such technologies as trucking, adaptive link rates, etc. The network components to become switched off are carefully selected and tradeoffs are investigated to balance network performance and conservation. Within this paper, we study "green" routing where we don't prune the web topology [1]. A strategy without topology pruning may also be used inside a network after pruning some links or nodes for more energy conservation. We are able to then easily incorporate the routing formula in to the OSPF protocol. Under this hop-by-hop design, we face the next challenges. We present an extensive study. We first create a power model and validate the model using real experiments in commercial routers. Then we develop concepts along with a baseline hop-by-hop eco-friendly routing formula that guarantees loop-free routing.

2. EXISTING SYSTEM:

Online, routers and switches account for almost all energy consumption. Increasingly higher end routers are developed and deployed presently. For instance, a 'cisco' CRS-1 router can draw about one Megawatt under full configuration, 10,000 occasions greater than a PC. By 2010, 5,000 'cisco' CRS-1 routers were deployed. Facing such high energy consumption, there are lots of studies for energy conservation from the Internet. Generally, these studies switch network components, for example line cards and routers, into sleep mode. As a result, these studies compute a topology with less nodes and links. Disadvantages of existing system: It might degrade network resistant against failures [2]. The network components to become switched off are care-fully selected and tradeoffs are investigated to balance network performance and conservation.

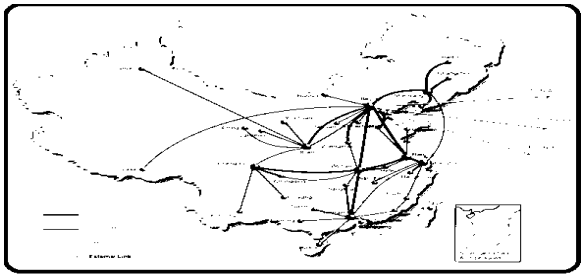


Fig.1.System architecture

The traffic of various pathways with each other boosts the utilization ratio of links, and results in greater energy consumption. This can be a standard local versus. global optimal problem. Direct measurements to populate a traffic matrix are usually prohibitively costly. The process to estimate a traffic matrix from partial information is of high complexity, because the connected optimization issue is non-convex.

3. SYSTEM APPROACH:

Therefore, we are able to select pathways that consume less power while delivering traffic. Within this paper, we rather select a hop-by-hop approach. This kind of approach is appropriate for that systems without MPLS deployed. More particularly, each router can individually compute next hops, just like the things they're doing in Dijkstra today. We are able to then easily incorporate the routing formula in to the OSPF protocol. Benefits of suggested system: Intrinsically, our work implies that there might be more refined control than an on-off (-1) charge of the routers in energy conservation. We further develop a sophisticated formula that substantially increases the baseline formula in energy conservation. We develop an formula that concurrently views energy conservation and path stretch [3]. We currently study hop-by-hop eco-friendly routing (Eco-friendly-HR).Then we study some intrinsic relationships between link weights and power consumption, and develop a sophisticated formula Dijkstra Eco-friendly-Adv that improves energy conservation. Important QoS performance from the network for example path stretch might be considered concurrently, and could be naturally adjusted.

Link Model: A hyperlink between two routers is physically associated with two line cards, and also the line cards take in the majority power the routers. Non-trunk links: We are able to divide the ability consumption into three groups: i) power consumed by OS and control plane ii) power consumed by line card CPU processor and iii) power consumed by operations like buffer I/O, packet lookup, etc. Trunk links: For any trunk link, the main difference may be the discrete stair-like behavior. We model two intrinsic causes of the discrete stair-like behavior: physical links could be powered off in various traffic volumes and various components lined up cards could be switched-off in various traffic volumes. We have seen that for any non-trunk link, the ability consumption is slightly super-straight line towards the traffic volume. For any trunk link, the ability consumption shows an even bigger difference along with a discrete stair-like behavior. Another observation would be that the power consumption changes little once the line card components change power condition the slope of every step from the trunk link curve is comparable to the slope from the non-trunk link curve. The ability model we suggested is dependent on analysis and measurements on real routers. Similar answers are reported inside a recent independent work.

Framework of Eco-friendly Internet: The goal of eco-friendly Internet routing would be to minimize the entire energy consumption within the network. We decide a hop by-hop approach because it may be easily built-into current Internet routing architecture. The traffic of various pathways with each other boosts the utilization ratio of links, and results in greater energy consumption. This can be a standard local versus. global optimal problem. One possible option would be to allow each router compute routing according to global traffic matrices that reflect the level of traffic flowing between all possible source and destination pairs [4]. We design a way weight

like the path weight utilized by Dijkstra, in which the weight reflects the entire energy conservation according to partial traffic data. The road weights should be carefully made to make certain the hop-by-hop routing is loop-free. Intrinsically, to attain a loop-free routing, there are specific qualities the path weights should follow. There are two steps to prevent hop-by-hop routing loops: certain qualities have to be satisfied along with a routing formula was created accordingly. We are able to obtain a consistent (thus loop-free) hop-by-hop routing if every node uses D-lightest pathways to forward packets.

Dijkstra-Eco-friendly Formula: We advise a way weight along with a baseline formula Dijkstra-Eco-friendly-B to attain loop-free. Then we study some intrinsic relationships between link weights and power consumption, and develop a sophisticated formula Dijkstra-Eco-friendly-Adv that improves energy conservation. For every link in the road to destination node d, we assign an believed traffic volume or "virtual traffic volume". We compute the virtual traffic volume by posing an exponential penalty to some start traffic volume for every additional hop. Then, using the virtual traffic volume, the hyperlink power is computed following a power function. We are able to acquire a consistent (thus loop-free) hop-by-hop routing by making use of a Dijkstra-like formula. We develop Formula Dijkstra-Eco-friendly-B. P within the inputs denotes the group of the ability-traffic functions of all of the links in E. There are a couple of variations between Dijkstra-Eco-friendly-B and also the standard Dijkstra. The computation complexity of Dijkstra-Eco-friendly-B is equivalent to those of the conventional Dijkstra within the worst situation. To have greater energy conservation, we take particular notice at two primary factors affecting power consumption [5]. The hyperlink weight should be affected by it. We consider a serious situation the power consumption is proportional to traffic volume xl. This kind of assumption is really a special situation in our power model. Although the assumption is good, it's in conjunction with the trend of developing power-proportional routers. Generally, we have a heuristic by multiplying the load of the trunk link to an issue. However, the factor for various trunk links shouldn't be exactly the same. On a single hands, when we place a big traffic volume on the trunk link, the ability consumption will probably leap to some greater stair. However, if your small traffic volume may cause the ability consumption to leap to some greater stair, we also require a big factor for that link. Dijkstra-Eco-friendly-Adv concentrates on achieving more energy conservation, and follows the concepts of Dijkstra-Eco-friendly-B to ensure loop-free routing. We design a hyperlink weight in 2 steps. We design a sophisticated formula which could run inside a hop-by-hop manner, namely the Dijkstra-Eco-friendly-Adv formula. Clearly, the eco-friendly pathways and also the shortest pathways can't be concurrently achieved. An average metric to judge the way a computed path is different from shortest path is path stretch: the number of the size of an s-d road to those of the shortest path between this s-d pair. First, we discuss the bounds around the optimal power saving without topology pruning, and also the power saving ratio that Eco-friendly-HR is capable of [6]. Second, we discuss the routing dynamics of Eco-friendly-HR, and reveal that routing oscillations and transient micro-loops could be prevented. Third, we read the relationship between Eco-friendly-HR and QoS needs, and show that it's impossible to locate a strictly left-isotonic path weight structure optimizing one path weight while bounding another, because of the intrinsic nature of routing algebra.

4. PREVIOUS STUDY:

You will find studies on saving energy from the routers. You will find studies on energy conservation from the Internet from upper layers perspective. Studies in order to save energy from the network routing perspective. GreenTE is suggested to aggregate

traffic using MPLS tunnels, in order to switch the underutilized network components into sleep mode and therefore save energy. Fact is suggested to recognize energy critical as well as on-demand pathways offline. Also, you will find studies in order to save energy without sleep mode. However, to attain good performance, a centralized formula continues to be required to assign sleeping links. ESACON is suggested to collaboratively select sleeping links with special connectivity qualities. Routing pathways will be computed after these links are removed. Our design is dependent on the observation the energy use of a hyperlink could be determined by the traffic volume [7]. A routing formula may keep this in mind. We might consider eco-friendly as one sort of services the Internet should provision. There have been two different approaches in Internet QoS support beyond shortest path routing. The first is centralized computation. Within this paper, we leverage the algebra model to build up hop-by-hop computing for eco-friendly Internet routing, that is loop-free.

5. CONCLUSION:

We still visit a 65 % of one's saving once the utilization is low and Dijkstra-Eco-friendly can help to save greater than 20 % from the energy once the utilization is up to 70 %. Within this paper, we studied eco-friendly Internet routing. We validated our model using real experiments. We suggested a hop-by-hop approach and progressively developed algorithms that guarantee loop-free routing, substantially reduce energy footprint online, and jointly consider QoS needs for example path stretch. We presented an electrical model that quantifies the connection between traffic volume and power consumption. Like a initial work, we admit there are many unsolved questions. This really is helpful when MPLS does apply, and could provide theoretical bounding for that possible maximum power conservation. Especially, we are curious about further investigating a centralized plan.

REFERENCES:

[1] Yuan Yang, Student Member, IEEE, Mingwei Xu, Member, IEEE,Dan Wang, Member, IEEE, and Suogang Li, “A Hop-by-Hop Routing Mechanismfor Green Internet”, ieee transactions on parallel and distributed systems, vol. 27, no. 1, january 2016.

[2] O. Heckmann, M. Piringer, J. Schmitt, and R. Steinmetz, “Generating realistic ISP-level network topologies,” IEEE Commun. Lett., vol. 7, no. 6, pp. 335–336, Jul. 2003.

[3] M. Xu, Y. Shang, D. Li, and X. Wang, “Greening data center networks with throughput-guaranteed power-aware routing,” Comput. Netw., vol. 57, no. 15, pp. 2880–2899, 2013.

[4] R. Kubo, J. Kani, H. Ujikawa, T. Sakamoto, Y. Fujimoto, N. Yoshimoto, H. Hadama, "Study and demonstration of sleep and adaptive link rate control mechanisms for energy efficient 10G-EPON," IEEE/OSA J. Opt. Commun. Netw., vol. 2, no. 9,pp. 716–729, Sep. 2010.
[5] J. L. Sobrinho, "Algebra and algorithms for QoS path computation and hop-by-hop routing in the internet," IEEE/ACM Trans. Netw., vol. 10, no. 2, pp. 541–550, Aug. 2002.
[6] Y. M. Kim, E. J. Lee, H. S. Park, J.-K. Choi, and H.-S. Park, "Ant colony based self-adaptive energy saving routing for energy efficient Internet," Comput. Netw., vol. 56, no. 10, pp. 2343–2354, 2012.
[7] J. Wang and K. Nahrstedt, "Hop-by-hop routing algorithms for premium-class traffic in DiffServ networks," ACM SIGCOMM Comput. Commun. Rev., vol. 32, pp. 73–88, 2002.

AN IMPRESSIVE PRE-PROCESSING STRATEGY FOR VISUAL CAPTION

Dr.C.Jayaprakash[1]., R Durga Chandrika[2]., M Shirisha[3]., S Ankitha[4]., V Ravanya[5]

1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- dr.jayaprakash.cs@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0515, 17RG1A0536, 17RG1A0553, 17RG1A0559), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT: ***The aim of image tag completion would be to precisely recover the missing labels for the images. To allow nonlinearity and the computational efficiency simultaneously, we turn to a locality sensitive approach, using the assumption that although nonlinear globally, the model could be straight line in your area, which enables the use of straight line models when samples are limited to individual parts of the information space. To effectively infuse the thought of locality sensitivity, an easy and efficient pre-processing module is made to learn appropriate representation for data partition, along with a global consensus regularize is brought to mitigate the chance of over fitting. The present completion methods are often founded on straight line assumptions, therefore, the acquired models are restricted because of their incapability to capture complex correlation patterns. Extensive empirical evaluations conducted on three datasets demonstrate the success and efficiency from the suggested method, where our method outperforms previous ones with a large margin. Meanwhile, low-rank matrix factorization is utilized as local models, in which the local geometry structures are preserved for that low-dimensional representation of both tags and samples. We advise a locality sensitive low-rank model for image tag completion, which approximates the worldwide nonlinear model with an accumulation of local straight line models, through which complex correlation structures could be taken.***

Keywords— Multi-Task Learning (MTL), image tag completion, locality sensitive model, low-rank matrix factorization, over-fitting.

1. INTRODUCTION:

User-labeled visual data, for example images that are submitted and shared in Flicker, are often connected with imprecise and incomplete tags. This can pose threats towards the retrieval or indexing of those images, causing them hard to be utilized by users. Therefore, image tag completion or refinement has become a warm trouble in the multimedia community. Many visual applications have taken advantage of the episode of web images, the imprecise and incomplete tags arbitrarily supplied by users, because the thorn from the rose, may hamper the performance of retrieval or indexing systems counting on such data. Within this paper, we advise a singular locality sensitive low-rank model for image tag completion, which approximates the worldwide nonlinear model with an accumulation of local straight line models [1]. The very first issue involving in this locality sensitive framework is how you can conduct significant data partition, that is nontrivial within the tag completion scenario, because the distance between samples, that is necessary to most partition methods, is very hard to rely on when measured by low-level features and incomplete user-provided tags. The 2nd problem concerns the making of the neighborhood models, that's, how you can effectively model the neighborhood correlations between similar samples and related tags. Within this paper, our method draws inspiration from Multi-Task Learning and formulates the neighborhood models by low-rank matrix factorization. We advise a locality sensitive low-rank model for image tag completion, which approximates the worldwide nonlinear model with an accumulation of local straight line models, through which complex correlation structures could be taken.

2. EXISTING SYSTEM:

Included in this, condition-of-the-art performance is as reported by label-transfer methods. JEC adopted equal weights for every feature and transferred labels inside a greedy manner. Tag Proem bedded metric learning to find out more discriminative weights [2]. 2PKNN extended LMNN right into a multi-label scenario and built semantic groups to improve annotation performance for rare tags.

Disadvantages of existing system: Learning image annotation models from partly labeled training data is a lot more challenging than solving traditional AIA tasks, since the possible lack of fully labeled training set limits the leverage of some sophisticated supervised models, thus the annotation precision is way from acceptable. The majority of the aforementioned methods unsuccessful to think about the complex structures past the capacity of straight line models.

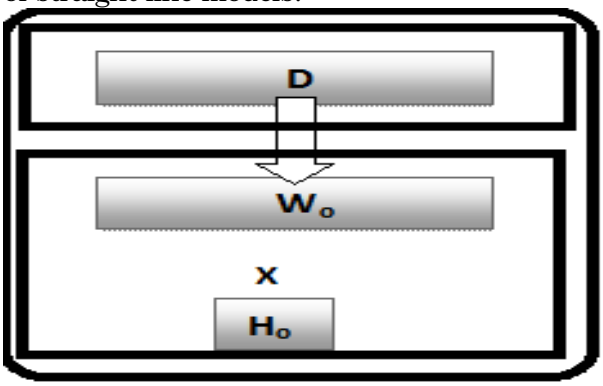


Fig.1.Proposed Model

3. MTL TECHNIQUE:

Within this paper, our method draws inspiration from Multi-Task Learning (MTL) and formulates the neighborhood models by low-rank matrix factorization. Particularly, each initial tag sub-matrix is decomposed right into a low-rank basis matrix along with a sparse coefficient matrix, and also the compressed representation for the tags and samples are learnt, correspondingly. This type of model has the capacity to promote information discussing between related tags in addition to similar images [3]. However, it's not more suitable to understand local models individually, because the creation of data partition is usually not even close to acceptable, even with the aid of the pre-processing module. Consequently, the neighborhood models learned individually have a tendency to over fit the information limited to individual regions. Therefore, to alleviate the chance of over-fitting in addition to promote sturdiness from the suggested LSLR method, a worldwide consensus model is brought to regularize the neighborhood models.

Preliminary Study: Our goal for tag completion would be to recover the entire tag matrix Y. The suggested method achieves this via several modules, including pre-processing, data partition, and also the learning of local models. According to this novel representation, all of the images within the dataset are split into multiple groups, to ensure that samples inside the same group are semantically related. Then our final completed matrix Y could be acquired by integrating all of the sub-matrices Yi s. The aim of data partition would be to divide the whole sample space into an accumulation of local neighborhoods or groups, so that samples within each group are semantically related [4]. However, once we noticed in our experiments, direct partitions usually neglect to generate significant groups, no matter using visual features or incomplete initial tags. Within this paper, a cluster is called an untidy cluster if it is images aren't really semantically related, along with a compact cluster otherwise. Our initial step would be to get rid of the side-effect of both high-frequency and rare tags by removing their corresponding posts within the initial tag matrix, given that they hardly appear because the primary content from the images. The 2nd step would be to discover the low-dimensional representation for every image. The information partition module takes as input W0 , and assigns a cluster label to every sample. Our approach will not make any particular assumptions on the option of partition algorithms, thus various methods can be viewed as, including k-means clustering, locality sensitive hashing.

Group Low-Rank Model: Particularly, our method preserves local geometry structures both in the tag and image subspaces for every cluster. Much like existing methods, the suggested formula also assumes the feature vector for every image could be linearly reconstructed through the feature vectors of countless other images within the same cluster [5]. Based on the LLE assumption, the

structural information encoded in Si ought to be robust towards the sparse renovation process. The coefficient matrix Ti encodes the neighborhood geometry structures within the tag space, by presuming the distribution of every tag could be linearly reconstructed through the distribution of other tags. Therefore, consistency between tags and pictures are generally maintained.

Local Models Consistency: optimizing each Wi and Hi individually for every cluster isn't more suitable because of potential over fitting, specifically for these cluttered clusters. Under such conditions, images depicting exactly the same concept might be partitioned into multiple clusters, whereas samples readily available for learning a particular model maybe inadequate. Therefore, the training process for any cluttered cluster could be amended by forcing its tag representation Hi to become similar using the reference matrix H. In this manner, the chance of over fitting might be alleviated by discussing information among images within various clusters [6].

4. PREVIOUS WORK:

Numerous methods happen to be suggested in this region, including mixture models for example MBRM, SML, subject models for example mmLDA, cLDA, tr-mmLDA, discriminative methods, and label-transfer schemes. Therefore, several recent reports are conducted on developing annotation algorithms robust to missing labels, including. Learning image annotation models from partly labeled training data is a lot more challenging than solving traditional AIA tasks, since the possible lack of fully labeled training set limits the leverage of some sophisticated supervised models, thus the annotation precision is way from acceptable [7]. Significant efforts happen to be dedicated to the job of image tag completion, among which a variety of approaches happen to be explored from divergent perspectives. Methodologically, the thought of approximating a nonlinear model using an accumulation of local straight line models continues to be explored in other locations too. Within this paper, to use this tactic to image tag completion, several critical factors are introduced. The lately suggested LSR method conducted straight line sparse renovation for every image and every tag, correspondingly.

5. CONCLUSION:

Several adaptations are brought to let the fusion of locality sensitivity and occasional-rank factorization, together with a easy and effective pre-processing module along with a global consensus regularize to mitigate the chance of over fitting. Within this paper we advise a locality sensitive low-rank model for image tag completion. Our method achieves superior results on three datasets and outperforms pervious methods with a large margin. Within this paper, our method draws inspiration from Multi-Task Learning (MTL) and formulates the neighborhood models by low-rank matrix factorization. Particularly, each initial tag sub-matrix is decomposed right into a low-rank basis matrix along with a sparse coefficient matrix, and also the compressed representation for the tags and samples are learnt, correspondingly.

REFERENCES:

[1] Xue Li, Bin Shen, Member, IEEE, Bao-Di Liu, and Yu-Jin Zhang, Senior Member, IEEE, “A Locality Sensitive Low-Rank Modelfor Image Tag Completion”, ieee transactions on multimedia, vol. 18, no. 3, march 2016.

[2] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, “Locality-sensitive hashing scheme based on p-stable distributions,” in Proc. 20th Annu. Symp. Comput. Geometry, 2004, pp. 253–262.

[3] C. Yang, M. Dong, and J. Hua, “Region-based image annotation using asymmetrical support vector machine-based multiple-instance learning,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., Jun. 2006, vol. 2, pp. 2057–2063.

[4] S. S. Bucak, R. Jin, and A. K. Jain, "Multi-label learning with incomplete class assignments," in Proc. IEEE Conf. Comput. Vis. Pattern Recog., Jun. 2011, pp. 2801–2808.

[5] B.-D. Liu, Y.-X.Wang, B. Shen, Y.-J. Zhang, and Y.-J.Wang, "Blockwise coordinate descent schemes for sparse representation," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., May 2014, pp. 5267–5271.

[6] G. Zhu, S. Yan, and Y. Ma, "Image tag refinement towards low-rank, content-tag prior and error sparsity," in Proc. Int. Conf.Multimedia, 2010, pp. 461–470.

[7] S. Feng, R. Manmatha, and V. Lavrenko, "Multiple Bernoulli relevance models for image and video annotation," in Proc. IEEE Conf. Comput. Vis. Pattern Recog., Jun. 2004, vol. 2, pp. 1002–1009.

AN INTERNET BASED MULTI-USER DATA-SHARED SYSTEM INTEGRATING INTO CLOUD

Dr. Dr.J.Nelson[1]., N Shireesha[2]., S Nikitha[3]., T Sai Manisha[4]., V Keerthi a[5]
1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- drjenelson.mrcew@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0540, 17RG1A0550, 17RG1A0555, 17RG1A0560), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***The issues of information storing and knowledge computing in mobile-Internet applications could be overcome by mobile cloud-computing as the new paradigm may also accomplish cloud based multi-user data discussing, finish geographical service limitation, and process real-time tasks efficiently simultaneously. With integrating into cloud-computing, security issues for example data confidentiality and user authority may arise within the mobile cloud-computing system, which is concerned because the primary constraints towards the developments of mobile cloud-computing. To be able to provide safe and sound operation, a hierarchical access control method using modified hierarchical attribute-based file encryption along with a modified three-layer structure is suggested within this paper. Within this paper, a hierarchical access control method utilizing a modified hierarchical attribute-based file encryption along with a modified three-layer structure is suggested. The ABE based access control method uses several tags to mark the attributes that the specific approved user must possess. Inside a specific mobile cloud-computing model, enormous data which can be from all sorts of cellular devices, for example smart phones, functioned phones and PDAs and so forth could be controlled and monitored through the system, and also the data could be responsive to unauthorized 3rd party and constraint to legal users too.***

Keywords— Attribute-based access, access control. Mobile cloud computing

1. INTRODUCTION:

Actually, most cellular devices have the capability to capture some data in the atmosphere nowadays, for instance, nearly every Smartphone are outfitted with sensors of closeness, accelerometer, gyroscope, compass, barometer, camera, Gps navigation, microphone. What people that use the cellular devices and applications require is that mobile-Internet can give them the service that is user-friendly, high-speed, and steady. Additionally, the safety problems with mobile terminals and also the Access to the internet are attached importance to. There's no accurate meaning of mobile cloud-computing, several concepts were suggested [1]. Mixing the idea of WSN, cellular devices could be considered as mobile sensors that can provide other cellular devices who're people that use the mobile cloud services with a few sensing information including atmosphere monitoring data, health monitoring data, and so forth. Access control issue handles supplying use of approved users and stopping unauthorized users to gain access to data. Attaching a summary of approved users to every information is the easiest means to fix achieve access control. Cloud-computing is definitely an Internet-based computing pattern by which shared sources are supplied to devices when needed. It's a growing but promising paradigm to integrating cellular devices into cloud-computing, and also the integration performs within the cloud based hierarchical multi-user data-shared atmosphere. Within the suggested scenario, users with various privilege levels have different legal rights to gain access to negligence sensing data from the cellular devices [2]. You with certain tag sets can obtain access to the particular encrypted data and decrypt it. The novel plan mainly concentrates on the information processing, storing and being able to access, which is made to make sure the users with legal government bodies to obtain corresponding classified data and also to restrict illegal users and unauthorized legal users obtain access to the information that makes it very appropriate for that mobile cloud-computing paradigms.

2. EXISTING SYSTEM:

Senders secure message with certain features of the approved receivers. The ABE based access control method uses several tags to

mark the attributes that the specific approved user must possess. You with certain tag sets can obtain access to the particular encrypted data and decrypt it. Plenty of paper introduced the plan concerning the attribute based file encryption access control method within the cloud-computing [3]. Within the mobile loud computing atmosphere, you will find tremendous data which must be processed and marked with attributions for that convenient attributing access before storing. Simultaneously, the hierarchical structure from the application users needs an authentication center entity to manage their attributes. Disadvantages of existing system: Doesn't guarantee Availability Problems with Confidentiality. Consumers' data weren't stored secret in cloud systems Data Integrity Issue No Multiple Controls.

3. VARIANT APPROACH:

Within the suggested scenario, users with various privilege levels have different legal rights to gain access to negligence sensing data from the cellular devices. Therefore, one same data needs to be encrypted into cipher text once, which ought so that you can be decrypted multiple occasions by different approved users. Differing in the existing paradigms like the HABE formula and also the original three-layer structure, the novel plan mainly concentrates on the information processing, storing and being able to access, which is made to make sure the application users with legal access government bodies to obtain corresponding sensing data and also to restrict illegal users and unauthorized legal users obtain access to the information, the suggested promising paradigm causes it to be very appropriate for that mobile cloud-computing based paradigm. Within this paper, a hierarchical access control method using modified hierarchical attribute-based file encryption along with a modified three-layer structures suggested [4]. What ought to be emphasized would be that the most significant highlight of within the suggested paper can be defined as the modified three-layer structure is made for solving the safety issues highlighted above. Benefits of suggested system: One cipher text could be decrypted by a number of keys. Both precise level description and user attribute ought to be supported within the access structure from the method.

Concerns in Mobile Cloud: Authority of information users: Different authority-level system to obtain access to sensing data for application users ought to be established because the paradigm is used within the hierarchical multi-user shared atmosphere, that also implies that you with greater authority level is deserving of all of the data the users with lower privilege level could obtain access to, as the lower privilege users can't obtain the data beyond his/her authority. Confidentiality of information: Even though the cloud services found in the scenario are supplied by private cloud which is designed to stay safe, it's still necessary to guarantee the sensing data protected against malicious organizations that don't fit in with the mobile cloud system. You will find mainly two techniques to enhance availability in cloud that are virtualization and redundancy. Presently, cloud technologies are mainly based virtual machine, since cloud providers can offer separated virtualized memory, virtualized storage, and virtualized CPU cycles, to ensure that users can invariably have them. Confidentiality is a huge barrier for cloud providers to popularize cloud to consumers because it arrives. There essentially exist two common approaches in current cloud infrastructures, say physical isolation and file encryption. Data integrity ensures people who their storing information is not modified by others or collapsing because of system failure [5]. To be able to possess a secure control system, cloud vendors may require a specialized operating-system. Mobile cloud-computing model within this paper implies that mobile phone users run applications on remote cloud servers rather of cellular devices themselves, the paradigm performs nearly as good as normal cloud-computing with computers with the exception that mobile cloud model connects cellular devices and

cloud servers through 3G or 4G while cloud-computing paradigm.

Updated model: It is crucial that you with lower privilege cannot obtain access to some good info the greater privilege user could possibly get to, as the greater authority user can obtain access to all of the data that's accessible for users in lower hierarchical position since different people that use the mobile cloud-computing system constitute a hierarchical authority system. So a safe and secure and hierarchical access control method ought to be suggested to use within the mobile cloud-computing system. The dwelling of file encryption keys should performs just like the hierarchical structure from the mobile cloud-computing users. One encrypted data could be received by a number of users. An altered hierarchical attribute-based file encryption access control method used in mobile cloud-computing is suggested within this paper, which changes a suggested plan known as hierarchical attribute-based file encryption HABE. One benefit of IBE would be that the sender didn't need to search the general public keys info on certificate authority (CA) online, which reduced the problem of poor CA performance. This improved system relieved PKG of effective burden that has been enhanced the machine efficiency by authenticating identities and transporting keys within locality area rather of worldwide area [6]. The general public key of the user is explained some IDs made up of the general public key of father node and also the users own ID within the approach to G-HIBE, the most crucial feature from the proposal would be that the users public key could reflect precise position from the user within the hierarchical structure. The main from the suggested plan is known as modified hierarchical attribute-based file encryption, which differs from the HABE plan. Each data user proven within the figure offers a distinctive ID that is a character string made to describe the characteristics of internal parties inside the system.

Access Controlling Methods: The sensing weather information is transported towards the layer1 which is a type of IaaS cloud service supplied by the cloud provider. The applications can exploit the sensors set up in the cellular devices to capture the elements data the applications need, including temperature value, humidity information, atmospheric pressure and so forth. The information model we present is inspired through the data model suggested, according to which our data model consists by format, device ID, size, time, value and period. How big sensing weather information is based on the raw weather data itself, which signifies how big just one weather data [7]. For time, as lengthy like a mobile phone captures data in the atmosphere where it's in, time the delivering action occurs is going to be considered because the time attribute from the raw sensing data. Something sign represents the most crucial sign of sensing data, this is it means is different from format to format, and different types of cellular devices have different meanings. You can obtain access to the cipher texts only when he/she satisfies the needs.

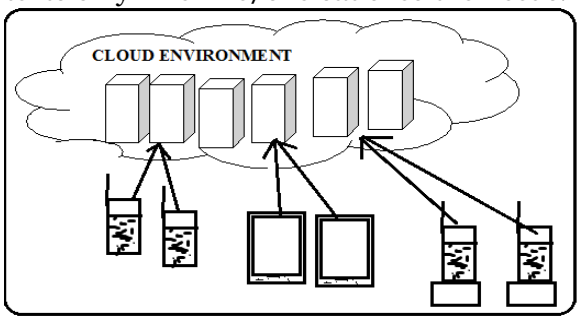


Fig.1.Mobile cloud computing overview

4. CONCLUSION:

The plan not just accomplishes the hierarchical access charge of mobile sensing data within the mobile cloud-computing model, but protects the information from being acquired by an untrusted 3rd party. The suggested access control method using MHABE is made to be applied inside a hierarchical multiuser data-shared atmosphere that is very appropriate for any mobile cloud-computing model to safeguard

the information privacy and defend unauthorized access. The keys within the authentication center should have exactly the same hierarchical structure just like the structure of user's privilege levels. The paper suggested an altered HABE plan if you take benefits of attributes based file encryption and hierarchical identity based file encryption access control processing. In contrast to the initial HABE plan, the novel plan could be more adaptive for mobile cloud-computing atmosphere to process, store and connect to the enormous data and files as the novel system allow different privilege entities access their allowed data and files.

REFERENCES:

[1] Yuan peng Xie, Hong Wen, Bin Wu, Yixin Jiang and Jiaxiao Meng, "A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing", IEEE Transactions on Cloud Computing, 2016.

[2] Q. Han, S. Liang, and H. Zhang, "Mobile cloud sensing, big data, and 5g networks make an intelligent and smart world," Network, IEEE, vol. 29, no. 2, pp. 40–45, 2015.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007, pp. 321–334.

[4] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Effects of wi-fi and bluetooth battery exhaustion attacks on mobile devices," in System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010, pp. 1–9.

[5] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, 2010, pp. 105–112.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98.

TRUSTBSM: INTEGRATION OF MULTIPLE DATA INTO RECOMMENDATION SYSTEM

Dr.A.Janardhan[1]., A Rishika[2]., B Bidisha[3]., K Mouna Sri[4]., M Shirisha[5]
1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- dhana48@yahoo.co.in)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0501, 17RG1A0508, 17RG1A0527, 17RG1A0535), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT:

Our analysis of rely upon four real-world data sets established that trust and ratings were complementary to one another, and both pivotal for additional accurate recommendations. Computational complexity of Trust BSM indicated its capacity of scaling as much as large-scale data sets. An analysis of social trust data from four real-world data sets shows that not just the specific but the implicit influence of both ratings and trust should be considered inside a recommendation model. One possible explanation is the fact that these trust-based models focus an excessive amount of around the utility of user trust but disregard the influence of item ratings themselves. The influence could be explicit or implicit. We advise Trust BSM, a trust-based matrix factorization way of recommendations. Trust BSM therefore builds on the top of the condition-of-the-art recommendation formula, BSM, by further incorporating both explicit and implicit influence of reliable and having faith in users around the conjecture of products to have an active user. The suggested strategy is the first one to extend BSM with social trust information.

Keywords— Trust-based model, matrix factorization, implicit trust, recommendation algorithm.

1. INTRODUCTION:

Collaborative filtering is among the most widely used strategies to implement a recommender system. The thought of CF is the fact that users concentrating on the same preferences previously will probably favor exactly the same products later on. However, CF is affected with two well-known issues: data sparsity and cold start. To assist resolve these problems, many researchers make an effort to incorporate social trust information to their recommendation models, considering that model-based CF approaches outshine memory-based ones [1]. The implicit influence of ratings continues to be shown helpful in supplying accurate recommendations. First, trust details are extremely sparse, yet complementary to rating information. Second, users are strongly correlated using their out-going reliable neighbors. The 3rd observation further signifies an identical conclusion within-coming having faith in neighbors. Additionally, we further think about the influence of trust users around the rating conjecture to have an active user. However, the specific influence of trust can be used to constrain that user-specific vectors should comply with their social trust relationships. In this manner, the concerned issues could be better alleviated. Therefore, both explicit and implicit influence of item ratings and user trust continues to be considered within our model, indicating its novelty. Additionally, a weighted-_-regularization strategy is accustomed to assist in avoiding over-fitting for model learning. Our first contribution would be to do an empirical trust analysis and realize that trust and ratings can complement to one another, which users might be strongly or weakly correlated with one another based on various kinds of social relationships [2]. Trust BSM integrates multiple information sources in to the recommendation model to be able to lessen the data sparsity and cold start problems as well as their degradation of recommendation performance. Propose a singular trust-based recommendation approach that comes with both influence of rating and trust information. conduct extensive experiments to judge the potency of the suggested approach in 2 various kinds of testing views of users and cold-start users.

2. EXISTING SYSTEM:

Many approaches happen to be suggested in this subject, including both memory- and model-based methods. Golbeck

proposes a Tidal Trust method of aggregate the ratings of reliable neighbors for any rating conjecture, where trust is computed inside a breadth-first manner. Guo et al. complement a user's rating profile by merging individuals of reliable users by which better recommendations cane generated, and also the cold start and knowledge sparsity problems could be better handled. However, memory-based approaches have a problem in adjusting to large-scale data sets, and therefore are frequently time-consuming to look candidate neighbors in large user space. Zhu et al. propose a graph Laplacian regularizer to capture the potentially social relationships among users, and make up the social recommendation problem like a low rank semi-definite problem [3]. However, empirical evaluation signifies that very marginal enhancements are acquired in comparison to the RSTE model. Yang et.al. propose a hybrid method TrustMF that mixes both a truster model along with a trustee model in the perspectives of truster's and trustees, that's, both users who trust the active user and individuals who're reliable through the user will influence the user's ratings on unknown products. Disadvantages of existing system: Existing trust-based models might not work nicely when there exists only trust-alike relationships. These observations could other sorts of recommendation problems. Existing trust based models consider just the explicit influence of ratings. The utility of ratings isn't well exploited. Existing trust-based models don't think about the explicit and implicit influence of trust concurrently.

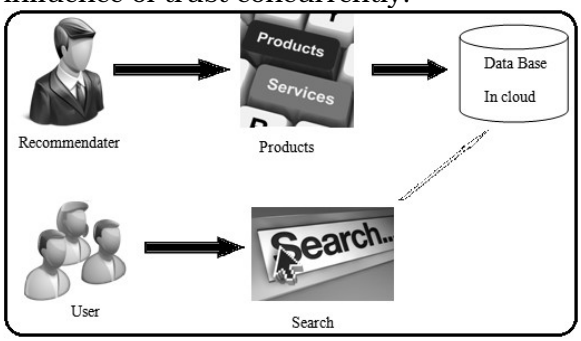


Fig.1.Proposed Method

3. TRUST-BASED MODEL:

We advise a singular trust-based recommendation model regularized with user trust and item ratings, referred to as TrustBSM. Our approach builds on the top of the condition-of-the-art model BSM by which both explicit and implicit influence of user-item ratings are participating to create predictions. Additionally, we further think about the influence of trust users around the rating conjecture to have an active user. This helps to ensure that user specific vectors could be learned using their trust information even when a couple of or no ratings receive. In this manner, the concerned issues could be better alleviated. Therefore, both explicit and implicit influences of item ratings and user trust happen to be considered within our model, indicating its novelty. Additionally, a weighted-regularization strategy is accustomed to assist in avoiding over-fitting for model learning. The experimental results around the data sets show our approach works considerably much better than other trust-based counterparts along with other ratings-only high-performing models when it comes to predictive precision, and it is more able to dealing with the cold-start situations [4]. There's two primary recommendation tasks in recommender systems, namely item recommendation and rating conjecture. Most algorithmic approaches are just created for both of the advice tasks, and our work concentrate on the rating conjecture task.

Trust Analysis: Trust could be further split up into exploit trust and implicit trust. Explicit trust refers back to the trust statements directly per users. We define the trust-alike relationships because the social relationships which are similar with, but less strong than social trust. The similarities are that both types of relationships indicate user preferences to some degree and therefore helpful for recommender systems, as the variations are individuals trust-alike relationships are frequently less strong in strength and apt to be noisier. the social relationships in Epinions

and Ciao are trust relationships whereas individuals in Flixster and FilmTrust are trust-alike relationships. In connection with this, a trust-aware recommender system that focuses an excessive amount of on trust utility will probably achieve only marginal gains in recommendation performance. Additionally, the sparsity of explicit trust also implies the significance of involving implicit rely upon collaborative filtering. However, trust details are complementary towards the rating information. As a result, although getting distinct distributions over the different data sets, trust could be a complementary information source to item ratings for recommender systems. Within this work, we concentrate on the influence of social rely upon rating conjecture, i.e., the influence of trust neighbors with an active user's rating for any particular item, a.k.a. social influence. Within the social systems with relatively weak trust-alike relationships, implicit influence might be more indicative than explicit values for recommendations [5]. Hence, a trust-based model that ignores the implicit influence of item ratings and user trust can lead to deteriorated performance if being put on such cases. The 3rd observation signifies that the influence of truster's might be comparable with this of trustees, and therefore might also provide added value to item ratings. Our approach presented next is made upon these 3 observations.

A Trust-Based Recommendation Model: The recommendations condition in the work would be to predict the rating that the user can give for an unknown item, for instance, the worth that user u3 can give to item i3, according to both a person-item rating matrix along with a user-user trust matrix. Other well-recognized recommendation problems include for instance top-N item recommendation. Since a person only rated a little part of products, the rating matrix R is just partly observed and oftentimes very sparse. The actual assumption is the fact that both users and products could be characterized by a small amount of features. We limit the trusters within the trust matrix and also the active users within the rating matrix to talk about exactly the same user-feature space to be able to bridge them together.

TrustBSM Model: our TrustBSM model is made on the top of the condition-of-the-art model referred to as BSM suggested by Koren. The explanation behind BSM is to consider user/item biases and also the influence of rated products apart from user/item specific vectors on rating conjecture. Formerly, we've stressed the significance of trust influence for much better recommendations, and it is possibility to be generalized to believe-alike relationships. Hence, we are able to boost the trust-not aware BSM model by both explicit and implicit influence of trust. The implicit influence of trust neighbors on rating conjecture therefore includes a double edged sword: the influence of both trustees and trusters [6]. An all natural and simple strategy is to linearly combine the 2 kinds of implicit trust influence. Inside a trust relationship, a person u could be symbolized either by pu as trustor or by wu as trustee. Another way would be to model the influence of user u's trust neighbors, including both reliable and having faith in users, in the way of having faith in users. Additionally, as described earlier, we constrain the user-specific vectors decomposed in the rating matrix and individuals decomposed in the trust matrix share exactly the same feature space to be able to bridge both matrices together. In this manner, these two kinds of information could be exploited inside a unified recommendation model. However, we reason that such consideration may pressure the model to become more biased towards popular users and products. Besides, because the active users might be socially associated with other trust neighbors, the penalization on user-specific vector considers two cases: reliable by others and having faith in other users. The computational duration of understanding the TrustBSM model is principally taken by

evaluating the aim function L and it is gradients against feature vectors [7]. The important thing idea behind the TrustBSM model is to take into consideration both explicit and implicit influences of item ratings as well as social trust information when predicting users' ratings for unknown products.

4. CONCLUSION:

Our first contribution would be to do an empirical trust analysis and realize that trust and ratings can complement to one another, which users might be strongly or weakly correlated with one another based on various kinds of social relationships. These observations motivate us to think about both explicit and implicit influence of ratings and trust into our trust-based model. Potentially, these observations might be also advantageous for solving other sorts of recommendation problems. Our analysis of rely upon four real-world data sets established that trust and ratings were complementary to one another, and both pivotal for additional accurate recommendations. Computational complexity of TrustBSM indicated its capacity of scaling as much as large-scale data sets. Comprehensive experimental results around the four real-world data sets demonstrated our approach TrustBSM outperformed both trust- and ratings-based methods in predictive precision across different testing views and across users with various trust levels. However, the literature has proven that models for rating conjecture cannot suit the job of top-N item recommendation. Our novel approach, TrustBSM, considers both explicit and implicit influence of ratings as well as trust information when predicting ratings of unknown products. Both trust influence of trustees and trusters of active users take part in our model. Additionally, a weighted regularization strategy is adapted and used to further regularize the generation of user- and item-specific latent feature vectors. We figured that our approach can better alleviate the information sparsity and cold start problems of recommender systems.

REFERENCES:

[1] GuibingGuo, Jie Zhang, and Neil Yorke-Smith, "A Novel Recommendation Model Regularizedwith User Trust and Item Ratings", ieee transactions on knowledge and data engineering 2016.

[2] Q. Yuan, L. Chen, and S. Zhao, "Factorization vs. regularization: fusing heterogeneous social relationships in top-n recommendation," in Proceedings of the 5th ACM conference on Recommender systems (RecSys), 2011, pp. 245–252.

[3] H. Fang, Y. Bao, and J. Zhang, "Leveraging decomposed trust in probabilistic matrix factorization for effective recommendation," in Proceedings of the 28th AAAI Conference on Artificial Intelligence (AAAI), 2014, pp. 30–36.

[4] G. Guo, J. Zhang, and N. Yorke-Smith, "Leveraging multiviews of trust and similarity to enhance clustering-based recommender systems," Knowledge-Based Systems (KBS), vol. 74, no. 0, pp. 14 –27, 2015.

[5] H. Ma, I. King, and M. Lyu, "Learning to recommend with social trust ensemble," in Proceedings of the 32nd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR), 2009, pp. 203–210.

[6] M. Jamali and M. Ester, "Trustwalker: a random walk model for combining trust-based and item-based recommendation," in Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), 2009, pp. 397–406.

A VIBRANT CODEBOOK PRODUCTION SCHEME FOCUSING HIGH DIMENSIONAL VISUALS

P Lavnya[1]., B Salomi[2]., B Srinija[3]., J Mounika[4]., U Kalyani[5]
1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- mail.to.plavanya@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0510, 17RG1A0511, 17RG1A0523, 17RG1A0558), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***A singular objective function for codebook optimization inside a P2P atmosphere is suggested, which views both relevance information and also the workload balance concurrently. Therefore, we advise an engaged codebook updating method by optimizing the mutual information between your resultant codebook and relevance information, and also the workload balance among nodes that manage different codewords. A distributed codebook updating formula according to splitting/merging of person codewords is suggested, which optimizes the aim function with low updating cost. While the majority of the existing methods concentrate on indexing high dimensional visual features and also have limitations of scalability, within this paper we advise a scalable method for content-based image retrieval in peer-to-peer systems by using the bag-of-visual words model. The codebook such an atmosphere must be updated periodically, instead of stored static. Within this paper, we present a singular approach to dynamically generate increase a worldwide codebook, which views both discriminability and workload balance. Additionally, a peer-to-peer network frequently evolves dynamically, making a static codebook less efficient for retrieval tasks. To be able to further improve retrieval performance and lower network cost, indexing pruning techniques are developed. In contrast to centralized environments, the important thing challenge would be to efficiently get you a global codebook, as images are distributed over the whole peer-to-peer network.***

Keywords: peer-to-peer, information maximization, Bag-of-visual-words (BoVW), Codebook.

1. INTRODUCTION:

The ever-growing quantity of multimedia data and computational turn on P2P systems exposes both need and possibility of massive multimedia retrieval applications for example content-based image discussing, and copyright violation recognition. To aid content indexing and steer clear of message flooding, structured overlay systems for example Distributed Hash Tables are frequently implemented on the top of the physical network. However, the bag-of-visual-words model continues to be effectively useful for massive image retrieval [1]. To use the BoVW model, the next three steps are needed: numerous local regions or tips is going to be identified from your image and every region or a key point is going to be symbolized having a high dimensional descriptor because the features extracted have been in a continuing space, a codebook is generated to quantize the feature vectors into discrete codewords, thus a picture could be construed as some feature codewords and like the BoW model, record distributions from the codewords inside a given image is required to represent the look. Within this paper we make use of the well-studied tf-idf weighting plan and cosine distance because the similarity measurement. Therefore it is important to minimize the network cost and the workload balanced during both codebook updating and retrieval. For data dynamics, the information inside a P2P network is under constant churn. While processing queries, each node collects the relevance information and workload data. Using the relevance information, we increase the information supplied by the codebook concerning the retrieval results, thus minimizing the data loss suffered by quantization. With workload data, we try to acquire a fair workload among nodes, thus staying away from overloading or under loading nodes. For that retrieval process, we could leverage the present research on P2P-based text retrieval systems, because the BoVW model is definitely an example towards the BoW model [2].

2. EXISTING SYSTEM:

The present systems adopt a worldwide feature approach: a picture is symbolized like a high dimensional feature vector, and also the similarity between files is measured while using distance between two feature vectors. Usually, the feature vectors are listed in a

distributed high-dimensional index or Locality Sensitive Hashing (LSH) within the DHT overlay As opposed to centralized environments, data in P2P systems is shipped among different nodes, thus a CBIR formula must index and check for images inside a distributed manner.P2P systems they are under constant churn, where nodes join/leave and files publish to/remove in the network, the index must be updated dynamically to adjust to such changes. Dexing and Locality-Sensitive Hashing. Our prime-dimensional indexing based approaches keep feature vectors inside a data structure, often a tree or perhaps a graph, to attain effective search space pruning during retrieval. In structured P2P systems, our prime-dimensional index is determined inside a distributed excess of the P2P overlay, dexing and Locality-Sensitive Hashing [3]. Our prime-dimensional indexing based approaches keep feature vectors inside a data structure, often a tree or perhaps a graph, to attain effective search space pruning during retrieval. In structured P2P systems, our prime-dimensional index is determined inside a distributed excess of the P2P overlay. Disadvantages of existing system: Even just in a centralized atmosphere, the performance of high-dimensional indexing is affected with the well-known "curse of dimensionality". Even if it's possible to update the hash functions with altering data, applying it within the DHTs is extremely challenging. Because the information is stored among nodes of corresponding hash ID, single-bit change from the hash function output can lead to large part of (if not completely) data being assigned to a new node, causing heavy network traffic.

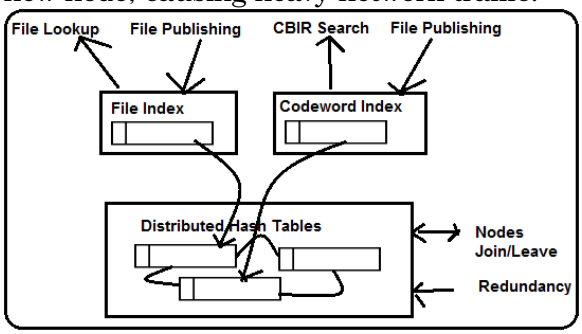


Fig.1.System Framework

3. GENERATING CODEBOOK:

Within this paper, we present a singular approach to dynamically generate increase a worldwide codebook, which views both discriminability and workload balance. While processing queries, each node collects the relevance information and workload data. Using the relevance information, we increase the information supplied by the codebook concerning the retrieval results, thus minimizing the data loss suffered by quantization. With workload data, we try to acquire a fair workload among nodes, thus staying away from overloading or under loading nodes. According to both of these criteria, the codebook partitioning is updated routinely by splitting/merging codewords, thus allowing the codebook to developed to reduce in size in compliance towards the data distribution. To reduce the price of codebook updating, the choice whether a codeword ought to be split/merged is taken by its managing node individually. Finally, the updates are synchronized over the network in the finish of every iteration [4]. Consequently, the discriminability and workload balance is enhanced continuously using the churn from the P2P network.

Framework from the model: To aid various operations in our CBIR system, we develop a file index along with a codeword index over DHT. The codeword index, which stores the postings of every codeword, is put into offer the storage and retrieval of BoVW features. It's basically an inverted index which stores records with codeword ID as DHT key, and also the corresponding postings wk as value. All of the operations from the CBIR system are converted into lookup or modification from the records from the file and/or codeword index. File Index: Searching in the proprietors of the exact file is conducted having a DHT lookup operation. Publishing a brand new file is conducted with a DHT store operation. Codeword Index: The CBIR search is basically an inverted index lookup within the codeword index. Whenever a new file is added, besides publishing an admission to the file index the file owner may also extract and quantize the

characteristics to create codewords, then place them towards the corresponding records within the codeword index [5]. Whenever a file is taken away in the file index (without any owner), the related codeword postings is going to be taken off the codeword index. The worldwide BoVW codebook is updated via splitting and merging codewords. The SPLIT/MERGE operations are basically publishing/removing records from the codeword index.

Analyzing Complexity: Our bodies completes a question within the following steps: a) feature extraction b) quantization c1) delivering posting lookup message c2) receiving postings and d) aggregating postings and producing the rank list. Within our system, we allow the codebook size grow as increasing numbers of nodes join the network. Therefore, our suggested retrieval approach is scalable when it comes to both query cost and scope. For codebook generation increase, each iteration includes three steps: a) determine the update operation for every codeword b) for split and merge, transfer the postings to/from neighbor nodes and c) synchronize the brand new group of codewords over the network.

Codebook Generation and Updating: Our codebook updating formula runs iteratively. Throughout an updating iteration, each codeword node pk decides be it codeword k ought to be split/merged/unchanged in line with the relevance information collected from past queries, and also the current workload. The iterative process runs continuously to be able to maintain an up-to-date codebook during data churn [6]. When it comes to information maximization, we aim to locate a partitioning from the feature space so that partitions/codewords are correlated towards the collected relevance information. For workload balance, we try to partition the feature space evenly and accommodate the computational capacity of every nodes, to ensure that no nodes could be overloaded or under loaded.

Removing Technique with BoVW: Once the codebook is prepared, for any given query, the retrieval process basically includes three steps: removing visual features and acquiring BoVW based representation for that query, retrieving the postings via DHT lookup, and calculating the similarity between your query and candidate images. In massive BoW based retrieval systems index pruning has been utilized to lessen the retrieval cost. We assess the suggested system having a multi-threaded program that simulates the codeword index, in which the updating procedure for each codeword node is performed within an individual thread. Consequently, the suggested approach is scalable to the amount of images shared inside a P2P network and also the evolving nature of P2P systems. To be able to further enhance the retrieval performance from the suggested approach and lower network cost, indexing pruning techniques are applied.

4. LITERATURE OVERVIEW:

GFModel: The worldwide feature model represents each image with one high-dimensional feature vector, and measures the similarity between images using the distance between their feature vectors. This model is adopted by many people existing P2P CBIR systems. The Locality-Sensitive Hashing based approaches use special hash functions that output exactly the same value for similar objects. To enhance the locality from the hash functions, most works compromise the even distribution of hash buckets. We observe that the BoVW histogram, which is discussed later, may also be considered and processed like a high dimensional global feature.

BoVW Model: The bag-of-visual-words model represents each image having a bag of quantized codewords produced from local features, and measures the similarity between images using the BoVW histogram similar to some bag-of-words type of text Retrieval. There's two ways of distribute index tuples: document partition, and term partition. Document partition typically includes a greater network cost than term partition, particularly when the index includes a good term sparsity. To help lessen the network cost and tackle the problem of workload balance with term partition, different techniques happen to be

suggested [7]. Our suggested method accomplish this in an exceedingly different way: we keep your term distribution unchanged, but update the codebook to keep the performance when information is altered. In this manner, nodes managing different terms may change the workload individually having a reduced network cost.

Codebook Generation: our suggested codebook learning method takes both codebook discriminability and workload balance into account. The discriminability is measured through the mutual information supplied by the codebook about user feedback. To create our codebook adaptive to dynamic P2P environments, the codebook partitioning is enhanced by splitting/merging codewords, therefore allowing the codebook to develop to reduce in size in compliance towards the data distribution and available sources.

5. CONCLUSION:

It's the first study to research scalable CBIR using the BoVW model in P2P systems. Peer-to-peer networking provides a scalable solution for discussing multimedia data over the network. With a lot of visual data distributed among different nodes, it's an important but challenging issue to do content-based retrieval in peer-to-peer systems. Within this paper we present a bag-of-visual-words model based method for content based image retrieval in peer- peer systems. To be able to overcome the problem in generating and looking after a worldwide codebook once the BoVW model is deployed in P2P systems, we formulate the issue of updating a current codebook as optimizing the retrieval precision and workload balance.

REFERENCES:

[1] Lelin Zhang, Student Member, IEEE, Zhiyong Wang, Member, IEEE,Tao Mei, Senior Member, IEEE, and David Dagan Feng, Fellow, IEEE, "A Scalable Approach for Content-BasedImage Retrieval in Peer-to-Peer Networks", ieee transactions on knowledge and data engineering, vol. 28, no. 4, april 2016.

[2] J. Sivic and A. Zisserman, "Video Google: A text retrieval approach to object matching in videos," in Proc. IEEE Int. Conf. Comput. Vis., 2003, vol. 2, pp. 1470–1477.

[3] C. Tang, Z. Xu, and S. Dwarkadas, "Peer-to-peer information retrieval using self-organizing semantic overlay networks," in Proc. ACM Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2003, pp. 175–186.

[4] T. Mei, Y. Rui, S. Li, and Q. Tian, "Multimedia search reranking: A literature survey", ACM Comput. Surveys, vol. 46, no. 3, pp. 38:1–38:38, Jan. 2014.

[5] M. R. Trad, A. Joly, and N. Boujemaa, "Distributed KNN-graph approximation via hashing," in Proc. ACM Int. Conf. Multimedia Retrieval, 2012, pp. 43:1–43:8.

[6] D. Li, J. Cao, X. Lu, and K. C. Chan, "Efficient range query processing in peer-to-peer systems," IEEE Trans. Knowl. Data Eng., vol. 21, no. 1, pp. 78–91, Jan. 2009.

[7] H. J_egou, F. Perronnin, M. Douze, J. S_anchez, P. P_erez, and C. Schmid, "Aggregating local image descriptors into compact codes," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 9, pp. 1704–1716, Sep. 2012.

GENERATING A TRAPDOOR FOR EACH PROPERTY IN SECRET CODE

N Radhika[1]., K Harika[2]., K Tanvi [3]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- radhika_ckv29@yahoo.com)

2, 3 B.Tech IV Year CSE, (17RG1A0528, 17RG1A0529),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Nonetheless, her interests are going to be uncovered towards the shop website because the cookies record the keywords of her interests. With the aid of understanding cloud server provider and trapdoor connected with hired keyword like "cosmetics", the consumer looks for the matching ciphertext without dripping the privacy of "cosmetics". The encrypted ciphertexts is going to be distributed to intended receivers whose access structure is going to be satisfied by attribute set baked into ciphertexts. This sort of computing model brings challenges towards the privacy and security of information kept in cloud. Attribute-based file encryption technology has been utilized to create fine-grained access control system, which supplies one good approach to solve the safety issues in cloud setting. However, the computation cost and ciphertext size in many ABE schemes grow using the complexity from the access policy. Outsourced ABE with fine grained access control system can largely lessen the computation cost for users who wish to access encrypted data kept in cloud by outsourcing the heavy computation to cloud company. In the following paragraphs, we advise a Clubpenguin-ABE plan that gives outsourcing key-issuing, understanding and keyword search function. A is definitely an tree-based access policy bound track of user private key, is definitely an attribute set baked into ciphertext, may be the attribute world, and it is a threshold value occur advance. Many applications use complex access control mechanisms to safeguard encrypted sensitive information. Our plan is efficient because we only have to download the partial understanding ciphertext akin to a particular keyword. Within our plan, time-consuming pairing operation could be outsourced towards the cloud company, as the slight operations can be achieved by users. An essential issue is how you can search helpful information from large data kept in CSPs.***

Keywords— Encryption, cloud computing, outsourced key-issuing, outsourced decryption, keyword search.

1. INTRODUCTION

Outsourced ABE(OABE) with fine-grained access control system can largely lessen the computation cost for users who wish to access encrypted data kept in cloud by outsourcing the heavy computation to cloud company (CSP) [1]. However, as the quantity of encrypted files kept in cloud has become very huge, that will hinder efficient query processing. In Clubpenguin-ABE plan, a malicious user maybe shares his attributes along with other users that might leak his understanding privilege like a understanding black box because of financial profits [2]. TA may be the attribute authority center, which accounts for the initialization of system parameters, and also the generation of attribute private keys and trapdoor. Two kinds of ABE schemes, namely key-policy ABE and ciphertext-policy ABE are suggested. For KP-ABE plan, each ciphertext is expounded toa group of attributes, and every user's private secret is connected by having an access insurance policy for attributes. The safety requirement of our ABE plan is comparable to that suggested. We adopt a relaxation based on the secure notion known as replay able CCA (RCCA) security, which allows modifications towards the ciphertext and they're notable to alter the implied message in an ideal way. More precisely, they follow the protocol, but try to obtain additional information based on remarkable ability. Furthermore, curious users are allowed to collude with D-CSP and S-CSP. Verifiability is a vital feature of KSF-OABE, so our future works would be to construct KSF-OABE which could provide verifiability [3].

2. TRADITIONAL METHOD:

The computing paradigm also brings some challenges towards the privacy and security of information whenever a user outsources sensitive data to cloud servers. To resolve the problem, we create the indexes for" cosmetics" and "clothing" inside a secure

manner. Many applications use complex access control mechanisms to safeguard encrypted sensitive information [4]. Sahai and Waters addressed this issue by presenting the idea for ABE. For KP-ABE plan, each ciphertext relates to some attributes, and every user's private secret is connected by having an access insurance policy for attributes.

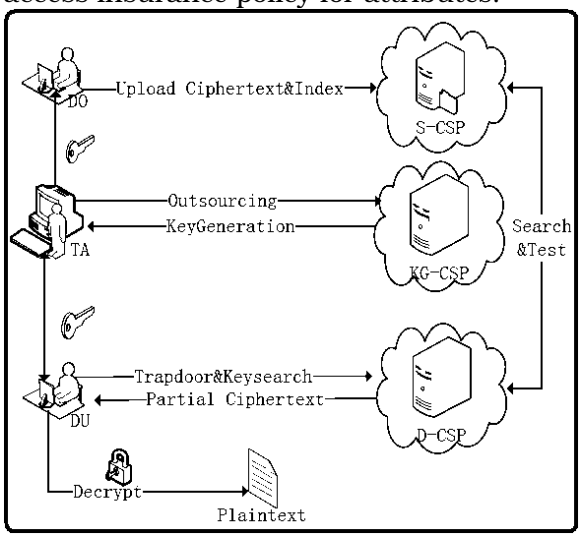


Fig.1.Proposed system framework

3. ENHANCED ENCRYPTION:

It established fact the shopping website provides extensive referral links that are collected by shopping website with the cookies. The cookies record the keywords that you simply frequently query. For instance, if Alice loves to buy online and frequently browses the cosmetics and clothing, she frequently enters keywords like "cosmetics" and "clothing". Nonetheless, her interests are going to be uncovered towards the shop website because the cookies record the keywords of her interests. Cloud-computing becomes more and more popular for data proprietors to delegate their data to public cloud servers while allowing intended data users to retrieve these data kept in cloud. The suggested KSF-OABE plan is demonstrated secure against selected-plaintext attack (CPA). CSP performs partial understanding task delegated by data user not understanding anything concerning the plaintext. Furthermore, the CSP are capable of doing encrypted keyword search not understanding anything concerning the keywords baked into trapdoor [5]. Our plan is efficient because we only have to download the partial understanding ciphertext akin to a particular keyword. Within our plan, time-consuming pairing operation could be outsourced towards the cloud company, as the slight operations can be achieved by users. An essential issue is how you can search helpful information from large data kept in CSPs. The cookies record the keywords that you simply frequently query. The suggested plan props up purpose of keywords search which could greatly improve communication efficiency and additional safeguard the privacy and security of users. The RCCA to safeguard our KSF-OABE is referred to as a game title from a challenger as well as an foe. The prospective for that foe is to buy any helpful info on ciphertext and index of keywords which aren't meant for him. For Clubpenguin-ABE plan, the roles of the attribute set as well as an access policy are reversed. The very first challenge in our construction on privacy and security would be to defend the conspiracy attack from dishonest users and D-CSP. The suggested KSF-OABE plan with keyword search function is safe against selected-plaintext attack launched by foe in selective model under DBDH assumption [6]. The 2nd challenge in our construction on privacy and security would be to defend the conspiracy attack from curious KG-CSP. Apparently, to be able to recover the content, our plan is efficient because we only have to download the partial understanding ciphertext akin to a particular keyword. Within our plan, time-consuming pairing operation could be outsourced towards the cloud company, as the slight operations can be achieved by users.

4. CONCLUSION:

ACP-ABE plan that supports outsourcing key-issuing, understanding and keyword search function is CPA-secure when the foe cannot launch queries in above game. Understanding ACP-ABE plan that supports outsourcing key-issuing, understanding and keyword search function is selectively secure when the foe must submit the challenger

attribute set. We compared the performance from the four procedures in our plan. We have seen the computation costs in the stages of Setup and File encryption grow linearly considering the variety of the attribute both in systems and also the computation costs within our plan.

REFERENCES:

[1] H.L. Qian, J.G. Li, Y.C. Zhang and J.G. Han, "Privacy Preserving Personal Health Record Using Multi-Authority Attribute-Based Encryption with Revocation, "International Journal of Information Security, pp. 1-11, 2015,doi:10.1007/s10207-014-0270-9.

[2] M. Yang, F. Liu, J.L. Han and Z.L. Wang, "An Efficient Attribute Based Encryption Scheme with Revocation for Outsourced Data Sharing Control," Proc. 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC '11), pp. 516-520, Oct. 2011, doi:10.1109/IMCCC.2011.134.

[3] W.R.Liu, J.W.Liu, Q.H.Wu, B.Qin, and Y.Y.Zhou, "Practical Direct Chosen Ciphertext Secure Key-Policy Attribute-Based Encryption with Public Ciphertext Test,"ESORICS'14, LNCS 8713, Berlin: Springer-Verlag, pp. 91-108, 2014.

[4] B. Libert and D. Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption,"Proc. 11th International Workshop on Practice and Theory in Public Key Cryptography(PKC'08),R. Cramer, ed., LNCS 4939, Berlin: Springer-Verlag, pp. 360-379, 2008.

[5] J. Li, X.F. Chen, J.W. Li, C.F. Jia, J.F. Maand W.J. Lou, "Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption,"Proc.18th European Symposium on Research in Computer Security(ESORICS '13),LNCS8134,Berlin: Springer-Verlag, pp. 592-609, 2013.

[6] J.G.Li, Y.R.Shi, and Y.C.Zhang, "Searchable Ciphertext-Policy Attribute-Based Encryption with Revocation in Cloud Storage,"International Journal of Communication Systems, 2015,doi:10.1002/dac.2942

RANDOM WALK THROUGH IN NET FOR A RESOLUTION TO FIND A DOC/DEVICE

V Sireesha[1]., Affia Sultana[2]., K Maheswari[3]., T Shiva priya[4]., U Pranitha[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- veernalasireesha@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0502, 17RG1A0524, 17RG1A0554, 17RG1A0556),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT:

Among the fundamental functions of these systems is efficiently resolving queries or finding files/sources. This is actually the problem addressed within this paper. In structured systems, peers/files/sources are organized to create overlays with specific topologies and qualities. Locating a document or resource within an unstructured peer-to-peer network is definitely an exceedingly difficult problem. The approach is proven to become stabilize the query load susceptible to a grade and services information constraint, i.e., an assurance that queries' routes meet pre-specified class-based bounds on their own connected a priori possibility of query resolution. The inefficiencies of purely unstructured systems could be partly addressed by hybrid P2P systems. Additional aspects connected with reducing complexity, estimating parameters, and adaptation to class-based query resolution odds and traffic loads are studied. The job of proposes a strategy where peers cache the final results of past queries as informed by reverse-path forwarding. This method involves considerable overhead, isn't load sensitive, and hasn't yet given guarantees on performance. An explicit portrayal from the capacity region for such systems is offered and numerically fit it connected with random walk based searches.

Keywords— Distributed Hash Table (DHT), P2P network, stability, reverse-path forwarding.

1. INTRODUCTION

Search mechanisms that perform name resolution according to distributed hash table coordinate systems could be devised to attain good forwarding-delay qualities. Such systems, the query traffic may rely on how keys are assigned. This post is conveyed to super peers whenever a subordinate peer joins an excellent peer. Unstructured systems, by comparison, are simpler to put together and keep, however their mostly random overlay topologies make realizing efficient searches challenging [1]. Within this paper we advise a question routing approach that makes up about arbitrary overlay topologies, nodes with heterogeneous processing capacity, e.g., reflecting their amount of altruism and heterogeneous class-based likelihoods of query resolution at nodes which might reflect query loads and the way files/sources are distributed over the network. Inside a purely unstructured P2P network, a node only knows its overlay neighbors. With your limited information, search approaches for unstructured systems have mostly been according to limited-scope flooding, simulated random walks, as well as their variants. Regrettably in heterogeneous settings where service capacity or resolution likelihoods vary across peers, such search techniques perform poorly under high query loads. Super-peers can resolve queries by examining the files/sources they've, in addition to individuals of the subordinate community. To balance the burden across heterogeneous super-peers, the insurance policy is aimed at lowering the differential backlog at neighboring super-peers, while considering the category and history information to enhance the query's resolvability. By comparison, goal to supply a grade and services information in resolving queries without any fixed destinations. We propose several natural enhancements to the backpressure based query routing policy. We model the uncertainty within the places where a question might be resolved based upon in which the file/object of great interest is put. Within our approach we introduce an idea of query classes. The concept is the fact that this type of grouping of queries into classes can be used a minimal overhead method of make helpful inferences regarding how to relay queries [2]. Basically, our policy is really a biased random walk where forwarding decision for every query is dependent on immediate query loads at super-peers. Within our P2P

query routing setting the destination of the totally unfamiliar a priori. We reduce delays using a simple 'work conserving' policy which efficiently uses available sources in routing queries each and every node. We further propose a condition aggregation policy targeted at lowering the complexity as a result of the necessity to track a brief history of presently unresolved searches.

2. ORIGINAL MODEL:

Inside a purely unstructured P2P network, a node only knows its overlay neighbors. With your limited information, search approaches for unstructured systems have mostly been according to limited-scope flooding, simulated random walks, as well as their variants. Regrettably in heterogeneous settings where service capacity or resolution likelihoods vary across peers, such search techniques perform poorly under high query loads [3]. The inefficiencies of purely unstructured systems could be partly addressed by hybrid P2P systems, e.g., FastTrack and Gnutella2. Disadvantages of existing system: In structured systems the problem of search/discovery is now use those of maintaining the structural invariants needed to attain efficient in query resolution specifically in dynamic settings with peer/content churn or when reactive load balancing is needed. Standard backpressure-based routing our policies are afflicted by a significant drawback: each node must share the condition of their potentially many non-empty queues using its neighbors. Complexity problem is going to be also elevated.

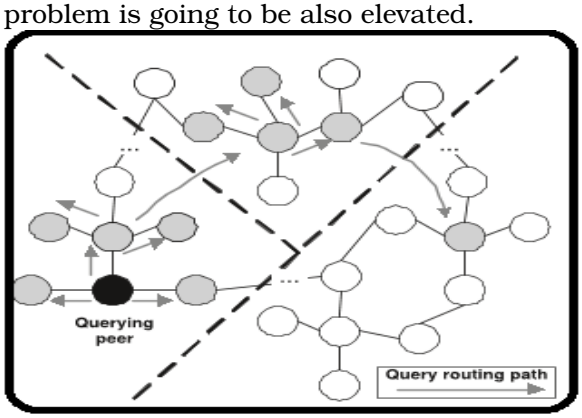


Fig.1.Proposed system framework

3. QUERY RESOLUTION SCHEME:

Given a hybrid P2P topology and query classification, we advise a singular query resolution mechanism which stabilizes the machine for those query loads inside a 'capacity region', i.e., the group of loads that stability is achievable. Basically, our policy is really a biased random walk where forwarding decision for every query is dependent on immediate query loads at super-peers. To balance the burden across heterogeneous super-peers, the insurance policy is aimed at lowering the differential backlog at neighboring super-peers, while considering the category and history information to enhance the query's resolvability [4]. Our policy draws upon standard backpressure routing formula, which is often used to attain stability in packet switching systems, we advise a question forwarding mechanism for unstructured P2P systems using the following qualities. It dynamically makes up about heterogeneity in super-peer's'service rate,' reflecting their altruism, and query loads over the network. To the very best of our understanding, this is actually the first try to rigorously take into account such heterogeneity in devising searching mechanism for P2P systems. It is dependent on classifying queries into classes. This classification works as a kind of name aggregation, which helps nodes to infer the likelihoods of resolving class queries, which, consequently, are utilized in finding out how to forward queries. Our approach is fully distributed for the reason that it calls for information discussing only among neighbors, and achieves stability susceptible to a Grade and services information constraint on query resolution. The GoS constraint matches guaranteeing that every query class follows a route that it features a reasonable 'chance' to be resolved. We offer and evaluate several interesting variations on the stable mechanism which help considerably enhance the delay performance, and additional lessen the complexity which makes it amenable to implementation [5]. Benefits of suggested system: Estimating Query Resolution Odds

Alternate Grades and services information Strategies It is dependent on classifying queries into classes The GoS constraint matches guaranteeing that every query class follows a route that, it features a reasonable 'chance' to be resolved which provides abases for substantially reducing complexity by approximations.

Query Forwarding Strategy: Queries are forwarded in the finish from the slot. Observe that included in this are policies in which the condition deterministically determines the query-type to become serviced and also the forwarding strategy each and every node. We'll propose a question scheduling and forwarding policy that ensures the GoS for every class, is shipped, simple to apply, and it is stable. Subordinate peers may initiate a question request in a super peer, but don't take part in forwarding or query resolution. A typical mechanism adopted in P2P systems would be to evict a question in the network if it's unresolved after getting traversed some fixed quantity of nodes. For the purposes we model this kind of exit strategy directly by itself [6]. The chance a node can resolve this type of query depends not just on its class but additionally its history, i.e., the group of nodes it visited previously. Note, history captures just the group of visited nodes and never an order that they are visited. We think that time is slotted, and every super-peer comes with a connected service rate, akin to positive integer quantity of queries it's prepared to resolve/forward in every slot. The network is stable if each queue is stable. Next we define the 'capacity region' for query loads on the network. They are diverse from the conventional multi commodity flow conservation laws and regulations meaning our conservation equations are made to capture the next aspects arising in P2P search systems: (a) history dependent possibility of query resolution each and every node, (b) updates in 'types' of queries because they get given to different nodes, (c) computing the caliber of service received by query via its background and designing a suitable exit strategy upon receiving enough service. However, this type of centralized policy might not be practically achievable, furthermore arrival rates might not be known a priori. Further, designing a reliable search formula has become challenging since, as the routing decisions should be according to immediate queue loads in the neighbors, the choices themselves modify the type/queue that a question belongs. Also, while our focus, for the time being, is on policies where matches the conditional odds of query class resolutions, susceptible to the GoS modification, other modifications might be made. The fundamental backpressure formula, though stable, is extremely inefficient. Inside a slot, each node serves just the queue with greatest relative backlog. In situation that specific queue has under queries browsing it, the spare services are supplied to blank queries, whether or not the other queues are non-empty. We currently devise a far more efficient protocol that serves blank queries only if all of the queues are non-empty and it is thus work-conserving and it is stable too. The concept is, if the amount of queries within the queue with greatest relative backlog is under total service rate, the job conserving policy serves the queries in second greatest backlogged queue, and so forth, until either total of queries are offered or all of the queues are empty. Since, inside a fully connected network, allowing queries to revisit nodes provides no advantages, queries are given to only individual's nodes which aren't formerly visited. To date we've assumed that resolution odds for queries of various types are known. We advise simple modification and approximations that significantly lessen the overheads, although with a few penalty within the performance [7]. Used they may be easily believed. To guarantee impartial estimates could be acquired each and every node, suppose a part of your concerns is marked 'RW', forwarded through the random walk policy having a large TTL, and given scheduling priority over other queries.

4. CONCLUSION:

The important thing idea would be to define equivalence classes of query types that share a 'similar' history, meaning they have similar conditional odds of resolution, and also have them share a queue. Within the baseline random walk policy, upon service, each node forwards an unresolved query to among the neighbors selected uniformly randomly. In summary, we provided a singular, distributed, and reliable search insurance policy for unstructured peer-to-peer systems with super-peers. Our backpressure based policy can offer capacity gains of as large over traditional random walk techniques. Reducing complexity Estimating parameters, and adaptation to class-based query resolution odds and traffic loads are studied Stable Policies Also, while our focus, for the time being, is on policies where matches the conditional odds of query class resolutions, susceptible to the GoS modification, other modifications might be made. We provided modifications towards the formula making it amenable to implementation.

REFERENCES:

[1] Virag Shah, Gustavo de Veciana, Fellow, IEEE, and George Kesidis, "A Stable Approach for Routing Queries inUnstructured P2P Networks", ieee/acm transactions on networking, 2016.

[2] D. Menasche, L. Massoulie, and D. Towsley, "Reciprocity and barter in peer-to-peer systems," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[3] C. Gkantsidis, M. Mihail, and A. Saberi, "Hybrid search schemes for unstructured peer to peer networks," in Proc. IEEE INFOCOM, 2005, pp. 1526–1537.

[4] M. J. Neely, E. Modiano, and C. E. Rohrs, "Dynamic power allocation and routing for time varying wireless networks," in Proc. IEEE INFOCOM, 2003, pp. 745–755.

[5] M. Alresaini, M. Sathiamoorthy, B. Krishnamachari, and M. Neely, "Backpressure with adaptive redundancy (BWAR)," in Proc. IEEE INFOCOM, Mar. 2012, pp. 2300–2308.

[6] L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks," IEEE Trans. Autom. Control, vol. 37, no. 12, pp. 1936–1948, Dec. 1992.

[7] Y. Cui, E. Yeh, and R. Liu, "Enhancing the delay performance of dynamic backpressure algorithms," IEEE/ACM Trans. Netw., 2015, to be published.

DESIGNING A SECURE AND INFORMATIVE DETERRENT-DEPENDENT FOR FINDINGS

N Suneeta[1]., B Anusha[2]., B Prasanna[3]., K Thanu Sree [4]., K Jyothi[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- sunitha_netala@yahoo.co.in)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0506, 17RG1A0509, 17RG1A0531, 17RG1A0532),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

Within this paper, we think about a tougher model, where multiple data proprietors are participating, and also the cloud server would most likely behave dishonestly. There are several researches that concentrate on search engine results Verification. However, data file encryption becomes a hurdle to the effective use of traditional applications. Within this paper, we adopt this rated and privacy preserving keyword search plan to come back the very best-k search engine results. Within this paper, we explore the issue of verification for that secure rated keyword search, underneath the model where cloud servers would most likely behave dishonestly. Our goal would be to systematically construct schemes that may verify if they came back top-k search engine results are correct. Without effort, law enforcement chief can gather all of the policemen to ensure if the suspect commits a criminal offense. This plan are affected some delay, but it'll strengthen the deterrent around the cloud server. Within this paper, we adopt this rated and privacy preserving keyword search plan to come back the very best-k search engine results. Within this paper, we explore the issue of verification for that secure rated keyword search, underneath the model where cloud servers would most likely behave dishonestly. However, when the data users uncover the dishonest behavior, the cloud server ought to be seriously penalized. The deterrent within our plan comes from a number of constructions, including embedding secret sampling data and anchor data within the verification data buffer, forcing the cloud conduct blind computations on ciphertext, updating the verification data dynamically, and so forth. All of the cloud server knows is the fact that, once he behaves dishonestly, he'd be found with a good venture, and punished seriously once discovered.

Keywords: Dishonest cloud server, data verification, deterrent, top-k search.

1. INTRODUCTION:

All of the cloud server knows is the fact that, once he behaves dishonestly, he'd be found with a good venture, and punished seriously once discovered. Existing schemes share a typical assumption, i.e., data proprietors anticipate an order of search engine results. However, in practical applications, numerous data proprietors are participating each data owner only knows its very own partial order [1]. We advise to optimize the need for parameters utilized in the making of verification data buffer. Approved data users can issue queries not understanding secret keys of those data proprietors. Then an Additive Order Preserving Function household is suggested, which helps different data proprietors to encode their relevance scores with various secret keys, helping cloud server return the very best-k relevant search engine results to data users without revealing any sensitive information [2]. The suggested plan should avoid the cloud server from understanding the actual worth of the key verification data, and which data owners' data are came back as verification data. Xu et al. suggested a multi-keyword rated query plan on encrypted data, which helps an engaged keyword dictionary and avoids the issue where the rank order is perturbed by a number of high frequency keywords [3]. Within our previous work, we suggested a safe and secure rated multi-keyword search plan to aid multiple data proprietors. However, these techniques cannot be relevant to verify the very best-k rated search engine results in cloud-computing where multiple data proprietors are participating. Each one of these schemes thinks that the cloud server is "curious but honest". The linked signature chaining schemes, assume all original data are purchased, then your data owner signs for consecutive data products. Data proprietors first rank all data products, then put the purchased data products within the leaf node further, they create a Merkle hash tree

in the leaf node recursively until they obtain a root node.

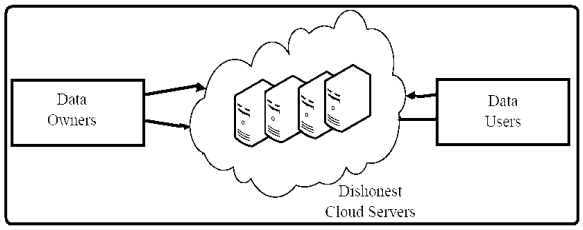


Fig.1.System architecture

2. DETERRENT SCHEME:

The suggested plan should allow data proprietors to create the verification data efficiently. The cloud server also needs to return the verification data without presenting heavy costs. Along the way, law enforcement chief helps to ensure that the suspect doesn't know which policemen know his action, and which policemen are asked through the police chief [4]. For any given keyword, each data owner only knows its very own partial order. However, these techniques cannot be relevant to verify the very best-k rated search engine results within the cloud-computing atmosphere, where numerous data proprietors are participating. The information user is capable of this goal simply by setting an ID group of his preferred data proprietors. Not the same as previous data verification schemes, we advise a singular deterrent-based plan. With this carefully devised verification data, the cloud server cannot know which data proprietors, or the number of data proprietors exchange anchor data which is employed for verifying the cloud server's misbehavior [5]. Regrettably, in practical applications, the cloud server might be compromised and behave dishonestly. Clearly, data collision may cause data to become unrecoverable. Therefore, the quantity of retrieved data will decrease whenever we map a lot of data products in to the verification data buffer. With this systematically designed verification construction, the cloud server cannot know which data owners' data take root within the verification data buffer, or the number of data owners' verification data are really employed for verification. In addition, our suggested plan enables the information users to manage the communication cost for that verification based on their preferences that is particularly important for that resource limited data users. We think that the information proprietors and approved data users share a secret hash function, e.g., the keyed-Hash Message Authentication Code. The approved data user decrypts his search engine results. When the data user finds any suspicious data, he'll construct and submit a secret verification request. You will find three other ways to avoid the cloud from knowing which verification data are really retrieved through the data user. To avoid the information user from recovering the verification data and discovering misbehavior, the cloud server would contaminate the records within the verification buffer set, and trick that collision occurs in these records. The verification is performed in 2 steps. Once an approved data user wants to carry out a rated secure keyword search of these encrypted files, he first generates his trapdoor and submits it with variable k towards the cloud server [6].

3. VERSATILE RESOURCE MANAGEMENT:

Cloud-computing provides tremendous benefits including quick access, decreased costs, quick deployment, and versatile resource management. File encryption on sensitive data before outsourcing is another way to preserve data privacy against adversaries. We advise a singular safe and effective deterrent based verification plan for secure rated keyword search. Within our system, multiple data proprietors are participating. For any given keyword, each data owner only knows its very own partial order. Within this paper, we adopt this rated and privacy preserving keyword search plan to come back the very best-k search engine results. Within this paper, we explore the issue of verification for that secure rated keyword search, underneath the model where cloud servers would most likely behave dishonestly. However, these

techniques cannot be relevant to verify the very best-k rated search engine results within the cloud-computing atmosphere, where numerous data proprietors are participating. The information user is capable of this goal simply by setting an ID group of his preferred data proprietors. However, the ID set shouldn't be uncovered towards the cloud server.

4. CONCLUSION:

The computational cost for that data proprietors allocated to verification mainly originates from constructing the verification data. Our suggested plan shouldn't only ensure a powerful deterrent for potential attacks, but additionally achieve high recognition probability when the compromised cloud server misbehaves. The suggested plan should deter the cloud server from behaving dishonestly. When the cloud server behaves dishonestly, the plan should identify it with a good venture. Furthermore, when any suspicious action is detected, data proprietors can dynamically update the verification data stored around the cloud server. In addition, we advise to optimize the need for parameters utilized in the making of the key verification data buffer.

REFERENCES:

[1] H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relational query results in data publishing," in Proceedings of the 2005 ACM SIGMOD international conference on Management of data. ACM, 2005, pp. 407–418.

[2] Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios, "Authenticated indexing for outsourced spatial databases," The VLDB JournalíThe International Journal on Very Large Data Bases, vol. 18, no. 3, pp. 631–648, 2009.

[3] M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in Proc. IEEE 31th International Conference on Distributed Computing Systems (ICDCS'11), Minneapolis, MN, Jun. 2011, pp. 383–392.

[4] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. IEEE ASIACCS'13, Hangzhou, China, May 2013, pp. 71–81.

[5] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained ownerenforced search authorization in the cloud," in Proc. IEEE INFOCOM' 14, Toronto, Canada, May 2014, pp. 226–234.

[6] B. Hore, E. C. Chang, M. H. Diallo, and S. Mehrotra, "Indexing encrypted documents for supporting efficient keyword search," in Proc. Secure Data Management (SDM'12), Istanbul, Turkey, Aug. 2012, pp. 93–110.

DOCUMENT HUNT BASED ON LEAST RELEVANCE THRESHOLD AGAINST INCREASE IN SIZE

P Swetha Nagasri[1]., M Gayathri[2]., P Swapna[3]., P Sony[4]., P Rajeshwari[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- pswetha369@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0539, 17RG1A0543, 17RG1A0544, 17RG1A0545),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Within this paper, a hierarchical clustering technique is suggested to aid more search semantics also to satisfy the interest in fast cipher text search inside a big data atmosphere. Additionally, we evaluate looking efficiency and security under two popular threat models. One challenge would be that the relationship between documents is going to be normally hidden while file encryption, which can result in significant search precision performance degradation. Also the level of data in data centers has possessed a dramatic growth. This makes it much more difficult to design cipher text search schemes that may provide efficient and reliable online information retrieval on large amount of encrypted data. An experimental platform should assess the search efficiency, precision, and rank security. The experiment result proves the suggested architecture not just correctly solves the multi-keyword rated search problem, brings a noticeable difference searching efficiency, rank security, and also the relevance between retrieved documents. Within the search phase, this method can achieve a straight line computational complexity against an exponential size increase of document collection. Because of the insufficient rank mechanism, users need to take a lengthy time for you to select what they need when massive documents retain the query keyword. Thus, order-preserving techniques are employed to realize the rank mechanism, To be able to verify the authenticity of search engine results, a structure known as minimum hash sub-tree was created within this paper. In addition, the suggested method comes with an edge on the standard method within the rank privacy and relevance of retrieved documents.***

Keywords: rank security, multi-keyword search, hierarchical clustering, cipher text, rank privacy.

1. INTRODUCTION:

Within this paper, a vector space model can be used and each document is symbolized with a vector, meaning every document is visible like a reason for a higher dimensional space. Cloud data proprietors choose to delegate documents within an encrypted form with regards to privacy preserving. Therefore it is important to develop efficient and reliable cipher text search techniques. The connection between documents represents the qualities from the documents and therefore maintaining the connection is essential to completely express a document [1]. Because of the blind file encryption, this important property continues to be hidden within the conventional methods. Therefore, proposing a technique which could maintain and apply this relationship to hurry looking phase is desirable. However, because of software/hardware failure, and storage corruption, data search engine results coming back towards the users could have broken data and have been distorted through the malicious administrator or burglar. Cloud server will first search the groups and obtain the minimum preferred sub-category. Then your cloud server will choose the preferred k documents in the minimum preferred sub-category. To ensure the integrity from the Google listing, a verifiable structure according to hash function is built. An online root is built to represent all of the data and groups. The virtual root is denoted through the hash consequence of the concatenation of all of the groups found in the first level. The virtual root is going to be signed that it is verifiable. The suggested hierarchical approach clusters the documents in line with the minimum relevance threshold, after which partitions the resulting clusters into sub-clusters before the constraint around the maximum size cluster is arrived at.

2. SYSTEM MODEL:

Because of the blind file encryption, this important property continues to be hidden within the conventional methods. Therefore, proposing a technique which could maintain and apply this relationship to hurry looking phase is desirable. Sun et al. use Merkle hash tree and cryptographic signature to produce a verifiable MDB-tree. Within the past few years, scientific study has suggested many cipher text search schemes by the cryptography techniques [2]. Additionally, the connection between documents is hidden within the above methods. The connection between documents represents the qualities from the documents and therefore maintaining the connection is

essential to completely express a document. For instance, the connection may be used to express its category. If your document is separate from every other document except individual's documents that are based on sports, then it's simple for us to say this document is one of the groups of the sports. However, the work they do can't be directly utilized in our architecture that is oriented for privacy-preserving multiple keyword searches. Disadvantages of existing system: Existing methods have been verified with provable security, however their methods need massive operations and also have about time complexity [3]. Therefore, former methods aren't appropriate for that big data scenario where data volume is extremely big and applications require online information systems. Song et al. method includes a high searching cost because of the checking from the whole data collection word by word. Sun et al. provide a new architecture which achieves better search efficiency. However, in the stage of index building process, the relevance between documents is overlooked. Thus, an effective mechanism you can use to ensure looking results within big data scenario is important to both CSPs and finish users.

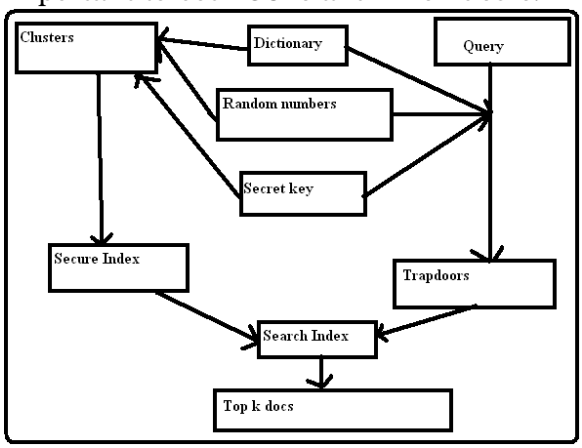


Fig.1.Enhanced system

3. ENHANCED IMPLEMENTATION:

Within the suggested architecture, looking the years has a straight line growth associated by having an exponential growing size data collection. We derive this concept in the observation that users retrieval needs usually focus on a particular field. Within this paper, a vector space model can be used and each document is symbolized with a vector, meaning every document is visible like a reason for a higher dimensional space. Because of the relationship between different documents, all of the documents could be split into several groups. Rather of utilizing the standard sequence search method, a backtracking formula is created to look the prospective documents. Cloud server will first search the groups and obtain the minimum preferred sub-category. Then your cloud server will choose the preferred k documents in the minimum preferred sub-category. The need for k is formerly made the decision through the user and delivered to the cloud server. If current sub-category can't fulfill the k documents, cloud server will trace to its parent and choose the preferred documents from the brother groups [4]. This method is going to be performed recursively before the preferred k documents are satisfied or even the root is arrived at. To ensure the integrity from the Google listing, a verifiable structure according to hash function is built. Benefits of suggested system: Looking time could be largely reduced by choosing the preferred category and abandoning the irrelevant groups. The virtual root is denoted through the hash consequence of the concatenation of all of the groups found in the first level. The virtual root is going to be signed that it is verifiable. To ensure looking result, user only must verify the virtual root, rather of verifying every document.

Contributed methods: We advise a hierarchical method to get a much better clustering result within a lot of data collection. How big each cluster is controlled like a trade-off between clustering precision and query efficiency. The relevance score is really a metric accustomed to assess the relationship between different documents. Because of the new documents put into a cluster, the constraint around the cluster might be damaged. Within the search phase, the cloud server will first compute the relevance score between query and cluster centers from the first level after which chooses the closest cluster. This method is going to be iterated to obtain the nearest child cluster before the tiniest cluster has been discovered. Every document is going to be hashed and also the

hash result will be utilized for the associated with the document. An online root is added and symbolized through the hash consequence of the concatenation from the groups found in the first level.

System Framework: The machine model contains three entities, the information owner, the information user, and also the cloud server. Within this model, both data owner and also the data user are reliable, as the cloud server is semi-reliable, that is in conjunction with the architecture. Retrieval precision relates to two factors: the relevance between your query and also the documents in result set. Trapdoor unlink ability implies that each trapdoor produced by the totally different, even for the similar query. Data privacy is definitely the confidentiality and privacy of documents [5]. The foe cannot obtain the plaintext of documents stored around the cloud server if data privacy is guaranteed. The cloud server supplies a huge space for storage, and also the computation sources required by cipher text search. The vector space model adopted through the MRSE-HCI plan is just like the MRSE, while the entire process of building index is completely different. The hierarchical index structure is introduced in to the MRSE-HCI rather of sequence index. Within this, every document is listed in a vector.

MRSE-HCI Architecture: The architecture shows, how the data owner builds the encrypted index with respect to the dictionary, random figures and secret key, the information user submits a question towards the cloud server to get preferred documents, and also the cloud server returns the prospective documents towards the data user. The key k is generated through the data owner selecting an n-bit pseudo sequence. Then data owner uses the dictionary Dew to change documents to an accumulation of document vectors DV. The information owner adopts a safe and secure symmetric file encryption formula. The information user transmits the query towards the data owner who'll later evaluate the query. For each document within the matched cluster, the cloud server extracts its corresponding encrypted document vector. The relevance method, can be used to evaluate the relevance of document-query and document-document. It's also accustomed to evaluate the relevance from the query and cluster centers. The suggested dynamic K-means formula, the minimum relevance threshold from the clusters is determined to help keep the cluster compact and dense [6]. When the relevance score from a document and it is center is smaller sized compared to threshold, a brand new cluster center is added and all sorts of documents are reassigned. Both of these bigger clusters are portrayed through the elliptical shape. Then both of these clusters are checked to determine whether their points fulfill the distance constraint. The cloud server computes the relevance score. The cloud server will get the kid cluster centers from the cluster center, then computes the relevance score. Verifying the authenticity of search engine results is proving itself to be a vital trouble in the cloud atmosphere. The hash worth of tree root node is dependent on the hash values of clusters within the first level. It's important to note the root node denotes the information set containing all clusters. Then your data owner generates the signature from the hash values from the root node and outsources the hash tree such as the root signature towards the cloud server [7]. The minimum hash sub-tree includes the hash values of leaf nodes within the matched cluster and non-leaf node akin to all cluster centers used to obtain the matched cluster within the searching phase. Finally, the information user uses the trapdoor to re-search the index built by part one of retrieved nodes. The information owner transmits the trapdoor generated through the document vector encrypted document and encrypted document vector towards the cloud sever. The cloud sever finds the nearest cluster, and puts the encrypted document and encrypted document vector in it. The fundamental information of documents and queries are inevitably leaked towards the honest-but-curious server since all of the data are stored in the server and also the queries posted towards the server. Eventually, all of the document vectors and cluster center vectors are encrypted through the secure KNN.

4. CONCLUSION:

Evaluating with the documents within the dataset, the amount of documents which user is aimed at is extremely small. Because of the few the preferred documents, a particular category could be further split into several sub-groups. An online root is built to represent all of the data and groups. We propose the MRSE-HCI architecture to adjust to the needs of information explosion, online information retrieval and semantic search. Simultaneously, a verifiable mechanism can also be suggested to be sure the correctness and completeness of search engine results. Within this paper, we investigated cipher text search within the scenario of cloud storage. We explore the issue of maintaining the semantic relationship between different plain documents within the related encrypted documents and provide the look approach to boost the performance from the semantic search. Experiments happen to be conducted while using collection set constructed from the IEEE Xplore. The outcomes reveal that having a sharp increase of documents within the dataset looking duration of the suggested method increases linearly whereas looking duration of the standard method increases tremendously.

REFERENCES:

[1] Chi Chen, Member, IEEE, Xiaojie Zhu, Student Member, IEEE, Peisong Shen, Student Member, IEEE,Jiankun Hu, Member, IEEE, Song Guo, Senior Member,IEEE, Zahir Tari, Senior Member, IEEE, andAlbert Y. Zomaya, Fellow, IEEE, "An Efficient Privacy-Preserving RankedKeyword Search Method", ieee transactions on parallel and distributed systems, vol. 27, no. 4, april 2016.

[2] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Proc. 27th Annu. Int. Cryptol. Conf. Adv. Cryptol., Santa Barbara, CA, 2007, pp. 535–552.

[3] C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst., Genova, ITALY, 2010, pp. 253–262.

[4] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for Boolean que-ries," in Proc. Adv. Cryptol,. Berlin, Heidelberg, 2013, pp. 353–373.

[5] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. 8th ACM SIGSAC Symp. Inform., Comput. Commun. Security, Hangzhou, China, 2013, pp. 71–82.

[6] I. H. Witten, A. Moffat, and T. C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images, 2nd ed. San Francisco, CA, USA : Morgan Kaufmann, 1999.

[7] C. M. Ralph, "Protocols for public key cryptosystems," in Proc. IEEE Symp. Security Priv, Oakland, CA, 1980, pp. 122–122.

CONSIDERING INSIGNIFICANT DIVISION OF I/O REQUEST PREVENTING OVERHEADS

K Sheetal[1]., CH Sai Deepika[2]., K Mounika[3]., P Urmila[4]., Shifa Sadequa[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- sheetalkulkarni.925@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0512, 17RG1A0533, 17RG1A0542, 17RG1A0551),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***POD is definitely an ongoing research study and we're presently exploring several directions for future year's research. a performance-oriented deduplication plan, to enhance the performance of primary storage systems within the Cloud by leveraging data deduplication around the I/O road to remove redundant write demands whilst saving space for storage. The explanation would be that the small I/O demands only take into account a small fraction from the storage capacity requirement, making deduplication in its unprofitable and potentially counterproductive thinking about the substantial deduplication overhead involved. The prototype from the POD plan is implemented being an embedded module in the block-device level along with a sub file deduplication approach can be used. However, our experimental studies claim that directly applying data deduplication to primary storage systems will probably cause space contention within the primary memory and knowledge fragmentation on disks. Select-Dedupe take the workload characteristics of small-I/O-request domination in to the design factors. It deduplicates all of the write demands if their write information is already stored sequentially on disks, such as the small write demands that will well be bypassed from through the capacity-oriented deduplication schemes. The index-lookup process then tries to obtain the redundant data chunks in the fingerprint index table based on the hash values. Whenever a redundant data chunk is located, it's substituted for a pointer within the metadata. Just the unique data chunks are written towards the disks. To prevent the negative read-performance impact from the deduplication-caused read amplification problem, POD is made to judiciously and selectively, rather of blindly, deduplicates write data and effectively make use of the storage cache. POD has two primary components: Select-Dedupe and iCache. Within our design, if your read ask that hits the Map table is split up into multiple small read demands through the Request Redirector module, Select-Dedupe will reorganize these data chunks for their original consecutive positions increase the Map table throughout the system idle time. Within this paper, we compare POD using the Hard disk drive-based storage systems without data deduplication with traditional full data deduplication, and also the capacity oriented plan iDedup.***

Keywords: Deduplication, I/O Deduplication, Data Redundancy, Primary Storage, I/O Performance, Storage Capacity

1. INTRODUCTION:

For that redundant write data, just the write data addressed to various locations may lead to capacity savings. Consequently, the majority of the hash index records should be stored on disks, in which the in-disk index-lookup operations may become a serious performance bottleneck in deduplication-based storage systems [1]. Since index cache is essential in increasing the write performance and browse cache is crucial for that read performance, the I/O burrstones characteristic will probably render ineffective the fixed cache partition between your read cache and also the index cache. As the latter signifies the information redundancy targeted by capacity-oriented deduplication schemes, it's the mixture of the previous and also the latter that signifies the I/O redundancy. POD is made to support the desirable the best-selling write-traffic-reducing ability of information deduplication while effectively addressing the deduplication-caused problems. POD increases the I/O performance of primary storage systems by focusing more about small me /Os and files while retaining the capability savings [2]. The iCache module includes two individual modules: Access Monitor and Swap Module. The Access Monitor module accounts for monitoring the intensity striking rate from the incoming read demands. In Select-Dedupe, write demands with redundant data has sorted out into three groups. The 2 functional components in iCache, the Access Monitor and also the Swap Module, interact to complete the iCache functions. The Access Monitor in iCache determines which cache, index cache or read cache, ought to be elevated in dimensions based on the current access pattern. The functional quantity of reduced write demands in Select-Dedupe greatly shortens the size of the disk I/O queue and

relieves its pressure, thus allowing the read demands to become serviced more rapidly.

2. CLASSICAL METHOD:

The present data deduplication schemes for primary storage, for example iDedup and Offline-Dedupe, are capacity oriented for the reason that they concentrate on storage capacity savings and just choose the large demands to deduplicates and bypass all of the small demands. The explanation would be that the small I/O demands only take into account a small fraction from the storage capacity requirement, making deduplication in its unprofitable and potentially counterproductive thinking about the substantial deduplication overhead involved. However, previous workload research has says small files dominate in primary storage systems (greater than 50 %) and therefore are at the bottom from the system performance bottleneck. In addition, because of the buffer effect, primary storage workloads exhibit apparent I/O burrstones [3]. Disadvantages of Existing System: From the performance perspective, the present data deduplication schemes neglect to think about these workload characteristics in primary storage systems, missing the chance to deal with probably the most important issues in primary storage, those of performance. Our experimental studies claim that directly applying data deduplication to primary storage systems will probably cause space contention within the primary memory and knowledge fragmentation on disks. This really is partly because data deduplication introduces significant index-memory overhead towards the existing system as well as in part just because a file or block is split up into multiple small data chunks which are frequently situated in non-consecutive locations on disks after deduplication. This fragmentation of information may cause a subsequent read request to invoke many, frequently random, disk I/O operations, resulting in performance degradation.

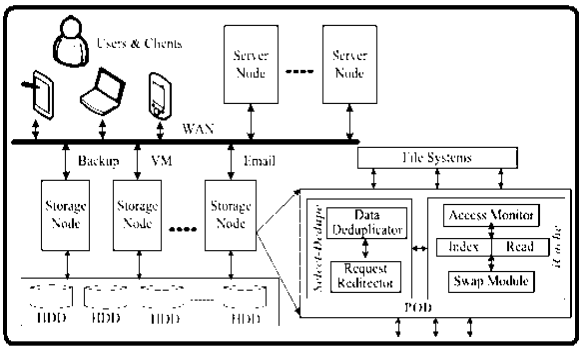


Fig.1.Proposed System architecture

3. REAL-TIME DEDUPLICATION:

To deal with the key performance issue of primary storage within the Cloud, and also the above deduplication-caused problems, we advise a Performance-Oriented data Deduplication plan, known as POD, as opposed to a capacity-oriented one, to enhance the I/O performance of primary storage systems within the Cloud by thinking about the workload characteristics. POD requires a two-pronged method of increasing the performance of primary storage systems and minimizing performance overhead of deduplication, namely, a request-based selective deduplication technique, known as Select-Dedupe, to relieve the data fragmentation as well as an adaptive memory management plan, known as iCache, to alleviate the memory contention between your burst read traffic and also the burst write traffic [4]. Benefits of Suggested System: POD considerably increases the performance and saves capacity of primary storage systems within the Cloud. The present data deduplication schemes for primary storage, for example iDedup and Offline-Dedupe, are capacity oriented for the reason that they concentrate on storage capacity savings and just choose the large demands to deduplicates and bypass all of the small demands [5]. Our experimental research shows that data redundancy exhibits a significantly greater intensity level around the I/O path than that on disks because of relatively high temporal access locality connected with small I/O demands to redundant data. To look at the internet aftereffect of the POD plan, within our trace-driven evaluation we make use of the

block level traces which were collected underneath the memory buffer cache so the caching/buffering aftereffect of the storage stack has already been fully taken through the traces. In primary storage data sets, small files are the most typical quality and as much as 62% files are smaller sized than 4KB. Capacity-oriented deduplication systems, for example iDedup, don't deduplicate the little I/O demands because reduplicating them contributes little towards the overall capacity savings. By calculating and evaluating the hash values from the incoming small write data, POD is made to identify and take away a lot of redundant write data, thus effectively filtering out small write demands and improving I/O performance of primary storage systems within the Cloud. To be able to lessen the storage and processing overhead needed to keep and query the large hash index table, POD only stores the new hash index records in memory [6]. The Count variable can also be accustomed to avoid the referenced data blocks from being modified or deleted. The style of iCache is dependent on the explanation the I/O workload of primary storage changes frequently with mixed read burrstones. The exchanged index data and browse data are stored on the reserved space around the back-finish hard drive. Within this experiment, iDedup and choose-Dedupe make use of the fixed cache partition between your index cache and browse cache while POD uses the dynamic cache partition.

4. CONCLUSION:

Recent Worldwide Data Corporation (IDC) reports say that in past 5 years the level of data has elevated by almost 9 occasions to 7ZB each year along with a greater than 44-fold growth to 35ZB is anticipated within the next 10 years. POD requires a two-pronged method of increasing the performance of primary storage systems and minimizing performance overhead of deduplication, namely, a request-based selective deduplication technique, known as Select-Dedupe, to relieve the data fragmentation as well as an adaptive memory management plan, known as iCache, to alleviate the memory contention between your burst read traffic and also the burst write traffic. To deal with the key performance issue of primary storage within the Cloud, and also the above deduplication-caused problems, we advise a Performance-Oriented data Deduplication plan, known as POD, as opposed to a capacity-oriented one, to enhance the I/O performance of primary storage systems within the Cloud by thinking about the workload characteristics. POD can be simply integrated into any Hard disk drive-based primary storage systems to accelerate their system performance. Furthermore, POD is in addition to the upper file systems, making POD more flexible and portable than whole-file deduplication and iDedup. Data consistency in POD necessitates that the referenced data be reliably stored on disks and also the key data structures 't be lost in situation of the power failure. We've implemented a prototype of POD like a module within the Linux operating-system and employ the trace-driven experiments to judge its usefulness and efficiency.

REFERENCES:

[1] M. Fu, D. Feng, Y. Hua, X. He, Z. Chen, W. Xia, F. Huang, and Q. Liu. Accelerating Restore and Garbage Collection in Deduplication-based Backup Systems via Exploiting Historical Information. In USENIX'14, Jun. 2014.

[2] J. Lofstead, M. Polte, G. Gibson, S. Klasky, K. Schwan, R. Oldfield, M. Wolf, and Q. Liu. Six Degrees of Scientific Data: Reading Patterns for Extreme Scale Science IO. In HPDC'11, Jun. 2011.

[3] C. Zhang, X. Yu, A. Krishnamurthy, and Randolph Y. Wang. Configuring and Scheduling an Eager-Writing Disk Array for a Transaction Processing Workload. In FAST'02, Jan. 2002.

[4] F. Chen, T. Luo, and X. Zhang. CAFTL: A Content-Aware Flash Translation Layer Enhancing the Lifespan of Flash Memory based Solid State Drives. In FAST'11, pages 77–90, Feb. 2011.

[5] E. Rozier and W. Sanders. A Framework for Efficient Evaluation of the Fault Tolerance of

Deduplicated Storage Systems. In DSN'12, Jun. 2012.
[6] Y. Hua and X. Liu. Scheduling Heterogeneous Flows with Delay-aware Deduplication for Avionics Applications. IEEE Transactions on Parallel and Distributed Systems, 23(9):1790–1802, 2012.

TRUSTED BROKERAGE SYSTEM WITH EXPANDED CAPABILITIES

CH V Krishna Mohan[1]., G Archana[2]., G Swathi[3]., S Noshitha Reddy[4]., S Supriya[5]
1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- chvkm@rediffmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0516, 17RG1A0517, 17RG1A0548, 17RG1A0549),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Within this work, we advise innovative authenticated index structures and verification protocols to permit clients to ensure the completeness and authenticity of brokers' solutions. To be able to overcome the constraints of existing techniques, both when it comes to efficiency and supported functionality, we advise a brand new authenticated index structure. Within the CSSV plan, we introduce yet another entity, the collector, besides CSPs, cloud clients and cloud brokers. The collector functions just like a certificate authority and it is assumed fully reliable, that is inline using the recent work. Our novel index structure may be the core element of our Cloud Service Selection Verification (CSSV) plan, which employs the thought of "separation of duties" to make sure strong security guarantees. However, existing brokerage schemes on cloud service selection typically think that brokers are totally reliable, and don't provide any guarantee within the correctness from the service recommendations. Each cloud broker handles a potentially great deal of online client's demands. The number query formula is equivalent to that within the B -tree, which starts in the root and traverses lower the tree following pointers that could indicate the important thing values inside the query range. The fundamental approach using MB cloud-tree indexes just the Cost property, and for that reason has limited ability to cope with queries that don't include Cost among the selection criteria, or with queries which have a number of other selection criteria besides Cost. Our theoretical and experimental results demonstrate the success and efficiency in our schemes in contrast to the condition-of-the-art. Our suggested both schemes work because they build authenticated index for results verification. The VR-tree is extremely time intensive because of the have to compute and aggregate multiple signatures. The verification performance from the three plans is comparable to the service selection. We implemented our approaches while using Polaris cryptographic library: the hash utilized in algorithms used MD5, and also the collector's signature was recognized using RSA signing formula.***

Keywords: Cloud service selection, brokerage system, Merkle hash tree, verification

1. INTRODUCTION:

We advise a cutting-edge Cloud Service Selection Verification plan and index structures to allow cloud clients to identify misbehavior from the cloud brokers throughout the service buying process. The VRtree is nearly two orders of magnitude slower than both of our schemes. It is because the outcomes verification of VR-tree needs a minimum of two bilinear pairing operations and numerous modular multiplications. Lately, Quad et al. suggested a strategy for cloud service selection according to both user feedback and cloud performance. Modeling approach has additionally been useful for service selection. Our work also is associated with this category. In contrast to existing works which possess the Merkle B -tree because the base structure, our work surpasses them simply because they either don't support multidimensional queries. Aiming at evaluating the performance and abilities of services provided by CSPs for facilitating customers' selections, Binnig et al. developed a new benchmark to suit the options of cloud-computing. Lenk et al. further suggested a brand new performance calculating way of Infrastructure-as-Service choices. Within this paper, we presented a cutting-edge Cloud Service Selection Verification (CSSV) system to attain cheating-free cloud service selection within cloud brokerage architecture. To be able to unify the follow-up process, the query normalization adds the domains of other non-query qualities towards the query. To the very best of our understanding, existing creates cloud service selection are focused only regarding how to choose the services that satisfy customers' needs.

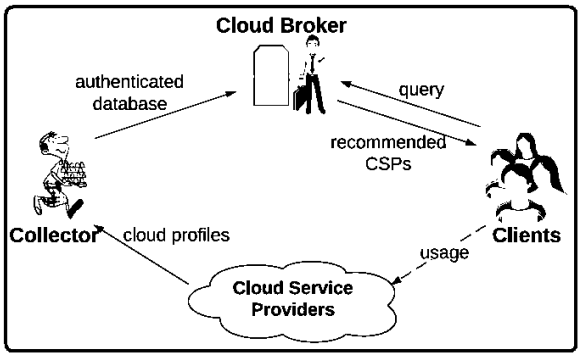


Fig.1.Proposed system framework

2. METHODOLOGY:

The collector is permitted to create gain selling the authenticated database to a number of cloud brokers. Using the available authenticated databases, the cloud brokers concentrate on handling most likely a lot of real-time service demands from clients. The Merkle hash tree includes a binary tree because the base structure. The leaf nodes within the Merkle hash tree retain the hash values from the original data products. Each internal node provides the hash worth of the concatenation from the hash values of their two children nodes. On the other hand, the VR-tree and MMBcloud-tree index all qualities of CSPs and therefore acquire a balanced performance when different the various parameters of queries. At query execution, the company picks the signatures from the data objects falling within the query range to create the proof messages. First, considering that most cloud providers use a pay-per-use business design, Cost is among the most generally happened criteria in cloud service selection queries. Second, because there are many possible values of Cost among CSPs, Cost is an extremely selective property making queries more effective. To specify CSPs' services that the clients can request to brokers, we consider ten common qualities of CSPs. Furthermore, each pointer within the internal node is connected with one hash value that's computed by concatenating the hash values of records in the child node. Our problem, i.e. verification of cloud brokers recommendations, is compounded by the possible lack of trustworthiness assumptions from the broker. To create the MBcloud-tree, the data of every CSP is placed in the same manner as that within the B -tree. A hash worth of the CSP is computed, and also the hash value will be accustomed to compute the hash values of their ancestor nodes completely to the root. Inside a cloud brokerage system, probably the most fundamental tasks would be to provide high-quality selection services for clients. That's, an agent provides clients with a summary of suggested CSPs that satisfy the clients' needs. Compute the space from a data point and it is nearest reference, and employ this distance along with a scaling value to create a catalog key with this data point. The VRtree is nearly two orders of magnitude slower than both of our schemes. It is because the outcomes verification of VR-tree needs a minimum of two bilinear pairing operations and numerous modular multiplications. To ensure authenticity of the CSP's profile, a naive option would be to want the CSP to sign its profile after which allow the client verify the signature. Signature-based approaches typically construct an authenticated and unforgivable chain within the data objects inside a specified order.

3. CLOUD SERVICES:

Cloud services provide a scalable number of spaces for storage and computing abilities that are broadly utilized by a growing quantity of business proprietors. Our novel index structure may be the core element of our Cloud Service Selection Verification (CSSV) plan, which employs the thought of "separation of duties" to make sure strong security guarantees. However, existing brokerage schemes on cloud service selection typically think that brokers are totally reliable, and don't provide any guarantee within the correctness from the service recommendations.

4. CONCLUSION:

The supply of numerous, possibly complex options, however, causes it to be hard for potential cloud clients to weigh and choose which options suit their needs the very best. On the other hand, the VR-tree and MMBcloud-tree index all qualities of CSPs and

therefore acquire a balanced performance when different the various parameters of queries. The greater CSPs, the greater insertion operations have to be conducted to construct the authenticated indices. Furthermore, both our methods outshine the VRtree by a couple of orders, since the VR-tree involves a lot of signatures for that CSPs in addition to partitions as a whole construction, while our methods just have lightweight hash operations.

REFERENCES:

[1] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in SIGMOD'06: Proceedings of the 2006 ACM SIGMOD international conference on Management of data. ACM Request Permissions, Jun. 2006.

[2] C. Yu, B. C. Ooi, K.-L. Tan, and H. V. Jagadish, "Indexing the distance: an efficient method to KNN processing," in Proceedings of the 27th International Conference on Very Large Data Bases. Morgan Kaufmann Publishers Inc., Sep. 2001, pp. 421–430.

[3] D. Papadopoulos, S. Papadopoulos, and N. Triandopoulos, "Taking authenticated range queries to arbitrary dimensions," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 819–830.

[4] E. Mykletun, M. Narasimha, and G. Tsudik, "Signature bouquets: immutability for aggregated/condensed signatures," in Computer Security – ESORICS 2004, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, vol. 3193, pp. 160–176.

[5] H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relational query results in data publishing," in Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data, 2005, pp. 407–418.

[6] C. Binnig, D. Kossmann, T. Kraska, and S. Loesing, "How is the weather tomorrow?: towards a benchmark for the cloud," in DBTest '09: Proceedings of the Second International Workshop on Testing Database Systems. ACM Request Permissions, Jun. 2009.

ENCRYPTED KEY-BASED INDEX SCHEME FOR REDUCED OUTLAY STATISTICS SUPERVISION

M Sujatha[1]., G Sukanya[2]., H Sneha Reddy[3]., P Rishitha[4]., R Kanthi Priya[5]
1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- sujathamantra@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0520, 17RG1A0521, 17RG1A0546, 17RG1A0547),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: Here, the machine searches Cloud Secure data quickly because the user types in query keywords. Many works were suggested in a variety of types of threat to achieve various functionalities for search for example single keyword search, multi-keyword rated search, and so forth. We submit a safe and secure search method which is dependent on the tree above encrypted cloud information, also it manages multi-keyword search in addition to dynamic process on assortment of documents. Due to important structure of tree-based index, forecasted search system will effectively get sub-straight line search some time and manage the entire process of deletion in addition to insertion of documents. The forecasted plan is recognized as to provide multi-keyword query in addition to precise result ranking, additionally dynamic update above document collections. For acquiring of high search effectiveness, we develop a tree-based index structure and propose a formula based on the index tree. Even if this concept is certainly not new for RDBMS based systems, this can be a new information-access paradigm for Encrypted Cloud Domains driven by user file discussing activities. Of these works, multi-keyword manner of rated search has gotten more importance because of its realistic applicability.

Keywords: Multi-keyword ranked search, Tree-based index, Sub-linear search, Encrypted cloud data, Documents, Result ranking..

1. INTRODUCTION:

Attracted through the features such of cloud-computing for example on-demand network access, least economic overhead and managing of enormous computing sources several organizations are enthused to delegate their information towards cloud services. Within the recent occasions several dynamic schemes were introduced for supporting insertion in addition to deletion operations on document collection [1]. Despite the fact that there are many advantages of cloud services, outsourcing of sensitive data in direction of secluded servers can make privacy issues. The most popular method which is often used for defense of information confidentiality is file encryption from the data sooner than the entire process of outsourcing however, this makes elevated cost concerning the usability of information. They are important works as it is achievable that data proprietors require updating of the info on cloud server however couple of active schemes will manage effective search procedure for multi keyword. Our work will submit a safe and secure search method which is dependent on the tree above encrypted cloud information, also it manages multi-keyword search in addition to dynamic process on assortment of documents. The types of vector space in addition to broadly used term frequency × inverse document frequency representation are pooled in index construction in addition to query generation of query for supplying the rated search procedure for multi-keyword. For acquiring of high search effectiveness, we develop a tree-based index structure and propose a formula based on the index tree [2]. The effective nearest neighbor formula can be used to secure index in addition to query vectors, and for the moment make certain calculation of accurate relevance score among encrypted index additionally to question vectors. Due to important structure of tree-based index, forecasted search system will effectively get sub-straight line search some time and manage the entire process of deletion in addition to insertion of documents.

2. EXISTING SYSTEM:

Existing techniques are keyword-based information retrieval that are broadly utilized on the plaintext data, can't be directly put on the encrypted data. Installing all of the data in the cloud and decrypt in your area is clearly impractical. To be able to address the above mentioned problem, scientific study has designed some general-purpose solutions with

fully-homomorphic file encryption or oblivious RAMs. However, these techniques aren't practical because of their high computational overhead for the cloud sever and user. On the other hand, better special-purpose solutions, for example searchable file encryption (SE) schemes make specific contributions when it comes to efficiency, functionality and security. Searchable file encryption schemes let the client to keep the encrypted data towards the cloud and execute keyword search over cipher text domain. Disadvantages: The cloud providers (CSPs) that keep your data for users may access user's sensitive information without authorization. Without secure the information, users directly upload the files in to the cloud means cannot applied the file encryption on data.

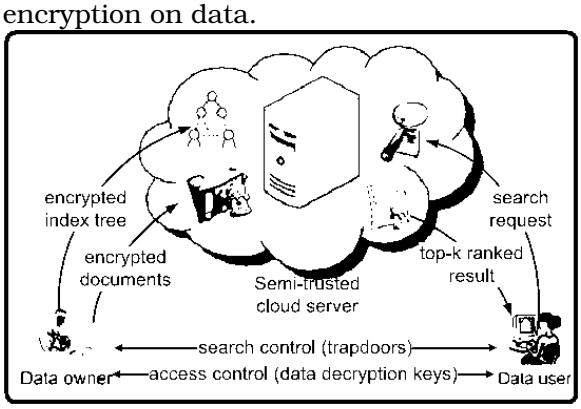


Fig.1.System architecture

3. PROPOSED SYSTEM:

This paper proposes a safe and secure tree-based search plan within the encrypted cloud data, which assists multi-keyword rated search and dynamic operation around the document collection. Particularly, the vector space model and also the broadly-used "term frequency (TF) inverse document frequency (IDF)" model are combined within the index construction and query generation to supply multi-keyword rated search. To be able to obtain high search efficiency, we create a tree-based index structure and propose a "Greedy Depth-first Search (GDFS)" formula according to this index tree. Because of the special structure in our tree-based index, the suggested search plan can flexibly achieve sub-straight line search some time and cope with the deletion and insertion of documents. The secure kNN formula is required to secure the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. To face up to different attacks in various threat models, we construct two secure search schemes: the fundamental dynamic multi-keyword rated search (BDMRS) plan within the known cipher text model, and also the enhanced dynamic multi-keyword rated search (EDMRS) plan within the known background model. Advantages: We design a searchable file encryption plan that supports both accurate multi-keyword rated search and versatile dynamic operation on document collection. The suggested plan is capable of greater search efficiency by executing our "Greedy Depth-first Search" formula.

Methodology: A great deal of scientific study has measured several solutions however these methods aren't realistic due to high computational overhead for cloud severs in addition to user. In comparison, more realistic solutions, for example the techniques of searchable file encryption have finished particular contributions concerning the competence, in addition to security. Numerous works were suggested to attain a number of functionalities for search for example single keyword search, multi-keyword rated search, and so forth and multi-keyword manner of rated search has gotten more importance because of its realistic applicability. The techniques of searchable file encryption will grant client to amass encrypted information towards cloud and bear out keyword search above cipher-text domain. A great deal of works were suggested in a variety of types of threat to achieve a number of search functionality which schemes will recover search engine results which are based on keyword existence. We offer a safe and secure search method which is dependent on the tree above encrypted cloud information, also it manages multi-keyword search in addition to dynamic process on assortment of documents. Because of important structure of tree-based index, forecasted search system will effectively

get sub-straight line search some time and manage the entire process of deletion in addition to insertion of documents [3]. The machine is recognized as to postpone cloud server from learning added specifics of document collection, index tree, in addition to query. Because of particular construction of tree-based index, search impossibility of suggested product is stored to logarithmic. And actually, suggested system can achieve advanced search competence additionally parallel search is flexibly transported to decrease time expenditure of search procedure. Types of vector space in addition to broadly used term frequency × inverse document frequency representation are pooled in index construction in addition to query generation of query for supplying the rated search procedure for multi-keyword [4]. For acquiring of high search effectiveness, we develop a tree-based index structure and propose a formula based on the index tree. To face up to record attacks, phantom terms are incorporated towards index vector meant for blinding the outcomes of search. The effective nearest neighbor formula can be used to secure index in addition to query vectors, and for the moment make certain calculation of accurate relevance score among encrypted index additionally to question vectors. Several works were suggested in a variety of types of threat to achieve a number of search functionality which schemes will recover search engine results which are based on keyword existence, which cannot offer acceptable result functionality. Searchable file encryption methods will grant clients to keep up encrypted information for the cloud and bear out keyword search above cipher-text domain. Due to various cryptographic primitives, searchable file encryption methods they fit up by way of public key otherwise symmetric key based cryptography. These works are particular keyword Boolean search techniques that are easy regarding functionality. Our work will advise a secure search method which is dependent on the tree above encrypted cloud information, also it manages multi-keyword search in addition to dynamic process on assortment of documents. Forecasted search system will effectively get sub-straight line search some time and manage the entire process of deletion in addition to insertion of documents. For acquiring of high search effectiveness, we develop a tree-based index structure and propose a formula based on the index tree. Vector space representation all together with term frequency × inverse document frequency representation is extensively used within plaintext information recovery that resourcefully manages rated procedure for multi-keyword search [5]. The authors have built searchable index tree based on vector space representation and implemented cosine measure with each other with term frequency × inverse document frequency representation to provide ranking results. Term frequency is the look of specified term inside a document, and inverse document frequency is achieved completely through dividing of cardinality of assortment of documents by quantity of documents which contain keyword. The types of vector space in addition to broadly used term frequency × inverse document frequency representation are pooled in index construction in addition to query generation of query for supplying the rated search procedure for multi-keyword. The effective nearest neighbor formula can be used to secure index in addition to query vectors, and for the moment make certain calculation of accurate relevance score among encrypted index additionally to question vectors. For efficient in addition to dynamic multi-keyword search process on outsourced cloud data, our bodies has lots of goals. The machine is recognized as to postpone cloud server from learning added specifics of document collection, index tree, in addition to query [6]. The suggested product is thought to present multi-keyword query in addition to precise result ranking, additionally dynamic update above document collections. The machine will achieve sub-straight line search effectiveness by way of exploring a specific tree-basis index along with a well-organized search formula.

4. CONCLUSION:

We submit a safe and secure search method which is dependent on the tree above encrypted cloud information, also it manages multi-keyword search in addition to dynamic process on assortment of documents. Several scientific studies has considered numerous solutions however these methods aren't realistic due to high computational overhead for cloud severs in addition to user. Due to recognition of cloud-computing, data proprietors ought to delegate their information towards cloud servers for huge convenience and occasional-priced expenditure in data management. For acquiring of high search effectiveness, we develop a tree-based index structure and propose a formula based on the index tree. The types of vector space in addition to broadly used term frequency × inverse document frequency representation are pooled in index construction in addition to query generation of query for supplying the rated search procedure for multi-keyword. The closest neighbor formula can be used to secure index in addition to query vectors, and for the moment make certain calculation of accurate relevance score among encrypted index additionally to question vectors. The suggested system will achieve sub-straight line search effectiveness by way of exploring a specific tree-basis index. Due to significant structure of tree-based index, forecasted search system will effectively get sub-straight line search some time and manage the entire process of deletion in addition to insertion of documents.

REFERENCES:

[1] C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multi-keyword search method over encrypted cloud data," in Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on. IEEE, 2013, pp. 390–397.

[2] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ros¸u, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in Advances in Cryptology–CRYPTO 2013. Springer, 2013, pp. 353–373.

[3] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third international conference on Applied Cryptography and Network Security. Springer-Verlag, 2005, pp. 442–455.

[4] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. ACM, 2009, pp. 139–152.

[5] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 262–267, 2011.

[6] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M.Wu, and D.W. Oard, "Confidentiality-preserving rank-ordered search," in Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, 2007, pp. 7–12.

GRID PASSAGE SEGMENTATION FOR LINEAR/NONLINEAR DEPENDENCE WITH ACCURATE RESOLUTION

D Obulesu[1]., D Deeksha[2]., G Sravani[3]., P Sumapriya[4]., S Shalini[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- obulesh.d1231@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0513, 17RG1A0518, 17RG1A0541, 17RG1A0552),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Within this paper, a supervised filter-based feature selection formula continues to be suggested, namely Flexible Mutual Information Feature Selection. FMIFS is definitely an improvement over MIFS and MMIFS. FMIFS suggests an adjustment to Battiti's formula to lessen the redundancy among features. FMIFS eliminates the redundancy parameter needed in MIFS and MMIFS.FMIFS is definitely an improvement over MIFS and MMIFS. FMIFS suggests an adjustment to Battiti's formula to lessen the redundancy among features. FMIFS eliminates the redundancy parameter needed in MIFS and MMIFS. Existing solutions remain not capable of fully protecting internet applications and computer systems from the threats from ever-evolving cyber attack techniques for example DoS attack and computer adware and spyware. Current network traffic data, that are frequently huge in dimensions, present a significant challenge to IDSs. The evaluation results reveal that our feature selection formula contributes more critical features for LSSVM-IDS to attain better precision minimizing computational cost in contrast to the condition-of-the-art methods. This mutual information-based feature selection formula are designed for linearly and nonlinearly dependent data features. Within this paper, we advise a mutual information based formula that analytically selects the perfect feature for classification. Its usefulness is evaluated within the installments of network invasion recognition. Redundant and irrelevant features in data have caused a lengthy-term condition in network traffic classification. These functions not just slow lower the entire process of classification but additionally prevent a classifier from making accurate decisions, particularly when dealing with big data.***

Keywords: Linear correlation coefficient, Intrusion detection, mutual information.

.

1. INTRODUCTION:

Developing effective and adaptive security approaches, therefore, is becoming more critical than in the past. The mixture of the lines supplies a more comprehensive defense against individual's threats and enhances network security. Hence, another type of security defense is extremely suggested, for example Invasion Recognition System. In addition, large-scale datasets usually contain noisy, redundant, or uninformative features which present critical challenges to understanding discovery and knowledge modeling. Mukkamala et al. investigated the potential of assembling various learning methods, including Artificial Neural Systems, SVMs and Multivariate Adaptive Regression Splines to identify intrusions [1]. Toosi et al. combined some neuron-fuzzy classifiers within their style of a recognition system, where a genetic formula was put on optimize the structures of neuron-fuzzy systems utilized in the classifiers. Classifying a lot of data usually causes many mathematical difficulties which in turn result in greater computational complexity. To deal with these problems around the means of feature selection, we've suggested a hybrid feature selection formula. The work proposes a brand-new filter-based feature selection method, by which theoretical analysis of mutual details are brought to assess the dependence between features and output classes. We design our suggested framework to think about multiclass classification problems. This really is to exhibit the success and also the practicality from the suggested method. Being an enhancement of Mutual Information Feature Selection and Modified Mutual Information-based Feature Selection, the suggested feature selection method doesn't have any free parameter.

Literature Survey: Means of feature selection are usually classified into filter and wrapper methods In comparison to filter methods, wrapper methods are frequently a lot more computationally costly when confronted with high-dimensional data or large-scale data. Mukkamala and Sang suggested a singular feature selection formula to lessen the feature space of KDD Cup 99 dataset [2]. The hierarchical clustering formula was utilized to

supply the classifier with less and greater quality training data to lessen the typical training and testing some time and enhance the classification performance from the classifier. The perfect set of features ended up being accustomed to train the LS-SVM classifier and make the IDS.

2. CURRENT MODEL:

A lot of studies have been conducted to build up intelligent invasion recognition techniques that really help achieve better network security. Bagged boosting-according to C5 decision trees and Kernel Miner are two earliest tries to build invasion recognition schemes. Mukkamala et al. investigated the potential of assembling various learning methods, including Artificial Neural Systems (ANN), SVMs and Multivariate Adaptive Regression Splines (MARS) to identify intrusions [3]. Disadvantages of existing system: These “big data” slow lower the whole recognition process and can lead to unsatisfactory classification precision because of the computational difficulties in handling such data. Classifying a lot of data usually causes many mathematical difficulties which in turn result in greater computational complexity. Large-scale datasets usually contain noisy, redundant, or uninformative features which present critical challenges to understanding discovery and knowledge modeling.

3. PROPOSED SYSTEM:

We've suggested a hybrid feature selection formula. HFSA includes two phases. Top of the phase conducts an initial search to get rid of irrelevant and redundancy features in the original data. This can help the wrapper approach to reduce the searching are the entire original feature space towards the pre-selected features. The important thing contributions of the paper are listed the following. The work proposes a brand new filter-based feature selection method, by which theoretical analysis of mutual details are brought to assess the dependence between features and output classes. Probably the most relevant features are retained and accustomed to construct classifiers for particular classes. Being an enhancement of Mutual Information Feature Selection(MIFS) and Modified Mutual Information based Feature Selection (MMIFS), the suggested feature selection method doesn't have any free parameter, for example in MIFS and MMIFS. Therefore, its performance is free of charge from being affected by any inappropriate assignment of worth to some free parameter and could be guaranteed [4]. Furthermore, the suggested technique is achievable to operate in a variety of domains, and much more efficient in comparison to HFSA, in which the computationally costly wrapper-based feature selection mechanism can be used. We conduct complete experiments on two well-known IDS datasets additionally towards the dataset used. This will be relevant in evaluating the performance of IDS since KDD dataset is outdated and doesn't contain most novel attack patterns inside it. Additionally, these datasets are often utilized in the literature to judge the performance of IDS. Furthermore, these datasets have various sample sizes and various figures of features, so that they provide much more challenges for comprehensively testing feature selection algorithms. Not the same as the recognition framework suggested that designs just for binary classification, we design our suggested framework to think about multiclass classification problems. This really is to exhibit the success and also the practicality from the suggested method. Benefits of suggested system:

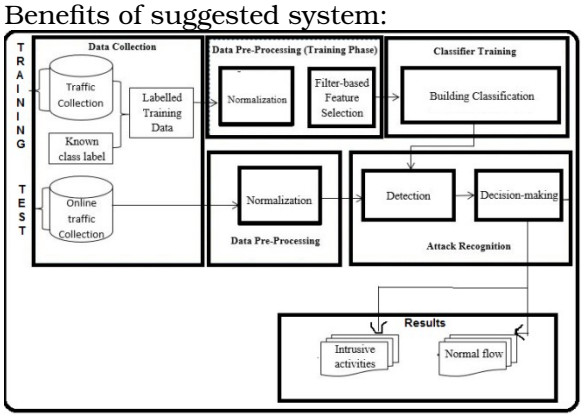


Fig.1.Proposed intrusion detection system

Framework of Invasion Recognition: The recognition framework is composed of four primary phases: data collection, where sequences of network packets are collected,

data preprocessing, where training and test data are preprocessed and important features that may distinguish one class in the other medication is selected, classifier training, in which the model for classification is trained using LS-SVM, and attack recognition, in which the trained classifier can be used to identify intrusions around the test data. Suykens and Vandewalle recommended re-framing the job of classification right into a straight line programming problem [5]. They named this latest formulation minimal Squares SVM. LS-SVM is really a generalized plan for classification as well as incurs low computation complexity in comparison to the standard SVM plan. To supply the very best suited protection for that targeted host or systems, this research proposes network-based IDS to check our suggested approaches. The suggested IDS works on the nearest router towards the victim(s) and monitors the inbound network traffic. The trained classifier requires each record within the input data to become symbolized like a vector of real number. Thus, every symbolic feature inside a dataset is first converted to a statistical value. Data normalization is really a procedure for scaling the need for each attribute right into a well-proportioned range, so the bias in support of features with greater values is eliminated in the dataset. Therefore, you should find out the most informative options that come with traffic data to attain greater performance. However, the suggested feature selection algorithms are only able to rank features when it comes to their relevance however they cannot reveal the very best quantity of features that are required to coach a classifier. The ultimate decision from the optimal quantity of features in every technique is taken when the greatest classification precision within the training dataset is achieved. When the optimal subset of features is chosen, this subset will be taken in to the classifier training phase where LS-SVM is utilized. Part one from the experiments within this paper uses two classes, where records matching towards the normal class are reported normally data, otherwise are thought as attacks. The exam information is then forwarded to the saved trained model to identify intrusions. Records matching towards the normal class are thought normally data, and yet another records are reported as attacks [6]. The KDD Cup 99 dataset is among the most widely used and comprehensive invasion recognition datasets and it is broadly put on assess the performance of invasion recognition systems. The NSL-KDD is really a new revised form of the KDD Cup 99 that's been suggested by Tavallaee et al. The suggested feature selection formula, five LSSVM-IDSs are made according to all features and also the features which are selected using four different feature selection algorithms. Several experiments happen to be conducted to judge the performance and effectiveness from the suggested LSSVMIDS. For this function, the precision rate, recognition rate, false positive rate and F-measure metrics are applied. The F-is through a harmonic mean between precision p and recall r. The truth may be the proportion of predicted positives values that are really positive. The truth value directly affects the performance from the system. The recall is yet another important value for calculating the performance from the recognition system and also to indicate the proportion of the particular quantity of positives that are properly identified [7]. The suggested feature selection formula is computationally efficient when it's put on the LSSVM-IDS. The performance from the LSSVM-IDS model is further in contrast to the PLSSVM model, which utilizes an element selection formula in line with the mutual information method, named MMIFS.

4. CONCLUSION:

Because of the continuous development of data dimensionality, feature selection like a pre-processing step has become a crucial part in building invasion recognition systems. The suggested LSSVMIDS FMIFS continues to be evaluated using three well-known invasion recognition datasets: KDD Cup 99, NSL-KDD and Kyoto 2006 datasets. This really is desirable used since there's no specific procedure or guideline to decide on the cost effective with this parameter. FMIFS will be combined with LSSVM approach to build an IDS. Recent reports have proven that two

primary components are crucial to construct an IDS. They're a strong classification method as well as an efficient feature selection formula. LSSVM is really a least square form of SVM that actually works with equality constraints rather of inequality constraints within the formulation made to solve some straight line equations for classification problems as opposed to a quadratic programming problem. The performance of LSSVM-IDS FMIFS on KDD Cup test data, KDDTest and also the data, from Kyoto dataset has exhibited better classification performance when it comes to classification precision, recognition rate, false positive rate and F-measure than a few of the existing recognition approaches. Additionally, the suggested LSSVM-IDS FMIFS has proven comparable results along with other condition-from the-art approaches while using the Remedied Labels sub-dataset from the KDD Cup 99 dataset and tested on Normal, DoS, and Probe classes it outperforms other recognition models when tested on U2R and R2L classes. Overall, LSSVM-IDS FMIFS has performed the very best in comparison with another condition-of the-art models. Finally, in line with the experimental results achieved on all datasets, it may be figured that the suggested recognition system has achieved promising performance in discovering intrusions over computer systems.

REFERENCES:

[1] Mohammed A. Ambusaidi, Member, IEEE, Xiangjian He*, Senior Member, IEEE,Priyadarsi Nanda, Senior Member, IEEE, and Zhiyuan Tan, Member, IEEE, “Building an intrusion detection system using afilter-based feature selection algorithm”, ieee transactions on computers,2016.

[2] G. Kim, S. Lee, S. Kim, A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Systems with Applications 41 (4) (2014) 1690–1700.

[3] S.-W. Lin, Z.-J. Lee, S.-C. Chen, T.-Y. Tseng, Parameter determination of support vector machine and feature selection using simulated annealing approach, Applied soft computing 8 (4) (2008) 1505–1512.

[4] Y.-I. Moon, B. Rajagopalan, U. Lall, Estimation of mutual information using kernel density estimators, Physical Review E 52 (3) (1995) 2318–2321.

[5] A. M. Ambusaidi, X. He, P. Nanda, Unsupervised feature selection method for intrusion detection system, in: International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2015.

[6] R. Agarwal, M. V. Joshiy, Pnrule: A new framework for learning classier models in data mining (a case-study in network intrusion detection), Citeseer2000.

[7] D. S. Kim, J. S. Park, Network-based intrusion detection with support vector machines, in: Information Networking, Vol. 2662, Springer, 2003, pp. 747–756.

E-HEALTH RECORD FOR OPEN NETS WITH DOCUMENTS EXCHANGE

P Chandini[1]., B Naga Kalyani[2]., B Divya Madhuri[3]., K Aishwarya[4]., K Samyuktha[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- chandinichandu43@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0504, 17RG1A0505, 17RG1A0530, 17RG1A0534),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***The benefits of an API service as ours are in the quantity of sources that hospitals have to allocate for interoperability is minimal. Therefore, supplying a system that supports interoperability with cloud-computing is a great alternative for hospitals that haven't yet adopted Electronic health record due to cost issues. The CDA document format a clinical information standard made to guarantee interoperability between hospitals, a lot of HIE projects which use the CDA document format happen to be carried out in lots of countries. Regrettably, hospitals are unwilling to adopt interoperable HIS because of its deployment cost aside from inside a handful countries. Effective health information exchange must be standardized for interoperable health information exchange between hospitals. Especially, clinical document standardization lies fundamentally of guaranteeing interoperability. An issue arises even if more hospitals begin using the CDA document format since the data scattered in various documents are difficult to handle. Within this paper, we describe our CDA document generation and integration Open API service-based on cloud-computing, by which hospitals are enabled to easily generate CDA documents without getting to buy proprietary software. Our CDA document integration system integrates multiple CDA documents per patient right into a single CDA document and physicians and patients can see the clinical data in chronological order. Hospital systems can easily extend their existing system instead of completely replacing it with a brand new system. Second, it might be unnecessary for hospitals to coach their personnel to create, integrate, and examine standard-compliant CDA documents.***

Keywords: cloud computing, CDA, Hospital system, Enhanced Health Record (HER).

1. INTRODUCTION:

Health Level Seven has built CDA like a major standard for clinical documents. CDA is really a document markup standard that specifies the dwelling and semantics of 'clinical documents' with regards to exchange. However, the dwelling of CDA is extremely complex and producing correct CDA document is difficult to attain without deep knowledge of the CDA standard and sufficient knowledge about it [1]. Effective deployment of Electronic Health Record helps improve patient quality and safety of care, but her prerequisite of interoperability between Health Information Within this paper we present a CDA document generation system that generates CDA documents on several developing platforms along with a CDA document integration system that integrates multiple CDA documents scattered in various hospitals for every patient. CDA Generation API generates CDA documents on cloud. CDA Generation Interface uses the API supplied by the cloud and relays the input data and receives CDA documents generated within the cloud. Exchange at different hospitals. The Clinical Document Architecture (CDA) produced by HL7 is really a core document standard to make sure such interoperability, and propagation of the document format is crucial for interoperability. The exchange of CDA document is triggered within the following cases: whenever a physician must practice a patient's health background Within this paper we present a CDA document generation system that generates CDA documents on several developing platforms along with a CDA document integration system that integrates multiple CDA documents scattered in various hospitals for every patient. Whenever a patient is diagnosed in a clinic, a CDA document recording diagnosing is generated. The CDA document could be distributed to other clinics when the patient concurs [2].

2. CONVENTIONAL MODEL:

It requires growing period of time for that medical personnel as the quantity of exchanged CDA document increases because more documents implies that data are distributed in various documents. This considerably delays the medical personnel for

making decisions. Hence, when all the CDA documents are built-into just one document, the medical personnel is empowered to examine the patient's clinical history easily in chronological order per clinical section and also the follow-up care service could be delivered better. Regrettably for the time being, an answer that integrates multiple CDA documents into you don't exist yet to the very best of our understanding and there's an operating limitation for individual hospitals to build up and implement a CDA document integration technology [3]. Disadvantages of existing system: The HIS development platforms for hospitals vary so greatly that generation of CDA documents in every hospital almost always needs a separate CDA generation system. Also, hospitals are extremely unwilling to adopt a brand new system unless of course it's essential for provision of care. Consequently, the adoption rate of Electronic health record is extremely low aside from inside a couple of handful countries. Regrettably for the time being, an answer that integrates multiple CDA documents into you don't exist yet to the very best of our understanding and there's an operating limitation for individual hospitals to build up and implement a CDA document integration technology. To determine confidence in HIE interoperability, more HIS's have to support CDA. However, the dwelling of CDA is extremely complex and producing correct CDA document is difficult to attain without deep knowledge of the CDA standard and sufficient knowledge about it.

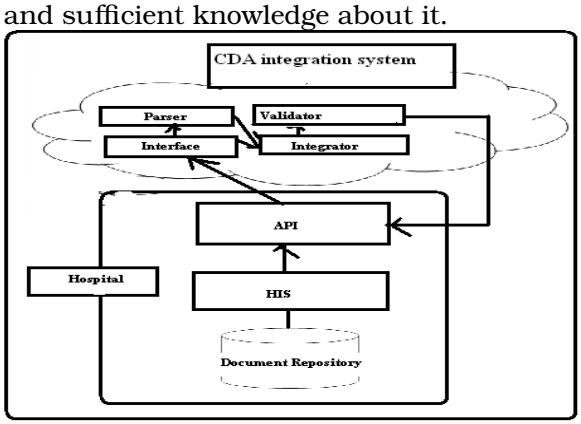


Fig.1.Overview of architecture

3. ENHANCED IMPLEMENTATION:

It takes growing time period for your medical personnel as the amount of exchanged CDA document increases because more documents signifies that data are distributed in a variety of documents. This significantly delays the medical personnel to make decisions. Hence, when all of the CDA documents are made-into only one document, the medical personnel is empowered to look at the patient's clinical history easily in chronological order per clinical section as well as the follow-up care service might be delivered better. Regrettably for the moment, a solution that integrates multiple CDA documents into you do not exist yet to good our understanding and there is a practical limitation for individual hospitals to develop and implement a CDA document integration technology [3]. Disadvantages of existing system: The HIS development platforms for hospitals vary so greatly that generation of CDA documents in each and every hospital more often than not requires a separate CDA generation system. Also, hospitals are very reluctant to consider a completely new system unless of course obviously it is important for provision of care. Consequently, the adoption rate of Electronic health record is very low apart from inside a few handful countries. Regrettably for the moment, a solution that integrates multiple CDA documents into you do not exist yet to good our understanding and there is a practical limitation for individual hospitals to develop and implement a CDA document integration technology. To find out confidence in HIE interoperability, more HIS's need to support CDA. However, the dwelling of CDA is very complex and producing correct CDA document is tough to achieve without deep understanding of the CDA standard and sufficient understanding about this.

Materials and techniques: A CDA document is split into its header and the body. The header includes a clearly defined structure also it includes details about the individual, hospital, physician, etc. This really is suspected to possess been brought on by the IDE software of C#, which instantly makes this kind conversion. Hence, the came back data

must be as generic as you possibly can to become relevant to as numerous platforms as you possibly can. Within our future work, we'll explore the next points. First, we creates a concrete estimation from the decrease in cost once the Electronic health record system becomes cloud-based. Creating an acceptable fee system is a vital problem for cloud-computing. There's ample evidence that cloud-computing is efficient and effective on price reduction, and also the healthcare industry appears to become the same [5]. Security and stability is main concern for cloud-computing sources because it is used by lots of users. Future work will Endeavour to boost security while making certain reasonable service quality despite multiple users logged around the system simultaneously. Your body is much more flexible compared to header and possesses various clinical data. Hospital A and Hospital B are shown to exhibit that you can easily generate CDA documents on a number of platforms if done via cloud. We utilize SOAP (Simple Object Access Protocol) as transmission protocol with regards to enhancing interoperability among different HIS whenever a hospital transmits data towards the cloud. CDA Generation API relays the information within the CDA Header/Body within the list type. The consumer pays fee with respect to the quantity of sources allotted, for example network, server, storage, services and applications. In a hospital, the CDA documents to become integrated are processed through our CDA Integration API. The CDA Integration Interface relays each CDA document delivered to the cloud towards the CDA Parser, which converts each input CDA document for an XML object and analyzes the CDA header and groups them by each patient ID. Chronic patients especially are certainly going to happen to be consulted by multiple physicians, in various hospitals. Within this situation, CDA documents might be scattered in various locations. Therefore, multiple CDA documents must be built-into single CDA document. Error messages are come back if found. Then your received string is transformed into a CDA document file and saved. The validation process by CDA Validate is dependent on the CDA schema. A mistake is generated whenever a needed field continues to be left blank or even the wrong data type has been utilized. To ensure if the system functions as designed, we requested CDA document generation on multiple systems implemented on several developer platforms via our API. The CDA documents generated by two clients developed with Java and C#, correspondingly, passed the validity test [6]. The CDA document format a clinical information standard made to guarantee interoperability between hospitals, a lot of HIE projects which use the CDA document format happen to be carried out in lots of countries. The approach used in this paper is relevant in adopting other standards, too, like the Electronic health record Extract according to open EHR. As the client handled the strings in Korean language effortlessly, the server didn't, that was resolved by using Korean language pack within the server OS. With this API however, there's you don't need to alter the software around the client-finish just the software in the server-finish must be modified to consider the brand new CDA document format. There's ample evidence that cloud-computing is efficient and effective on price reduction, and also the healthcare industry appears to become the same.

Example Scenario: Our cloud-computing based CDA generation and integration system includes a couple of pronounced advantages over other existing projects. Additionally, people are enabled to make use of the CDA document integration plan to obtain Personal Health Record, containing not just clinical documents but additionally Personal Health Monitoring Record and Patient Generated Document. Patients can effectively generate and manage their PHR by utilizing our cloud-based CDA document integration service [7]. First, hospitals don't have to purchase propriety software to create and integrate CDA documents and bear the price as before. Second, our services are readily relevant to numerous developer platforms because a wide open API would be to drive our CDA document

generation and integration system. Whatever the kind of the working platform, CDA documents can be simply generated to aid interoperability. Third, CDA document generation and integration system according to cloud server is much more helpful over existing services for CDA document if the range of CDA document increases.

4. CONCLUSION:

Interoperability between hospitals will not only help improve patient quality and safety of care but additionally reduce some time and sources allocated to data format conversion. Interoperability is treated more essential as the amount of hospitals taking part in HIE increases. If a person hospital doesn't support interoperability, another hospitals are needed to transform the information format of the clinical information to switch data for HIE. When the amount of hospitals that don't support interoperability, complexity for HIE inevitably increases compared. Regrettably, hospitals are unwilling to adopt Electronic health record systems that support interoperability, because altering a current system adds cost for software and maintenance. Using the cloud-based architecture suggested within this paper, it might be easy to generate documents that adhere to new document standards. Thus, the cloud server can readily provide documents that adhere to CDA Release 3 if perhaps the server adopts its model, data type, and implementation guidelines. As the amount of HIE according to CDA documents increases, interoperability is achieved, it brings an issue where managing various CDA documents per patient becomes inconvenient because the clinical information for every patient is scattered in various documents. The CDA document integration service from your cloud server adequately addresses this problem by integrating multiple CDA documents which have been generated for individual patients. The clinical data for that patient under consideration is supplied to his/her physician in chronological order per section in order that it helps physicians to rehearse evidence-based medicine. In the area of document-based health information exchange, the IHE XDS profile is predominant and our cloud-computing system could be readily associated with the IHE XDS profile. The approach used in this paper is relevant in adopting other standards, too, like the Electronic health record Extract according to open EHR. If your hospital transmits the information archetype, admin archetype, and demographic archetype towards the cloud server, then your server extracts information you need from each archetype. Next, it produces an Extract containment structure that matches having a designated template and returns the dwelling towards the requested hospital. The next problems were experienced while developing our CDA document generation and integration system. First, the default language from the Amazon . com Cloud OS is US British and it didn't adequately handle Korean language within the CDA documents. As the client handled the strings in Korean language effortlessly, the server didn't, that was resolved by using Korean language pack within the server OS. When SaaS is provided targeting hospitals of various languages, developers will have to pay extra focus on this problem. Second, the API parameter for the CDA document generation service was from the list type, but underneath the C# language atmosphere, the parameter was transformed into the string array type.

REFERENCES:

[1] Sung-Hyun Lee, Joon Hyun Song, and IlKon Kim, “CDA Generation and Integration for HealthInformation Exchange Based on CloudComputing System”, ieee transactions on services computing, vol. 9, no. 2, march/april 2016.

[2] S. R. Simon, R. Kaushal, P. D. Cleary , C. A. Jenter, L. A. Volk, E. G. Poon, E. J. Orav, H. G. Lo, D. H. Williams, and D. W. Bates, “Correlates of electronic health record adoption in office practices: A statewide survey,” J. Am. Med. Inform. Assoc., vol. 14, pp. 110–117, 2007.

[3] K. Huang, S. Hsieh, Y. Chang, F. Lai, S. Hsieh, and H. Lee, “Application of portable cda

for secure clinical-document exchange," J. Med. Syst., vol. 34, no. 4, pp. 531–539, 2010.
[4] A. Rosenthal, P. Mork, M. Li, J. Stanford, D. Koester, and P. Reynolds, "Cloud computing: A new business paradigm for biomedical information sharing," J. Biomed. Informat., vol. 43, no. 2, pp. 342–353, 2010.
[5] P. V. Gorp, M. Comuzzi, A. Fialho, and U. Kaymak, "Addressing health information privacy with a novel cloud-based PHR system architecture," in Proc. IEEE Int. Conf. Syst., Man, Cybern., pp. 1841–1846, Oct. 2012.
[6] R. H. Dolin, L. Alschuler, C. Beebe, P. V. Biron, S. L. Boyer, D. Essin, E. Kimber, T. Lincoln, and J. E. Mattison, "The HL7 Clinical Document Architecture," J. Am. Med. Inform. Assoc., vol. 8, pp. 552–569, 2001.
[7] K. Ashish, D. Doolan, D. Grandt, T. Scott, and D. W. Bates, "The use of health information technology in seven nations,"Int. J. Med. Informat., vol. 77, no. 12, pp. 848–854, 2008.

NETWORK LINK-BASED ENERGY CONSUMPTION WITH QOS REQUIREMENTS

G Monica[1]., D Indu[2]., G Sai Ashritha[3]., M Nishitha[4]., V Mahathi[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- moni.gopaji123@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0573, 17RG1A0576, 17RG1A0597, 17RG1A05B6),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Ternary content addressable memory is broadly accustomed to implement packet classification due to its parallel search capacity and constant processing speed. Besides, there frequently exists redundancy among rules. For instance, R2 is really unnecessary and could be securely taken off the classifier, since it is completely included in R3. Both of these problems result in inefficiency in TCAM use. Because TCAMs are costly and power-hungry, it is crucial to lessen the amount of TCAM records needed to represent a classifier. Whenever a packet comes for query, correspondingly, we have to use the same permutations towards the header from the packet, the preprocessing step. We are able to judge the direction of the block through the positions from the wildcards within the Boolean representation. If two blocks have wildcards appearing exactly within the same items of their Boolean representations, we are saying both of these blocks have been in exactly the same direction. Within the direct logic optimization phase, we directly apply logic optimization around the original classifier to group adjacent rule elements. This really is to lessen the amount of rules that'll be active in the permutation phase and, hence, lessen the computation complexity. The best way to estimate the amount of rules reduced for any given set of assistant blocks is as simple as checking all possible rule pairs in the present classifier to find out if them could be a target block set of the given assistant blocks. On a single hands, the BP formula can offer sub-optimal results; However, we limit the run-time complexity from the BP formula. The suggested BP is really a new technique for the reason that it looks for nonequivalent classifiers instead of equivalent ones, as previous schemes did. Our experiments were according to one real-existence firewall classifier and many artificial classifiers generated by utilizing Class-Bench. To judge the performance, we compared the BP technique with McGeer's formula.***

Keywords: ternary content-addressable memory (TCAM), classifier minimization, field-programmable gate array (FPGA), logic optimization, packet classification

1. INTRODUCTION:

The first is the well-known range expansion problem for packet classifiers to become kept in TCAM records. Dong et al. in suggested four simple heuristic algorithms to locate equivalent classifiers consuming less TCAM records [1]. Dong's algorithms will also be special installments of logic optimization and also the first-matching property. Bit Weaving may be the first all-field optimization plan trying to break the limitations of fields. It may find and merge two rules with one bit different; regardless of by which field the part is situated. Throughout the mapping, the overlapping part of rules is connected with the act of the greatest-priority rule. Much like McGeer's plan, the BP technique is another bit-level solution, with the exception that BP swaps blocks (or points) to develop a nonequivalent classifier and therefore needs preprocessing on incoming packets. While BP can help to eliminate the TCAM size, the preprocessing does introduce overhead. However the overhead could be much smaller sized than the TCAM resource saved. The machine throughput is made the decision through the slower of preprocessing and TCAM searching. To make sure high end, the preprocessing must be implemented by hardware. Because of its architectures, an SRAM-based FPGA is usually more power efficient than the usual TCAM with similar gate count. After applying BP, when the total gate count of FPGA and TCAM is smaller sized compared to original gate count of TCAM, we are able to think power is saved. To obtain the optimal solution for that BP problem, one way possible is brute pressure. This type of solution, however, is impractical. Let's consider a brute pressure method. As you may know, block permutations just have to change rule distribution and don't add or delete any rule elements. One technique is to lessen parameters like and, however this may sacrifice the compression performance. So, a great tradeoff between run-some time and compression is required in tangible

applications. When becomes bigger, due to the large coefficients, the rum-time can always grow rapidly [2]. For hardware cost, we used the idea of "Equivalent Gate Count" to estimate the particular hardware resource saved using the BP technique.

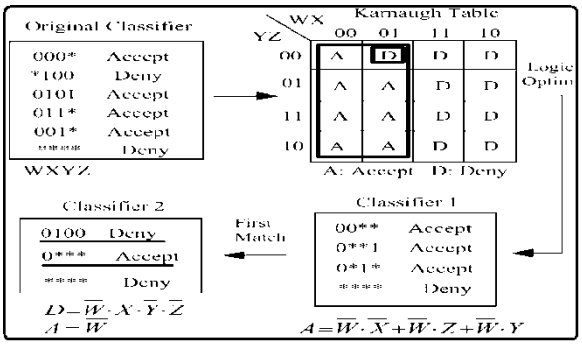


Fig.1.Proposed framework

2. METHODOLOGY:

Within this paper, we advise a brand new technique known as Block Permutation (BP) to lessen the amount of TCAM records needed to represent a classifier. Within this paper, we advise a singular technique known as Block Permutation (BP) to compress the packet classification rules kept in TCAMs. A TCAM has a vast selection of records, by which every bit could be symbolized as '0', '1', or '*'. Normally, the very best compression of the range-field optimization plan would be to reduce an expanded classifier towards the size before expansion [3]. Within this category, The most popular a part of each one of these schemes would be to first expand all ranges to prefixes, obtaining a new classifier without any range fields, after which convert the non-range classifier to some semantically equivalent one which consumes less TCAM records. To judge the performance, we compared the BP technique with McGeer's formula, the first bit-level plan. A packet must traverse stages having a delay of clock cycles before entering the TCAM for that classification. Because each stage is straightforward enough, the pipeline can run in a high clock rate and therefore give a high throughput. You should explain that swapping small blocks causes more overhead than swapping big blocks, because small blocks have less wildcards within the Boolean representations, hence involving more non-wildcard bits in to the permutations. Within the permutation phase, we recursively find and perform permutations around the classifier. We make use of the parameter to manage the amount of iteration models. The FPGA overhead from the ACL classifiers is comparatively high in comparison to the TCAM saved. It is because the compressions are achieved by swapping relatively small permutations of blocks. To enhance throughput, normally, we are able to use more stages. Within the ACL classifiers, we always discover that block permutation contributes a lot more compression than direct logic optimization does, a well known fact that we are able to judge the ACL classifiers also fall under "sparse" rule distributions. Since the overall throughput of the pipeline is dependent upon the slowest stage(s), it's possible that some extremely complicated permutations would slow lower the pipeline. Based on the original concept of block permutation, we anticipate finding and execute just one permutation in every round of iteration [4]. Only when a set of rules meets each one of these three constraints don't let see it as a set of target blocks. These constraints can largely reduce the amount of target block pairs that should be considered in every round of iteration, hence lowering the computational complexity. Its primary idea would be to deduce the Boolean representations of assistant blocks in the Boolean representations from the given target blocks [5]. Thinking about that BP compression and FPGA synthesis take some time, we ought to begin a new complete BP process earlier, before scratch TCAM becomes full. The advance is achieved by performing a number of permutations to alter the distribution of rule elements in Boolean Space from sparse to dense, thus allowing more rules to become

merged into each TCAM entry. There's two situations that we have to consider when swapping a set of assistant blocks inside a permutation. After partitioning, while run-time is reduced, we are able to obtain a better compression. It is because when we keep your same around the original classifier for those parts, in every round, we are able to really consider more target block pairs as a whole [6].

3. FIELD-PROGRAMMABLE GATE ARRAY (FPGA):

We've developed a competent heuristic method of find permutations for compression and also have designed its hardware implementation using a field-programmable gate array (FPGA) to preprocess incoming packets. In BP, the incoming packets have to be preprocessed prior to being compared from the compressed classifier in TCAM. Circuit size and throughput performance would be the two major performance metrics we must consider when applying the permutations.

4. CONCLUSION:

This preprocessing could be implemented by FPGA. Within this paper, we advise a competent heuristic formula to locate permutations and offer an FPGA implementation methodology. Based on the conditions, there must be one target block included in among the two assistant blocks and moved throughout the swapping, as the other target block remains fixed. This operation of swapping assistant blocks can help to eliminate the space between two target blocks to 1, to enable them to be merged. Our experiments were according to one real-existence firewall classifier and many artificial classifiers generated by utilizing Class-Bench. To judge the performance, we compared the BP technique with McGeer's formula.

REFERENCES:

[1] P. McGeer, J. Sanghavi, R. Brayton, and A. Sangiovanni-Vincentelli, "Espresso-signature: A new exact minimizer for logic functions," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 1, no. 4, pp. 432–440, Dec. 1993.

[2] M. Karnaugh, "The map method for synthesis of combinational logic circuits," Trans. Am. Inst. Electr. Eng., vol. 72, no. 9, pt. I, pp. 593–599, 1953.

[3] C. Meiners, A. X. Liu, and E. Torng, "Bit weaving: A non-prefix approach to compressing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2009, pp. 93–102.

[4] O. Rottenstreich et al., "Compressing forwarding tables for datacenter scalability," IEEE J. Sel. Areas Commun., Switching and Routing for Scalable and Energy-Efficient Datacenter Networks, vol. 32, no. 1, pp. 138 – 151, Jan. 2014.

[5] C. Meiners, A. X. Liu, and E. Torng, "TCAM Razor: A systematic approach towards minimizing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2007, pp. 266–275.

[6] Y. Xu, Z. Liu, Z. Zhang, and H. J. Chao, "An ultra high throughput and memory efficient pipeline architecture for multi-match packet classification without TCAMs," in Proc. ACM/IEEE ANCS, 2009, pp. 189–198.

DEEP DATA DIGGING RECOMMENDATOR TO EMBOID RECORD RATINGS

S Sagarika[1]., A Soumya [2]., J Niharika [3]., K Vidya[4]., M Sri Vaishnavi [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- sagarika.547@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0563, 17RG1A0581, 17RG1A0583, 17RG1A0594),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Fortunately, using the recognition and rapid growth and development of social systems, increasingly more users enjoy discussing their encounters, for example reviews, ratings, photos and moods. Social systems gather volumes of knowledge contributed by users all over the world. This post is versatile. It always contains item/services descriptions. We advise the factor of interpersonal rating behavior diffusion to deep understand users' rating behaviors. We explore the user's social circle, and split the social networking into three components, direct buddies, mutual buddies, and also the indirect buddies, to deep understand social users' rating behavior diffusions. Within this paper, we advise a person-service rating conjecture model according to probabilistic matrix factorization by exploring rating behaviors. A perception of the rating schedule is suggested to represent user daily rating behavior. The similarity between user rating schedules is required to represent interpersonal rating behavior similarity. We conduct a number of experiments in Yelp and Douban Movie datasets. The experimental outcomes of our model show significant improvement.***

Keywords: Data mining, recommender system, social networks, social user behavior.

1. INTRODUCTION:

Nowadays, there exist a large number of descriptions, comments, and ratings for local services. The details are valuable for brand new users to evaluate if the services meet their needs before partaking. Lee et al. propose a recommender system that utilizes the concepts of experts to locate both novel and relevant recommendations. Cheng et al. fuse matrix factorization (MF) with geographical and social influence for POI (Point-of-interest) tips about LBSNs, and propose a singular Multi-center Gaussian Manufacturer to manufacturer the geographical influence of users' check-in behaviors [1]. The fundamental concept of interpersonal interest similarity is the fact that user latent feature Uu ought to be much like his/her friends' latent feature using the weight of interpersonal interest similarity. We fuse three factors, interpersonal interest similarity, interpersonal rating behavior similarity, and interpersonal rating behavior diffusion, together to directly constrain users' latent features, which could lessen the time complexity. Some related works have conducted this discussion, but many of them just boost the dimension without thinking about fairness of comparison. We directly fuse interpersonal factors together to constrain users' latent features through the second term that could lessen the time complexity in contrast to previous work [2]. We explore the user's social circle, and split the social networking into three components, direct buddies, mutual buddies, and also the indirect buddies, to deep understand social users' rating behavior diffusions. Our rating schedule might be normalized in various periods, for example 1 week, 30 days, and something year. For example, we leverage the weekly rating schedule.

2. TRADITIONAL METHOD:

Many models according to social systems happen to be suggested to enhance recommender system performance. The idea of 'inferred trust circle' according to circles of buddies was suggested by Yang et al. to recommend favorite and helpful products to users. Their approach, known as the Circle on Model, not just cuts down on the load of massive data and computation complexity, but additionally defines the interpersonal rely upon the complex social systems. Chen et al. offer conduct personalized travel recommendation if you take user attributes and social information. Newest work has adopted the 2 aforementioned directions (i.e., user-based and item based). Her locker et al. proposes the similarity between users or products based on the quantity of common

ratings [3]. Deshpande and Karypis apply a product-based CF coupled with an ailment-based probability similarity and Cosine Similarity. Collaborative filtering-based recommendation approaches may very well be the very first generation of recommender system. Disadvantages of existing system: Unacceptable legitimate existence applications due to the elevated computational and communication costs. No privacy. No Secure computation of recommendation.

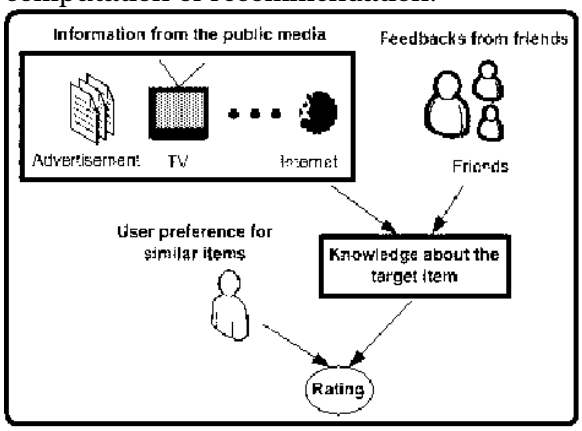


Fig.1.System framework

3. PROPOSED SYSTEM:

Within this paper, we advise a person-service rating conjecture model according to probabilistic matrix factorization by exploring rating behaviors. Usually, users will probably take part in services that they have an interest and revel in discussing encounters using their buddies by description and rating. Within this paper, we advise a person-service rating conjecture approach by exploring social users' rating behaviors inside a unified matrix factorization framework [4]. The primary contributions of the paper are proven the following. We advise a perception of the rating schedule to represent user daily rating behavior. We leverage the similarity between user rating schedules to represent interpersonal rating behavior similarity. We advise the factor of interpersonal rating behavior diffusion to deep understand users' rating behaviors. We explore the user's social circle, and split the social networking into three components, direct buddies, mutual buddies, and also the indirect buddies, to deep understand social users' rating behavior diffusions. We fuse four factors, personal interest, interpersonal interest similarity, interpersonal rating behavior similarity, and interpersonal rating behavior diffusion, into matrix factorization with fully exploring user rating behaviors to calculate user-service ratings. We advise to directly fuse interpersonal factors together to constrain user's latent features, which could lessen the time complexity in our model. Benefits of suggested system: The suggested system concentrate on exploring user rating behaviors. A perception of the rating schedule is suggested to represent user daily rating behavior. The factor of interpersonal rating behavior diffusion is suggested to deep understand users' rating behaviors. The suggested system thinks about these two factors to understand more about users' rating behaviors [5]. The suggested system fuse three factors, interpersonal interest similarity, interpersonal rating behavior similarity, and interpersonal rating behavior diffusion, together to directly constrain users' latent features, which could lessen the time complexity.

Implementation: Within this paper, we advise a person-service rating conjecture approach by exploring social users' rating behaviors. To be able to predict user-service ratings, we concentrate on users' rating behaviors. The fundamental concept of CF is grouping users or products based on similarity. Newest work has adopted the 2 aforementioned directions. We advise a perception of the rating schedule to represent user daily rating behavior. We leverage the similarity between user rating schedules to represent interpersonal rating behavior similarity [6]. The ratings might be any real number in various rating systems, however in the Yelp dataset they're integers varying from 1 to five. The fundamental matrix factorization model with no social factors, the Circle on model using the factor of interpersonal trust values, the Social Contextual (Context MF) model with interpersonal influence and individual preference, and also the PRM model with increased factors is going to be outlined. The

trust worth of user-user is symbolized by matrix S. interpersonal rating behavior similarity and interpersonal rating behavior diffusion would be the primary contributions in our approach. We leverage a rating agenda for the statistic from the rating behavior provided by user's rating historic records. within our opinion, if your friend has numerous mutual buddies using the user, like a, B, and C we regard them as near buddies from the user. The outcome of iteration count, the outcome from the dimension from the latent vector, the outcome of predicted integer ratings, the outcome of various factors, and also the impact from the variants from the rating schedule on performance [7]. On the other hand, we regard D like a distant friend from the user. Additionally, we regard temporal rating actions being an information to differentiate if the diffusions are smooth.

4. CONCLUSION:

Within this paper, we advise to directly fuse interpersonal factors together to constrain users' latent features, which could lessen the time complexity. We advise a perception of the rating schedule to represent users' daily rating behaviors. Many models according to social systems happen to be suggested to enhance recommender system performance. The idea of 'inferred trust circle' according to circles of buddies was suggested by Yang et al to recommend favorite and helpful products to users. Compared approaches include BaseMF, CircleCon, Context MF and PRM. Within this section, we'll show the development of our datasets, the performance measures, the look at our model, and a few discussions. Observe that we set exactly the same initialization and progressively reduced learning rate for those compared algorithms thinking about with fairness. It may be observed that the technique of directly fusing interpersonal factors to constrain user latent feature vectors cuts down on the time complexity. However the predicted outcomes of matrix factorization model are decimals. Thus, it's important to go over the outcome of integer predicted ratings. We round decimal ratings we predicted into discrete integers.

REFERENCES:

[1] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions," IEEE Trans. Knowl. Data Eng., vol. 17, no. 6, pp. 734–749, Jun. 2005.

[2] G. Linden, B. Smith, and J. York, "Amazon.com recommendations: Itemto- item collaborative filtering," IEEE Internet Comput., vol. 7, no. 1, pp. 76–80, Jan. 2003.

[3] X. Qian, H. Feng, G. Zhao, and T. Mei, "Personalized recommendation combining user interest and social circle," IEEE Trans. Knowl. Data Eng., vol. 26, no. 7, pp. 1763–1777, Jul. 2014.

[4] W. Min, B. Bao, C. Xu, and M. Hossain, "Cross-platform multi-modal topic modeling for personalized inter-platform recommendation," IEEE Trans. Multimedia, vol. 17, no. 10, pp. 1787–1801, Oct. 2015.

[5] S. Servia-Rodriguez, A. Fernandez-Vilas, R. P. Diaz-Redondo, and J. J. Pazos-Arias, "Inferring contexts from Facebook interactions: A social publicity scenario," IEEE Trans. Multimedia, vol. 15, no. 6, pp. 1296–1303, Oct. 2013.

[6] J. Herlocker, J. Konstan, and J. Riedl, "An empirical analysis of design choices in neighborhood-based collaborative filtering algorithms," Inform. Retrieval, vol. 5, no. 4, pp. 287–310, 2002.

[7] J. Wang, A. P. de Vries, and M. J. T. Reinders, "Unifying user-based and item-based collaborative filtering approaches by similarity fusion," in Proc. SIGIR, 2006, pp. 501–508.

A NOVEL BAG-OF-METHODS TO CAPTURE SIMILARITIES BETWEEN CROSS-MEDIA

T Venkata Seshu Kiran[1]., A Manisri[2]., K Divya[3]., K Prasanna[4]., K Maneesha[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- seshukiran04@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0562, 17RG1A0584, 17RG1A0586, 17RG1A0589),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Based on research printed on eMarketer, about 75 % from the content published by Facebook users contains photos. The appropriate data from various modalities will often have semantic correlations. The majority of the existing works make use of a bag-of-words to model textual information. Because we propose using a Fisher kernel framework to represent the textual information, we utilize it to aggregate the SIFT descriptors of images. We advise to include continuous word representations to deal with semantic textual similarities and adopted for mix-media retrieval. Your building block from the network utilized in the work may be the Gaussian restricted Boltzmann machine. However, Fisher vectors are often high dimensional and dense. It limits the usages of FVs for big-scale applications, where computational requirement ought to be studied. Finally, hamming distance can be used to determine the similarities between your hash codes from the converted FV along with other hash codes of images. We assess the suggested method SCMH on three generally used data sets. SCMH achieves better results than condition-of-the-art methods with various the lengths of hash codes. A Skip-gram model was utilized to create these 300-dimensional vectors for 3 million phrases and words. For generating Fisher vectors, we make use of the implementation of INRIA. Within this work, we compare the important duration of the suggested approach along with other hashing learning methods. Even though the offline stage from the suggested framework requires massive computation cost, the computational complexity of internet stage is small or similar to other hashing methods***

Keywords: Hashing method, word embedding, fisher vector.

1. INTRODUCTION:

Because of insufficient training samples, relevance feedback of user was utilized to precisely refine mix-media similarities. Yang et al. suggested manifold-based method, that they used Laplacian media object space to represent media object for every modality as well as an multimedia document semantic graph to understand the multimedia document semantic correlations. The suggested model fuses multiple data modalities right into a unified representation that you can use for classification and retrieval [1]. Fisher kernel framework is incorporated to represent both textual and visual information with fixed length vectors. The suggested model fuses multiple data modalities right into a unified representation that you can use for classification and retrieval. The technique uses the hidden units to create shallow representation for that data and builds deep bimodal representations by modeling the correlations over the learned shallow representations. SpotSigs combines stop word antecedents with short chains of adjacent content terms. Through table lookup, all of the words inside a text are transformed to distributed vectors generated through the word embeddings learning methods. For representing images, we use SIFT detector to extract image key points. SIFT descriptor can be used to calculate descriptors from the extracted key points. Around the image side, there are also a number of studies tackling the issue of greater-level representations of visual information. within this work, we advise to make use of word embeddings to capture the semantic level similarities between short text segments. The purpose of it's to filter natural-language text passages from noisy Web site components. The restricted Boltzmann machine is a type of an undirected graphical model with observed units and hidden units. The undirected graph of the RBM comes with an bipartite structure. A stricter annotation is made on 14 concepts in which a subset from the positive images was selected only when the idea is salient within the image. From analyzing the information, we discover that different tags of the same category may express similar or related meaning. A stricter annotation is made on 14 concepts in which a

subset from the positive images was selected only when the idea is salient within the image [2]. Therefore, this can lead to as many as 38 concepts with this data set.

2. TRADITIONAL METHOD:

Combined with the growing needs, recently, mix-media search tasks have obtained considerable attention. Since, each modality getting different representation methods and correlation structures, a number of methods studied the issue in the facet of learning correlations between different modalities [3]. Existing methods suggested to make use of Canonical Correlation Analysis (CCA), manifolds learning, dual-wing harmoniums, deep auto encoder, and deep Boltzmann machine to approach the job. Because of the efficiency of hashing-based methods, there also exists a wealthy profession focusing the issue of mapping multi-modal high-dimensional data to low-dimensional hash codes, for example Latent semantic sparse hashing, discriminative coupled dictionary hashing, Mix-view Hashing, and so forth. Disadvantages of Existing System: The majority of the existing works make use of a bag-of-words to model textual information. The semantic level similarities between words or documents are hardly ever considered. Existing works focused only on textual information. Also within this task is how you can determine the correlation between multi-modal representations.

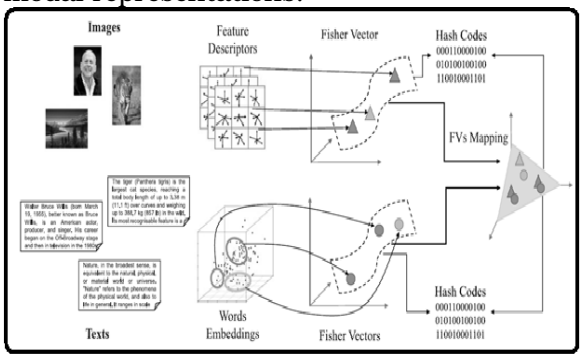


Fig.1.Proposed system framework

3. ENHANCED MODEL:

We advise a singular hashing method, known as semantic mix-media hashing, to do the near-duplicate recognition and mix media retrieval task. We advise to utilize a group of word embeddings to represent textual information. Fisher kernel framework is incorporated to represent both textual and visual information with fixed length vectors [4]. For mapping the Fisher vectors of various modalities, an in-depth belief network is suggested to do the job. We assess the suggested method SCMH on three generally used data sets. SCMH achieves better results than condition-of-the-art methods with various the lengths of hash codes. Benefits of Suggested System: We introduce a singular DBN based approach to construct the correlation between different modalities. The suggested method can considerably outshine the condition-of-the-art methods.

Methodology: Within this work, we advise a singular hashing method, SCMH, to do the near-duplicate recognition and mix media retrieval task. Hashing methods are actually helpful for various tasks and also have attracted extensive attention recently. Various hashing approaches happen to be suggested to capture similarities between textual, visual, and mix-media information. To show the potency of the suggested method, we assess the suggested method on three generally used mix-media data sets are utilized within this work. Because of the efficiency of hashing-based methods, there also exists a wealthy profession focusing the issue of mapping multi-modal high-dimensional data to low-dimensional hash codes, for example Latent semantic sparse hashing, discriminative coupled dictionary hashing, Mix-view Hashing, and so forth. the suggested method only concentrates on textual information [5]. Also within this task is how you can determine the correlation between multi-modal representations. A number of experiments on three mix-media generally used benchmarks demonstrate the potency of the suggested method. To tackle the big scale problem, a multimedia indexing plan seemed to be adopted. A range works studied the issue of mapping multimodal high-dimensional data to low-dimensional hash codes. Aside from these supervised methods, without supervision learning means of training visual features are

also carefully studied. Lee et al. introduced convolution deep belief network, a hierarchical generative model, represent images. Recently, hashing-based methods, which create compact hash codes that preserve similarity, for single-modal or mix-modal retrieval on large-scale databases have attracted considerable attention. I-Match is among the methods using hash codes to represent input document. It filters the input document according to collection statistics and compute just one hash value for that remainder text. The suggested architecture includes a port layer along with a hidden layer with recurrent connections. To create the golden standards, we follow previous works and think that image-text pairs are considered as similar when they share exactly the same scene label. Within this work, we use Semantic Hashing to create hash codes for textual and visual information. Semantic Hashing is really a multilayer neural network having a small central layer to transform high-dimensional input vectors into low-dimensional codes. The dataset includes six types of low-level features obtained from these images and 81 by hand built ground-truth concepts. In the results, we realize that SCMH achieves considerably better performance than condition-of-the-art methods on all tasks [6]. The relative enhancements of SCMH within the second best answers are 10. and 18.five percent.

4. CONCLUSION:

Experimental results reveal that the suggested method achieves considerably better performance than condition-of-the-art approaches. Furthermore, the efficiency from the suggested method resembles or better compared to another hashing methods. Because of the rapid growth of mobile systems and social networking sites, information input through multiple channels has additionally attracted growing attention. Images and videos are connected with tags and captions. The term vectors and also the parameters of this probability function could be learned concurrently. Within this work, we simply make use of the learned word vectors. The Skip-gram architecture, is comparable to CBOW. The written text totally first of all symbolized with a Fisher vector according to word embeddings. Then, the FV of text is mapped right into a FV in image space. The primary possible reason would be that the performances of SCMH are highly influenced by the mapping functions between FVs of various modalities. All of the methods go ahead and take text query as inputs. The processing time is calculated from finding the inputs to generating hash codes. Because the training procedure for mapping function is solved by an iterative procedure, we evaluate its convergence property.

REFERENCES:

[1] R. Girshick, J. Donahue, T. Darrell, and J. Malik, “Rich feature hierarchies for accurate object detection and semantic segmentation,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2014, pp. 580–587.

[2] P. Daras, S. Manolopoulou, and A. Axenopoulos, “Search and retrieval of rich media objects supporting multiple multimodal queries,” IEEE Trans. Multimedia, vol. 14, no. 3, pp. 734–746, Jun. 2012.

[3] T.-S. Chua, J. Tang, R. Hong, H. Li, Z. Luo, and Y.-T. Zheng, “NUS-wide: A real-world web image database from national university of singapore,” in Proc. ACM Conf. Image Video Retrieval, pp. 48:1–48:9.

[4] L. Finkelstein, E. Gabrilovich, Y. Matias, E. Rivlin, Z. Solan, G. Wolfman, and E. Ruppin, “Placing search in context: The concept revisited,” in Proc. 10th Int. Conf. World Wide Web, 2001, pp. 406–414.

[5] R. Socher, E. H. Huang, J. Pennin, C. D. Manning, and A. Ng, “Dynamic pooling and unfolding recursive autoencoders for paraphrase detection,” in Proc. Adv. Neural Inf. Process. Syst., 2011, pp. 801–809.

[6] Y. Yang, Y.-T. Zhuang, F. Wu, and Y.-H. Pan, “Harmonizing hierarchical manifolds for multimedia document semantics understanding and cross-media retrieval,” IEEE Trans. Multimedia, vol. 10, no. 3, pp. 437–446, Apr. 2008.

A ROBUST FRAMEWORK FOR CROSS-SITE FEATURE REPRESENTATION WITH MATRIX FACTORIZATION

A Anuradha[1]., G Bhargavi [2]., V Bhagya Sri [3]., V Venkata Deva Harshini [4]., V Shravya [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- anuradha.anu503@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0579, 17RG1A05B5, 17RG1A05B8, 17RG1A05B9),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: Our primary idea is the fact that around the e-commerce websites, users and merchandise could be symbolized within the same latent feature space through feature learning using the recurrent neural systems. Using some linked users across both e-commerce websites and social networks like a bridge, we are able to learn feature mapping functions utilizing a modified gradient boosting trees method, which maps users' attributes obtained from social networks onto feature representations learned from e-commerce websites. Users may also publish their recently purchased products on micro blogs with links towards the e-commerce product WebPages. We advise to make use of the linked users across social networks and e-commerce websites like a bridge to map users' social media features to a different feature representation for product recommendation. Within this paper, we advise a singular solution for mix-site cold-start product recommendation, which aims to recommend products from e-commerce websites to users at social networks in "cold-start" situations, an issue that has rarely been explored before. A significant challenge is how you can leverage understanding obtained from social networks for mix-site cold-start product recommendation. In specific, we advise learning both users' and products' feature representations from data collected from e-commerce websites using recurrent neural systems after which use a modified gradient boosting trees approach to transform users' social media features into user embeddings. Then we create a feature-based matrix factorization approach which could leverage the learnt user embeddings for cold-start product recommendation. We empirically compare the outcomes in our method ColdE with such two architectures, and discover the performance of utilizing Skip-gram is slightly worse compared to using CBOW.

Keywords: Linked users, cross-site, E-commerce, matrix factorization. Micro blogs..

1. INTRODUCTION:

Within this paper, we study a fascinating problem of recommending products from e-commerce websites to users at social networks who don't have historic purchase records, i.e., in "cold-start" situations. We advise to make use of the linked users across social networks and e-commerce websites like a bridge to map users' social media features to latent features for product recommendation [1]. In specific, we advise learning both users' and products' feature representations from data collected from e-commerce websites using recurrent neural systems after which use a modified gradient boosting trees approach to transform users' social media features into user embeddings. Some e-commerce websites also offer the mechanism of social login, which enables new users to register using their existing login information from social media services for example Face book, Twitter or Google . We advise to use the recurrent neural systems for learning correlated feature representations for users and merchandise from data collected from your e-commerce website.

2. DESIGNED SCHEME:

Most studies only concentrate on constructing solutions within certain e-commerce websites and mainly utilize users' historic transaction records. To the very best of our understanding, mix-site cold-start product recommendation continues to be rarely studied before. We are seeing a sizable body of searching focusing particularly around the cold-start recommendation problem. Seroussi et al. suggested to utilize the data from users' public profiles and topics obtained from user generated content right into a matrix factorization model for brand new users' rating conjecture [2]. Zhang et al. propose a semi-supervised ensemble learning formula. Schein suggested a technique by mixing content and collaborative data within single probabilistic framework. Lin et al. addressed the cold-start problem for Application recommendation using the social information. Disadvantages of existing system: Their features only include gender, age and Face book likes, instead of a number of features explored within our approach. They don't consider how you can transfer heterogeneous information from social

networking websites right into a form that's ready to be used around the e-commerce side, the answer to address the mix-site cold-start recommendation problem.

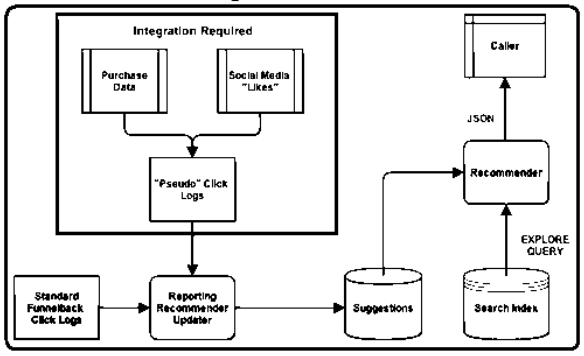


Fig.1.System architecture

3. IDEOLOGICAL SCHEME:

We known as this issue mix-site cold-start product recommendation. Within this paper, we study a fascinating problem of recommending products from e-commerce websites to users at social networks who don't have historic purchase records, i.e., in "cold-start" situations To deal with this concern, we advise to make use of the linked users across social networks and e-commerce websites like a bridge to map users' social media features to latent features for product recommendation [3]. Within our problem setting here, just the users' social media details are available which is a frightening task to change the social media information into latent user features which may be effectively employed for product recommendation. In specific, we advise learning both users' and products' feature representations from data collected from e-commerce websites using recurrent neural systems after which use a modified gradient boosting trees approach to transform users' social media features into user embeddings. Then we create a feature-based matrix factorization approach which could leverage the learnt user embeddings for cold start product recommendation. Benefits of suggested system: Our suggested framework is definitely good at addressing the mix-site cold-start product recommendation problem. We feel our study may have profound effect on both research and industry communities. We formulate a singular problem of recommending products from your e-commerce web site to social media users in "cold-start" situations. To the very best of our understanding, it's been rarely studied before. We advise to use the recurrent neural systems for learning correlated feature representations for users and merchandise from data collected from ane-commerce website. We advise an altered gradient boosting trees approach to transform users' micro blogging attributes to latent feature representation which may be easily incorporated for product recommendation. We advise and instantiate an element-based matrix factorization approach by user and product features for cold-start product recommendation.

System Fabrication: Recently, the limitations between e-commerce and social media have grown to be more and more blurred. Many e-commerce websites offer the mechanism of social login where users can sign up those sites utilizing their social networking identities for example their Face book accounts [4]. We'll study how you can extract micro blogging features and transform them right into a distributed feature representation before presenting an element-based matrix factorization approach, which includes the learned distributed feature representations for product recommendation. Because of the heterogeneous nature between both of these different data signals, information obtained from micro blogging services cannot usually be utilized directly for product recommendation on e-commerce websites. We formulate a singular problem of recommending products from your e-commerce web site to social media users in "cold-start" situations.

Micro blogging Qualities: We extract users' demographic attributes using their public profiles on SINA WEIBO. Demographic attributes happen to be proven to be really essential in marketing, particularly in product adoption for consumers. Prepare a summary of potentially helpful micro blogging attributes and construct the micro blogging feature vector Generate distributed feature representations and discover the mapping function. We predict a possible correlation

between text attributes and users' purchase preferences [5]. We consider two kinds of temporal activity distributions, namely daily activity distributions and weekly activity distributions. Word representations or embeddings learned using neural language models help addressing the issue of traditional bag-of word approaches which neglect to capture words' contextual semantics The main idea could be summarized the following. Given some symbol sequences, a set-length vector representation for every symbol could be learned inside a latent space by exploiting the context information among symbols, by which "similar" symbols is going to be mapped to nearby positions. When we treat each product ID like a word token, and convert the historic purchase records of the user right into a time placed sequence, we are able to then make use of the same techniques to learn product embeddings. The acquisition good reputation for a person can be viewed as like a "sentence" composed of the sequence of product IDs as word tokens. A person ID is positioned at the outset of each sentence, and both user IDs and product IDs are treated as word tokens inside a vocabulary within the learning process. The important thing idea is by using a small amount of linked users across sites like a bridge to understand the purpose which maps the initial feature representation au towards the distributed representation Gradient boosting algorithms try to provide an ensemble of weak mixers together form a powerful model inside a stage-wise process [6]. Once a characteristic is sampled, its corresponding attribute value features is going to be selected subsequently. We produce a super user embedding vector by averaging all available user embeddings. Second, we fit each dimension individually by having an individual MART model. According to our data analysis, we discovered that the of some dimensions in the same user may be correlated.

Cold-Start Product: Our idea may also be put on other feature-based recommendation algorithms, for example Factorization Machines. In conclusion, a person-product pair matches an element vector concatenated by global features, user features and product features. The concept is the fact that a person is more prone to purchase a merchandise that is closer within the unified latent feature space, and so the corresponding entry should get a bigger global bias value. The pair wise ranking model assumes the fitted value for that purchased method is bigger than the one which is not purchased with a user. Observe that all of the above ranking formulae don't use the consumer latent vector [7]. Recommendations that WEIBO users sometimes shared their purchase record on their own micro blogs using a system-generated short URL, which links towards the corresponding product entry on JINGDONG. all of the MART variants give similar results plus they perform consistently much better than the straightforward CART. Interestingly, when how big training data becomes smaller sized, MART sample and MART both outperforms MART old. We've the next observations: a) The written text attributes occupy the very best two rank positions7 b) Inside the demographic category, Gender and Interests tend to be more important than these. c) The social based attributes are rated relatively lower when compared to other two groups. For the methods, an essential component may be the embedding models, which may be set to 2 simple architectures, namely CBOW and Skip-gram.

4. CONCLUSION:

The mapped user features could be effectively integrated into an element-based matrix factorization method for cold-start product recommendation. We've built a sizable dataset from WEIBO and JINGDONG. The outcomes reveal that our suggested framework is definitely good at addressing the mix-site cold-start product recommendation problem. Within this paper, we've studied a singular problem, mix-site cold-start product recommendation, i.e., recommending products from e-commerce websites to micro blogging users without historic purchase records. We feel our study may have profound effect on both research and industry communities. Experimental results on the large dataset built

in the largest Chinese micro blogging service SINA WEIBO and also the largest Chinese B2C e-commerce website JINGDONG have proven the potency of our suggested framework. Presently, merely a simple neutral network architecture continues to be useful for user and product embeddings learning.

REFERENCES:

[1] Wayne Xin Zhao, Member, IEEE, Sui Li, Yulan He, Edward Y. Chang,Ji-Rong Wen, Senior Member, IEEE, and Xiaoming Li, Senior Member, IEEE, "Connecting Social Media to E-Commerce:Cold-Start Product Recommendation Using Microblogging Information", ieee transactions on knowledge and data engineering, vol. 28, no. 5, may 2016.

[2] Y. Zhang, G. Lai, M. Zhang, Y. Zhang, Y. Liu, and S. Ma, "Explicit factor models for explainable recommendation based on Phraselevel sentiment analysis," in Proc. 37th Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2014, pp. 83–92.

[3] Y. Seroussi, F. Bohnert, and I. Zukerman, "Personalised rating prediction for new users using latent factor models," in Proc. 22nd ACM Conf. Hypertext Hypermedia, 2011, pp. 47–56.

[4] N. N. Liu, X. Meng, C. Liu, and Q. Yang, "Wisdom of the better few: Cold start recommendation via representative based rating elicitation," in Proc. 5th ACM Conf. Recommender Syst., 2011, pp. 37–44.

[5] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, "You are who you know: Inferring user profiles in online social networks," in Proc. 3rd ACM Int. Conf. Web Search Data Mining, 2010, pp. 251–260.

[6] J. Lin, K. Sugiyama, M. Kan, and T. Chua, "Addressing cold-start in app recommendation: Latent user models constructed from twitter followers," in Proc. 36th Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2013, pp. 283–292.

[7] M. Giering, "Retail sales prediction and item recommendations using customer demographics at store level," SIGKDD Explor. Newsl., vol. 10, no. 2, pp. 84-89, Dec. 2008.

IMPLEMENTING A DENOISING HIGH QUALITY SENSING DEVICE TO INCREASE RELIABILITY

T Aswani[1]., U Sai Lakshmi[2]., B Nikitha [3]., G Thanuja[4]., P Swarna Monika[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- aswani.thummalagunta@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0561, 17RG1A0564, 17RG1A0577, 17RG1A05B0),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Within this paper, we explore the correlation between data of various models and offer two methods to monitor continuous holistic queries, one to get the precise solutions and yet another one for deriving the approximate results. Holistic queries are really as common as non-holistic queries. We evaluate this design through extensive simulations. Non-holistic queries, for example Count and Sum, share the decomposable characteristic. Existing approaches mostly are created for non-holistic queries like Average. However, it's not trivial to reply to holistic ones because of their non-decomposable property. Because of the limitation of message size, the merging process may lose some good info. We first propose two schemes in line with the data correlation between different models, with one to get the precise solutions and yet another one for deriving the approximate results. Because of the limitation of message size, the merging process may lose some good info. Generally, these techniques are only able to achieve approximate results with a few error guarantees by presenting different restricts and pruning algorithms around the data structure. Many prior attempts happen to be completed to create sophisticated data structures and algorithms which keep probably the most helpful information having a limited message size. The outcomes reveal that our approach considerably cuts down on the traffic cost in contrast to previous works while keeping exactly the same precision***

Keywords: Sensor networks, distributed data structures, holistic queries

1. INTRODUCTION:

Non-holistic queries usually provide a single result. Sensor systems are broadly utilized in various domains such as the intelligent transportation systems. Users issue queries to sensors and collect sensing data. Because of the poor sensing devices or random link failures, sensor data are frequently noisy [1]. To be able to boost the longevity of the query results, continuous queries are frequently employed. Within this work we concentrate on continuous holistic queries like Median. We advise a hybrid approach, mixing F-Bucket and wavelet-like approaches, to handle continuous holistic queries. Generally, aggregate queries could be classified into two different groups, non-holistic queries and holistic queries. Then we combine the 2 suggested schemes right into a hybrid approach that is adaptive towards the data altering speed. There are lots of variations between these two kinds of queries. When the sensor values in network are relatively stable, we apply a precise formula to calculate the precise median. Within the exact query approach, we use the bucket histogram that is referred as F (lexible)-Bucket, to obtain the exact answer for that query. Some other methods for example Manku etc. presented hybrid approximate algorithms for computing frequency counts over data streams [2].

2. PREVIOUS DESIGN:

Uncertainties may appear in both sensing data and queries. L-PEDAPs centered on routing tree construction and maintenance for query processing. For instance, Zhang et al. studied the issue of calculating the mixture as the query location is uncertain. Ye et al. suggested finding out possible query results of all imprecise sensing data. Yu et al. presented a technique which aiming at secure continuous aggregation querying [3]. Disadvantages of existing system: It will work better to obtain a median consequence of the monitoring area rather than derive a typical result, because the noise may modify the average result largely.

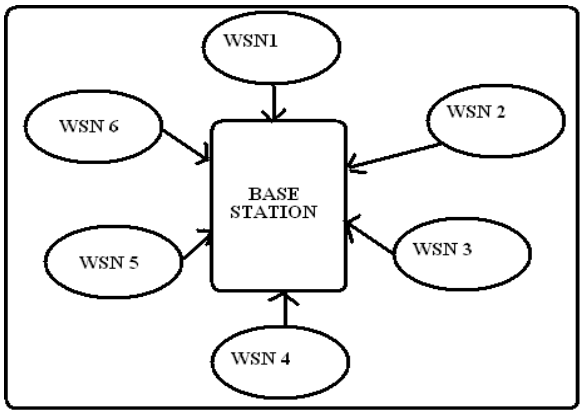


Fig.1.Enhanced system architecture

3. HOLISTIC SCHEME:

Within this paper, we explore the correlation between data of various models and offer two methods to monitor continuous holistic queries, one to get the precise solutions and yet another one for deriving the approximate results. Then, we advise a highly effective hybrid approach that adaptively selects appropriate one according to data altering speed and increases the performance of continuous queries. We advise a hybrid approach, mixing F-Bucket and wavelet-like approaches, to handle continuous holistic queries [4]. When the sensor values in network are relatively stable, we apply a precise formula to calculate the precise median. Once the data changes rapidly, our approach can adaptively change to the approximate formula. We advise a histogram-based method of get exact solutions for continuous queries. Particularly, we make use of the histogram summary structure to keep the worth distribution from the network. Each bucket within the histogram counts the amount of values inside a certain range. We advice two algorithms for refining the number assignment, Slip refining and Hierarchical refining. Benefits of suggested system: This merging process reduces transmissions at the expense of losing some good info. Finally, the sink aggregates all received AF-Buckets for an integrated one and calculates the query results. For that approximate plan, different quintiles could be directly calculated using the data distribution in AF-Bucket [5]. Generally, as both our exact and approximate schemes can return the information distribution of sensor values using F-Bucket and AF-Bucket correspondingly, many other kinds of queries could be clarified using the data distribution. The metric quantity of transmissions to judge the traffic price of each one of these approaches which is understood to be the entire size transmitted data packets in a single round.

Precise Query Method: We advise a hybrid approach, mixing F-Bucket and wavelet-like approaches, to handle continuous holistic queries. When the sensor values in network are relatively stable, we apply a precise formula to calculate the precise median. An easy method of get solutions for Q would be to retrieve all of the values from sensors, however, as pointed out before, this isn't energy-efficient. Thus, within this paper, we advise a histogram-based method of get exact solutions for continuous queries. Medium difficulty node receives F-Buckets from kids and merges all of them with its very own F-Bucket for an integrated one. Once the median value expires the ranges handled by these intermediate buckets, we have to adjust the number again. To be able to lessen the transmitted bytes, messages don't carry full F-Buckets only buckets that aren't empty. The refining process assigns more buckets towards the range in which the queried median is situated and adjust this assignment as the value distribution changes. This is done by subdividing the present range where median is situated. Finally, the majority of buckets are allotted to monitor this range and all of them is akin to something interval of length 1. Within this paper, we tackle one sort of popular queries, continuous holistic query, over sensor network. When compared to counterpart of this kind of query, non-holistic query, very little work continues to be done. However, holistic totally indeed essential for many sensor network applications to gather record data [6]. We still make use of the histogram summary to keep the data. Not the same as the precise query, each bucket within this structure stores the typical of several values and buckets are sorted by their values, which has similarities towards the formulation of Haar wavelet In every round, the leaf nodes

construct new AFBuckets and insert their values in. Then your AF-Buckets are sent to their parents. Within an intermediate node, the received AF-Buckets are incorporated together to become a built-in one.

Believed Query Formula: Within the Slip refining, we reckon that the median is based on the number next to current focused window and slip your window towards the adjacent range. However, when the median changes fast, we want multiple models to meet up with it. Within the Hierarchical refining, we first make use of an additional round to transfer the rough range covering median. Finally, in the sink we obtain an aggregated data structure, that we are able to run different queries. Merging of two AF-Buckets will forfeit information and cause error towards the query results. However, since our zero-padding and merging come from the AF-Bucket with smaller sized count towards the AF-Bucket with bigger count pair after pair, therefore the greatest AF-Bucket doesn't need to pad zeros. Our approach may also change to the precise query formula once the data altering is slow. To completely leverage the benefits of each method, within this work, we advise a singular metric named efficiency which models how rapidly the sensor value changes and it is impact on query processing. Since LIST and our Flexible Buckets algorithms both can offer the precise answer for median query, we simply evaluate their traffic cost [7]. We compare our approximate formula with Q-digest. Within this test, the proportion errors of both algorithms are positioned around 2 percent with appropriate parameter configuration. The experimental results reveal that the hybrid approach works more effectively in different conditions. The communication price of our approach is a lot less than Q-digest for different data altering rate, particularly when the sensor values change gradually, our hybrid method can help to eliminate the traffic cost greater than a half.

4. CONCLUSION:

We advise a highly effective hybrid approach that adaptively selects appropriate one according to data altering speed and increases the performance of continuous queries. We advise a histogram-based method of get exact solutions for continuous queries. Particularly, we make use of the histogram summary structure to keep the worth distribution from the network. Furthermore, we present a hybrid approach in line with the exact and approximation solutions, which applies the precise formula once the data altering rates are low and uses the approximation one once the rate becomes high. Experimental results reveal that the hybrid approach is capable of the same precision however with significantly less traffic cost when compared to other approximate methods. Within this paper, we take one typical query For instance, all Quintile queries could be solved by our approach with various parameters. Using the exact query plan, we have different quintiles by modifying the positioning of focused window during range refining process. Median for example as one example of our idea. To prevent delivering all of the sensing data to the sink, we advise two methods to monitor continuous holistic queries, a precise one, Flexible Bucket (F-Bucket), to reply to queries precisely along with a wavelet-like approximate one to get the results with small error. Actually, the suggested methods could be naturally extended to resolve other holistic queries.

REFERENCES:

[1] Kebin Liu, Member, IEEE, Lei Chen, Member, IEEE, Yunhao Liu, Fellow, IEEE,Wei Gong, Member, IEEE, and Amiya Nayak, Senior Member, IEEE, “Continuous Answering Holistic Queries overSensor Networks”, ieee transactions on parallel and distributed systems, vol. 27, no. 2, february 2016.

[2] L. Chih-Yu, P. Wen-Chih, and T. Yu-Chee, “Efficient in-network moving object tracking in wireless sensor networks,” IEEE Trans. Mobile Comput., vol. 5, no. 8, pp. 1044–1056, Aug. 2006.

[3] J. Hershberger, N. Shrivastava, S. Suri, and C. D. Toth, “Adaptive spatial partitioning for multidimensional data streams,” in Proc. 15th Annu. Int. Symp. Algorithms Comput., 2004, pp. 522–533.

[4] S. Madden, M. J. Franklin, J. Hellerstein, and W. Hong, “TAG: A Tiny AGgregation

service for ad-hoc sensor networks," in Proc. 5th Symp. Operating Syst. Design Implementation, 2002,
pp. 131–146.
[5] N. Shrivastava, C. Buragohain, D. Agrawal, and S. Suri, "Medians and beyond: New aggregation techniques for sensor networks," in Proc. 2nd ACM Conf. Embedded Netw. Sensor Syst, 2004, pp. 239–249.
[6] M. Ye, K. C. K. Lee, W. C. Lee, X. Liu, and M. C. Chen, "Querying uncertain minimum in wireless sensor networks," IEEE Trans. Knowl. Data Eng., vol. 24, no. 12, pp. 2274–2287, Dec. 2012.
[7] C. M. Chen, Y. H. Lin, Y. C. Lin, and H. M. Sun, "RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 4, pp. 727–734, Apr. 2012.

PARALLEL CRYPTOSYSTEM FOR PRIVATE FACTS RETRIEVAL WITHOUT REVEALING PROVIDER

K Prasanth Kumar[1]., E Tejaswini [2]., K Sai Tejaswi [3]., N Likitha [4]., Sk Farzana[5]
1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- kundaas@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A0575, 17RG1A0591, 17RG1A05A4, 17RG1A05B4),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: ***Location information collected from mobile users, knowingly and unknowingly, can reveal way over only a user's latitude and longitude. Within this paper, we study approximate k nearest neighbor queries in which the mobile user queries the place based company about approximate k nearest sights based on his current location. To evaluate the safety in our solutions, we define a burglar model web hosting kNN queries. The safety analysis has proven our solutions ensures both location privacy meaning the user doesn't reveal any details about his place to the LBS provider and query privacy meaning the user doesn't reveal which kind of POIs he's interested to the LBS provider. We think that the mobile user can buy his location from satellites anonymously, and also the base station and also the LBS provider don't collude to comprise the consumer location privacy or there is an anonymous funnel. RSA isn't a probabilistic file encryption plan. To change RSA to some probabilistic file encryption plan, we have to then add random bits in to the message m before encrypting m with RSA. The objective of doing this is to make sure that the mobile user can acquire just one kNN POIs per query. Additionally, when the mobile user can acquire a string of encrypted k nearest POIs within the response in the LBS server, he is able to frequently run the RR formula just with the LBS server to obtain a sequence of k nearest POIs without necessity of query generation and response generation. Performance has proven our fundamental protocol performs much well than the present PIR based LBS query protocols when it comes to both parallel computation and communication overhead.***

Keywords: RSA, Location based query, location and query privacy, private information retrieval, Paillier cryptosystem.

1. INTRODUCTION:

Within this paper, we study approximate k nearest neighbor queries in which the mobile user queries the place-based company about approximate k nearest sights based on his current location. LBS queries according to access control, mix zone and anonymity require company or even the middleware that maintains all user locations [1]. They're susceptible to misbehavior from the 3rd party. A reliable middleware relays between your mobile users and also the LBS provider. Before forwarding the place-based queries from the users towards the LBS, the middleware anonymizes their locations by pseudonyms. Fake dummy locations are generated randomly, and glued locations are selected from special ones for example road intersections. To beat the access pattern attacks, Elmehdwi et al. gave an answer for kNN query in line with the semantically secure Paillier file encryption, presuming two LBS servers exist, one getting the encrypted data and the other getting the understanding key. The aim would be to supply the LBS with searching abilities within the encoded data. Wong et al. propose a safe and secure point transformation, which preserves the relative distances of all of the database POIs to the query point. within the Response Retrieval (RR) formula, after acquiring the encrypted k nearest POIs, the mobile user needs the aid of the LBS server using the understanding from the k nearest POIs. The objective of our technique is to prevent independently evaluating distances that is difficult to do without revealing the position of the user [2]. Ghinita et al.'s protocol according to has two stages: retrieving the index from the cell in which the mobile user is situated while using Paillier cryptosystem and retrieving the POIs from the cell while using Kushilevitz-Ostrovsky PIR protocol

2. EXISTING SYSTEM:

Famous travel POIs and routes mostly are from four types of big social networking, Gps navigation trajectory, check-in data, geo-tags and blogs. However, general travel route planning cannot well meet users' personal needs. Personalized travel recommendation stands out on the POIs and routes by mining

user's travel records. The favorite technique is location-based collaborative filtering (LCF). To LCF, similar social users are measured in line with the location co-occurrence of formerly visited POIs. Then POIs are rated according to similar users' visiting records. However, existing studies haven't well solved the 2 challenges. For that first challenge, the majority of the travel recommendation works only centered on user topical interest mining but without thinking about other attributes like consumption capacity [3]. For that second challenge, existing studies focused more about famous route mining but without instantly mining user travel interest.

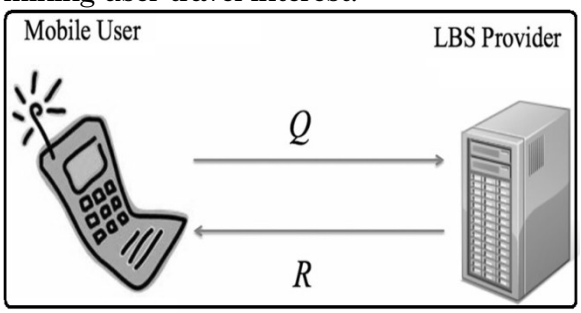


Fig.1.System framework

3. PROPOSED SYSTEM:

To deal with the difficulties pointed out above, we advise a Topical Package Model learning approach to instantly mine user travel interest from two social networking, community-contributed photos and travelogues. To deal with the very first challenge, we consider not just user's topical interest but the consumption capacity and preference of visiting some time and season [4]. Because it is hard to directly appraise the similarity between user and route, we develop a topical package space, and map both user's and route's textual descriptions towards the topical package space to obtain user topical package model (user package) and route topical package model (route package) under topical package space.

Implementation: It could reveal that he's interviewing for any job or "out" him like a participant in a gun rally or perhaps a peace protest. It may mean knowing that he/she spends time, and just how frequently. LBS queries according to dummy locations require mobile user at random to select some fake locations, to transmit the fake locations towards the LBS and also to get the false reports in the LBS within the mobile network. In contrast to existing solutions for kNN queries with location privacy, our option would be more effective. Experiments have proven our option would be simple for kNN queries. For that mobile user locating close to the border of two cells, he might query two cells round his location after which discover k nearest POIs one of the query responses. Current PIR-based LBS queries only permit the mobile user to discover k nearest POIs whatever the kind of POIs. The very first time, we look at the kind of POIs in kNN queries. LBS queries based geographic data transformation are vulnerable to access pattern attacks since the same query always returns exactly the same encoded results [5]. The very first time, we consider consecutive queries. Within our fundamental and generic kNN query protocols, the Paillier cryptosystem can be used to cover the kind t or even the type attributes (t1 t2 . . . tT) of POIs the mobile user has an interest in the LBS server. Particularly, our generic solution could be modified to help keep query privacy for partial type attributes. We provide a solution for that mobile user to question a string of POIs without necessity of multiple executions from the whole protocol. The safety from the blind understanding formula involves blindness. Without effort, the LBS server supplies a understanding plan to the mobile user within an encoded form not understanding either the actual input or even the real output. Our model concentrates on user location and query privacy protection from the LBS provider along with a kNN query protocol. The LBS provider provides location-based services towards the mobile user. Satellites supply the location information towards the mobile user. Personal Data Retrieval technique enables a person to retrieve an archive from the database server without revealing which record he's retrieving. PIR-based protocols are suggested for POI queries and made up of two stages. This

greatly increases the efficiency of consecutive queries. Security analysis has proven our protocols have location privacy, query privacy and knowledge privacy [6]. We break the semantic security from the Paillier plan. It's in contradiction using the assumption from the theorem. Our generic solution views a multi-dimension space where each POI is determined with location attributes. An approved user that offers the key transformation keys issues an encoded query towards the LBS. Both database and also the queries are unreadable through the LBS and, thus, location privacy remains safe and secure.

4. CONCLUSION:

To preserve query privacy, our fundamental solution enables the mobile user to retrieve one sort of POIs, for instance, approximate k nearest vehicle parks, without revealing towards the LBS provider which kind of points is retrieved. The primary variations between our previous work and our current paper are: 1) The prior work fixed the amount of nearest neighbor's k. The present work enables a variety of nearest neighbor's k as much as K, where K is a continuing 2) The prior work defined location privacy which implied query privacy. The present work defines location and query privacy individually 3) The prior work used the Rabin cryptosystem to avoid the mobile user to retrieve several data per query and didn't allow consecutive queries without multiple executions from the whole protocol. Our model views an area-based service scenario in mobile environments. We implemented our fundamental protocol and test its performance. The result of LBS queries according to k-anonymity depends heavily around the distribution and density from the mobile users, which, however, are past the charge of the place privacy technique. The suggested solutions mostly are built around the Paillier public-key cryptosystem and may provide both location and query privacy. The benefits of our work are 1) the machine instantly found user's and routes' travel topical preferences such as the topical interest, cost, some time and season, 2) we suggested not just POIs but additionally travel sequence, thinking about both recognition and user's travel preferences simultaneously. We found and rated famous routes in line with the similarity between user package and route package.

REFERENCES:

[1] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 699–726, 2010.

[2] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in Proc. 10th Int. Conf. Adv. Spatial Temporal Databases, 2007, pp. 239–257.

[3] C. Y. Chow, M. F. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based services," in Proc. 14th Annu. ACM Int. Symp. Adv. Geograph. Inform. Syst., 2006, pp. 171–178.

[4] R. Michael, "Digitalized signatures and public-key functions as intractable as factorization," MIT Lab. Comput. Sci., Cambridge, MA, US, Tech. Rep. MIT-LCS-TR-212, Jan. 1979.

[5] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location- based services with SybilQuery," in Proc. 11th Int. Conf. Ubiquitous Comput., 2009, pp. 31–40.

[6] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2009, pp. 139–152.

SUBSTANCE CATALOGING USING LEGEND IMPLANTED VECTOR SPACE

Deepika M Deepika [1]., Chiluveri Bhavana [2]., Mudedla Shreya [3]., Racherla Kavya Sri [4]., Sheri Sanjana Reddy [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- ynraju2003@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (17RG1A05J4, 17RG1A05K0, 17RG1A05K4, 17RG1A05K6), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

In comparison to tree-like indexes used in current works, our index receptives to dimensional growth and scales well with multi-dimensional results. Unwanted applicants are cut according to the lengths of points or keywords between MBRs and also the best-found diameter. NKS queries are useful to a range of applications such as social systems picture conversation, graph model search, GIS geolocation, etc. We provide both an exact version of the formulation and a rough one. We consider objects with key word labels and are therefore baked in a vector space in this article. Keyword focused searches in multidimensional text-rich databases have a wide variety of creative techniques and technology. Of these data sets we search questions which demand validated categories of keywords for the tightest groups of points. Our experimental results on human and artificial datasets demonstrate that ProMiSH can speed up up as many as 60 instances of tree-based conditions. Our special ProMiSH method, which uses random projection and hatch-based index systems, guarantees high degree of scalability and acceleration. We perform comprehensive experimental tests to show the effects of the procedures suggested.

Keywords— Projection and Multi Scale Hashing, Querying, multi-dimensional data, indexing, hashing.

1. INTRODUCTION

The NKS should contain entirely any user-provided keywords and k data point teams since all versions provide the keywords of query and type on the tightest cluster on the multi-dimensional space. The query is triggered by the query. A two-dimensional NKS question of data points. In this paper we look at multi-dimensional datasets with some keywords in each data point. In the functional space, the presence of keywords allows mass in new instruments to query these multi-dimensional datasets and investigate these. There are a number of keywords [1] on each point. The presence of keywords in space allows mass to be added to new methods for questioning and exploring these multi-dimensional datasets. NKS queries are useful for many uses, such as social systems picture discussion, diagram pattern search, GIS geolocation search, etc. NKS queries are useful when searching graphic patterns, in which labelled graphs root within the high scalability space. In that context, an NKS query within the embedded space could clarify the search for a subgraphic with such defined labels. Likewise, an NKS search with a high known diameter retrieves the best candidates. If the diameters of two candidates are equal, their cardinality scored them further. Our empirical findings indicate that such algorithms can take hours to finish with a multi-dimensional dataset of innumerable points. There is thus an excuse for a qualified formula that scales with the dimension of a dataset and gives massive datasets functional productivity in querying. To do a regional search ProMiSH-E uses some hash tables and inverted indexes. The Hashing Technique is motivated by Responsive Relief (LSH), an advanced means of locating the closest neighbour in large fields. A single search round of the hash table results in sub-punkte containing query results and ProMiSH-E searches each sub-panel using a fast-tapping method. For a greater space and time performance ProMiSH-A is certainly an estimated improvement in the ProMiSH-E. We test ProMiSH's output on actual and artificial datasets and rehearse VbR-Tree and CoSKQ as simple guidelines.[2] We evaluate this performance.

2. TRADITIONAL METHOD:

Location-specific keyword queries web within the GIS systems were earlier clarified using a mix of R-Tree and inverted index. Felipeet al. developed IR2-Tree to position objects from spatial datasets with different mixture of their distances towards the query

locations and also the relevance of the text descriptions towards the query keywords. Cong et al. integrated R-tree and inverted file to reply to a question much like Felipeet al. utilizing a different ranking function. Disadvantages of existing system: They don't provide concrete guidelines regarding how to enable efficient processing for the kind of queries where query coordinates are missing. In multi-dimensional spaces, it is not easy for users to supply significant coordinates, and our work handles another kind of queries where users are only able to provide keywords as input. Without query coordinates, it is not easy to evolve existing strategies to our problem. Observe that an easy reduction that treats the coordinates of every data point as you possibly can query coordinates suffers poor scalability.

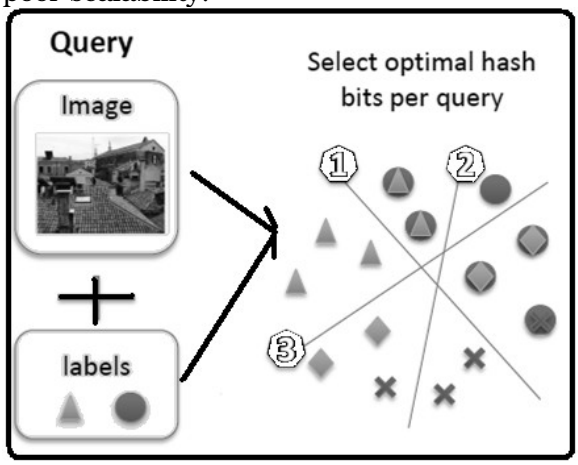


Fig.1.System Framework

3. UNIQUE APPROACH:

Within this paper, we study nearest keyword set queries on text-wealthy multi-dimensional datasets. An NKS totally some user-provided keywords, and caused by the query can include k teams of data points because both versions contains all of the query keywords and forms among the top-k tightest cluster within the multi-dimensional space. Within this paper, we consider multi-dimensional datasets where each data point has some keywords. This can lead to an exponential quantity of candidates and enormous query occasions. Virtual bR*-Tree is produced from the pre-stored R*-Tree. Therefore, Ikp could be stored on disk utilizing a directory-file structure. The existence of keywords in feature space enables to add mass to new tools to question and explore these multi-dimensional datasets. Within this paper, we advise ProMiSH to allow fast processing for NKS queries. Particularly, we develop a precise ProMiSH have a tendency to retrieves the perfect top-k results, as well as an approximate ProMiSH that's more effective when it comes to space and time, and has the capacity to obtain near-optimal leads to practice [3]. ProMiSH-E uses some hash tables and inverted indexes to carry out a localized search. Benefits of suggested system: Better space and time efficiency. A singular multi-scale index for exact and approximate NKS query processing. It's a competent search algorithm that actually work using the multi-scale indexes for fast query processing.

Methodology: The index includes two primary components. Inverted Index Ikp. The very first component is definitely an inverted index known as Ikp. In Ikp, we treat keywords as keys, and every keyword suggests some data points which are connected using the keyword. Hash table-Inverted Index Pairs HI. The 2nd component includes multiple hash tables and inverted indexes known as HI. All of the three parameters are non-negative integers. we present looking algorithms in ProMiSH-E that finds top-k recent results for NKS queries. We produce a formula for locating top-k tightest clusters inside a subset of points. A subset is acquired from the hash table bucket. Points within the subset are categorized in line with the query keywords. Then, all of the promising candidates are explored with a multi-way distance join of those groups. The join uses rk, the diameter from the kth result acquired to date by ProMiSH-E, because the distance threshold. An appropriate ordering from the group's results in a competent candidate exploration with a multi-way distance join. We first execute a pair wise inner joins from the groups with distance threshold rk. In inner join, a set of points from two groups are became a member of only when the space

together reaches most rk. Therefore, an effective groups results in a highly effective pruning of false candidates. Optimal ordering of groups for that least quantity of candidate's generation is NP-hard. We advise a greedy approach to obtain the ordering of groups. We explain the formula having a graph Groups fa, b, cg are nodes within the graph. The load of the edge may be the count of point pairs acquired by an inner join from the corresponding groups. The greedy method starts by selecting an advantage getting minimal weight. Should there be multiple edges with similar weight, then an advantage is chosen randomly. We execute a multi-way distance join from the groups by nested loops. An applicant is located whenever a tuple of size q is generated. If your candidate getting a diameter smaller sized compared to current worth of rk is located, then your priority queue PQ and the need for rk are updated. The brand new worth of rk can be used as distance threshold for future iterations of nested loops. Generally, ProMiSH-A is much more space and time efficient than ProMiSH-E, and has the capacity to obtain near-optimal leads to practice [4]. The index structure and also the search approach to ProMiSH-An act like ProMiSH-E therefore, we simply describe the variations together. The index structure of ProMiSH-A is different from ProMiSH-E when it comes to partitioning projection space of random unit vectors. ProMiSH-A partitions projection space into non-overlapping bins of equal width, unlike ProMiSH-E which partitions projection space into overlapping bins. Therefore, each data point o will get one bin id from the random unit vector z in ProMiSH-A. Just one signature is generated for every point o through the concatenation of their bin ids acquired from each one of the m random unit vectors. Each point is hashed right into a hash table having its signature. Looking formula in ProMiSH-A is different from ProMiSH-E within the termination condition. ProMiSH-A checks for any termination condition after fully exploring a hash table in a given index level: It terminates whether it has k records with nonempty data point takes hold its priority queue PQ. We index data points in D by ProMiSH-A, where each data point is forecasted onto m random unit vectors. The projection space of every random unit vector is partitioned into non-overlapping bins of equal width w. We evaluate the query time complexity and index space complexity in ProMiSH. Our evaluation employs real and artificial datasets. The actual datasets are collected from photo-discussing websites. We crawl images with descriptive tags from Flicker after which these images are changed into grayscale. We suggested a singular index known as ProMiSH according to random projections and hashing [5]. Within this paper, we suggested methods to the issue of top-k nearest keyword set search in multi-dimensional datasets. According to this index, we developed ProMiSH-E that finds an ideal subset of points and ProMiSH-A which searches near-optimal results with better efficiency. We generate synthetic datasets to judge the scalability of ProMiSH. Particularly, the information generation process is controlled by the parameters. We generate NKS queries legitimate and artificial datasets. Generally, the query generation process is controlled by two parameters: (1) Keywords per query q decides the amount of keywords in every query and (2) Dictionary size U signifies the entire quantity of keywords inside a target dataset. We apply real datasets to show the potency of ProMiSH-A. Given some queries, the response duration of a formula is understood to be the typical period of time the formula spends in processing one query. We use memory usage and indexing time because the metrics to judge the index size for ProMiSH-E and ProMiSH-A. Particularly, Indexing time signifies how long accustomed to build ProMiSH variants.

3. LITERATURE SURVEY:

Cao et al. and Lengthy et al. suggested algorithms to retrieve several spatial web objects so that the group's keywords cover the query's keywords and also the objects within the group are nearest towards the query

location and also have the cheapest inter-object distances. Our work differs from them. First, existing works mainly concentrate on the kind of queries in which the coordinates of query points are known [6]. The suggested techniques use location information as a vital part to carry out a best first explore the IR-Tree, and query coordinates play a simple role in almost all the algorithms to prune looking space. Though it may be easy to make their cost functions same towards the cost function in NKS queries, such tuning doesn't change their techniques. Second, in multi-dimensional spaces, it is not easy for users to supply significant coordinates, and our work handles another kind of queries where users are only able to provide keywords as input. Third, we create a novel index structure according to random projection with hashing. Unlike tree-like indexes adopted in existing works, our index is less responsive to the rise of dimensions and scales well with multi-dimensional data. Undesirable candidates are pruned in line with the distances between MBRs of points or keywords and also the best found diameter. However, the pruning techniques become ineffective with a rise in the dataset dimension as there's a sizable overlap between MBRs because of the curse of dimensionality. Both bR*-Tree and Virtual bR*-Tree, are structurally similar, and employ similar candidate generation and pruning techniques [7]. Memory usage grows gradually both in ProMiSH-E and ProMiSH-A when the amount of dimensions in data points increases. ProMiSH-A is much more efficient than ProMiSH-E when it comes to memory usage and indexing time. Therefore, Virtual bR*-Tree shares similar performance weaknesses as bR*-Tree. Our problem differs from nearest neighbor search. NKS queries provide no coordinate information, and aim to obtain the top-k tightest clusters which cover the input keyword set. Observe that VbR_-Tree and also the CoSKQ based method are excluded out of this experiment given that they mainly support top-1 search.

4. CONCLUSIONS:

A suitable order from the party results in an exploration by qualified candidate with a multi-way reach. In addition, our methods are well balanced by actual and artificial datasets. We intend to examine the ProMiSH disc extension. Sequentially ProMiSH-E reads only buckets required by Ikp for location of points with at least one keyword query. Our observational findings indicate that ProMiSH is faster than state-of-the-art tree-based technology, with efficiency gains in many orders. But the techniques of tailoring become useless as the dimension of the dataset increases as the dimensionality is largely overlapping between MBRs. Therefore, both hash tables and HI inverted indexes can be saved using a layout of a directory like Ikp again and a B-trree can be stored with all kinds of points within a dataset that use their ids to store them across the drive. Moreover, ProMiSH-E samples HI data structures from the smallest scale sequentially to construct the candidate point ids for that subset scan, and only reads buckets necessary in the hash-table and even the inverse HI structure index.

REFERENCES:

[1] Vishwakarma Singh, Bo Zong, and Ambuj K. Singh, “Nearest Keyword Set Search inMulti-Dimensional Datasets”, ieee transactions on knowledge and data engineering, vol. 28, no. 3, march 2016.

[2] X. Cao, G. Cong, C. S. Jensen, and B. C. Ooi, “Collective spatial keyword querying,” in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2011, pp. 373–384.

[3] I. De Felipe, V. Hristidis, and N. Rishe, “Keyword search on spatial databases,” in Proc. IEEE 24th Int. Conf. Data Eng., 2008, pp. 656–665.

[4] R. Hariharan, B. Hore, C. Li, and S. Mehrotra, “Processing spatialkeyword (SK) queries in geographic information retrieval (GIR) systems,” in Proc. 19th Int. Conf. Sci. Statistical Database Manage., 2007, p. 16.

[5] R. Weber, H.-J. Schek, and S. Blott, "A quantitative analysis and perfomance study for similarity-search methods in high-dimensional spaces," in Proc. 24th Int. Conf. Very Large Databases, 1998, pp. 194–205.
[6] Y. Tao, K. Yi, C. Sheng, and P. Kalnis, "Quality and efficiency in high dimensional nearest neighbor search," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2009, pp. 563—576.
[7] N. Beckmann, H.-P. Kriegel, R. Schneider, and B. Seeger, "The R*-tree: An efficient and robust access method for points and rectangles," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 1990, pp. 322–331.

A SYMMETRIC HIDDEN SCRIPT SCHEME FOR ENABLING SEARCH POLICY IN OPEN NETS

Bonthu Prasad[1]., Pavuluri Vijetha Chowdary [2]., S. Rajeshwari [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- prasadb31@gmail.com)
2, 3 B.Tech IV Year CSE, (17RG1A05K3, 18RG5A0504),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

This focuses on scanning encrypted records, which is an important way to encrypt files in the cloud or, in most instance, in a networked information system where servers are not completely secure, in anticipation of outsourcing. We formally show that our proposed strategy is safe selectively from chosen keyword attacks. In order to help multiple data consumers and various data contributors we design a unique and flexible, supported keyword search for encrypted data plans. Inside our architecture we discern attributes and keywords. Keywords are the real file content, while attributes correspond to user qualities. Furthermore, the proposed strategy is much better fit for the cloud outsourcing paradigm and is efficiently revoked through proxy reencryption and lazy re-file encryption techniques. In comparison to the current keyword search plan which is accepted for public use, our plan will concurrently achieve scalability and fineness. Not the same as our predicative file encryption search plan, our plan makes a randomly organised search for an accepted keyword. In contrast to the number of allowed users, look complexity is a straight line with the number of attributes within the scheme. This is why, for a large structure like the cloud, the one-to-many approval process is much more fitting. Our proposed ABKS-UR strategy and mechanism for verifying results by real-world data set and the difficulty of asymptotic computing in relation to combinations process.

Keywords— Attribute-based keyword search, fine-grained owner-enforced search authorization, multi-user search.

1. INTRODUCTION

File security is now regarded as a fundamental means of preserving the safety of users from the cloud server prior to outsourcing. By fine grain, we say that search authorization is regulated by the file level granularity. The high complexity of hidden key management simply does not provide for the symmetric cryptography schemes. PKC based search schemes can provide much more versatile and important searches[1] as opposed to symmetrical search methods. The Clubpenguin-ABE permits private user response to be linked by a communication structure with certain attributes and ciphertext. When you do an access control system inside a broadcast atmosphere, Clubpenguin-ABE is also the preferred alternative. In the public-key context, Hwang and Lee presented a multi user-specific search plan for conjunctive keywords. Sun and others recently introduced a multi-keyword text-search strategy for search outcome authentication by authenticating the proposed stable index tree. By using the re-file encryption proxy, Yu et al. have created a selectively protected Clubpenguin-ABE with ale's revocation attribute. User permission should be applied to allow multiple users seeking capabilities. Data owners generate a keyword index in the register, but securing the index only according to the features of the authorised user, through a permission structure[2]. Cao et al. proposed a first multi-keyword search strategy for encrypted cloud data with the help of "coordinate match," which preserves the anonymity of the search feature. to improve search features.

2. CLASSIC APPROACH:

There's been a curiosity about developing attribute based encryption due to the fine-grained access control property. Goyal et al. designed the very first key policy attribute-based file encryption plan, where ciphertext could be decrypted only when the attributes that can be used for file encryption fulfill the access structure around the user private key. Underneath the reverse situation, Clubpenguin-ABE enables user private answer to be connected with some attributes and ciphertext connected by having an access structure. Clubpenguin-ABE is really a preferred choice when making an access control mechanism inside a broadcast atmosphere. Cheung and Newport suggested a selectively secure Clubpenguin-ABE

construction within the standard model while using simple Boolean function, i.e., AND gate. By adopting proxy re-file encryption and lazy re-file encryption techniques, Yuet al. also devised a selectively secure Clubpenguin-ABE plan with ale attribute revocation that is perfectly appropriate for that data-outsourced cloud model. Disadvantages of existing system: The encrypted data could be effectively utilized then becomes another new challenge. Significant attention continues to be given and far effort has been created to deal with this problem, from secure search over encrypted data, secure function evaluation, to completely homomorphic file encryption systems that offer generic means to fix the issue theoretically but they are still too much from being practical because of the very high complexity. Symmetric cryptography based schemes are clearly not appropriate with this setting because of the high complexity of secret key management [3]. Extending user list method of the multi-owner setting as well as on a per file basis isn't trivial because it would impose significant scalability issue thinking about a possible many users and files based on the machine. Additional challenges include how to deal with the updates from the user lists within the situation of user enrollment, revocation, etc., underneath the dynamic cloud atmosphere.

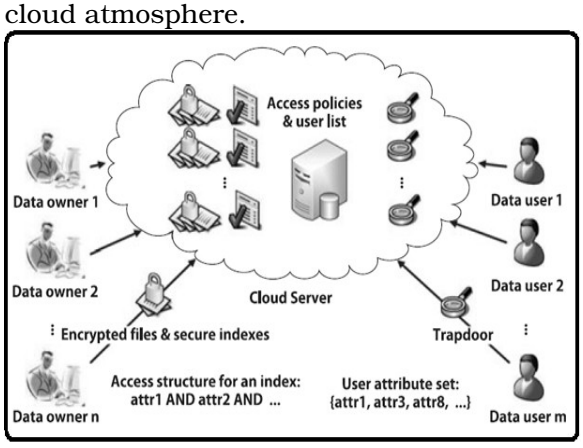


Fig.1.System Framework

3. ARTICULATED DESIGN:

This paper concentrates on the issue of search over encrypted data, which is a vital enabling way of the file encryption-before-outsourcing privacy protection paradigm in cloud-computing, or perhaps in general in almost any networked information system where servers aren't fully reliable. Within this paper, we address these open issues and offer an approved keyword search plan over encrypted cloud data with efficient user revocation within the multi-user multi-data-contributor scenario [4]. We understand fine-grained owner-enforced search authorization by exploiting ciphertext policy attribute-based file encryption (Clubpenguin-ABE) technique. Particularly, the information owner encrypts the index of every file by having an access policy produced by him, which defines which kind of users can search this index. The information user generates the trapdoor individually without counting on an always online reliable authority (TA). The cloud server can search within the encrypted indexes using the trapdoor on the user's account, after which returns matching result if and just when the user's attributes connected using the trapdoor fulfill the access policies baked into the encrypted indexes. We differentiate attributes and keywords within our design. Keywords are actual content from the files while attributes make reference to the qualities of users. The machine only keeps a small group of attributes for search authorization purpose. Data proprietors produce the index composed of keywords within the file but secure the index by having an access structure only in line with the features of approved users, making the suggested plan more scalable and appropriate for that massive file discussing system. To be able to further release the information owner in the troublesome user membership management, we use proxy re-file encryption and lazy re-file encryption strategies to shift the workload whenever possible towards the CS, through which our suggested plan enjoys efficient user revocation. Benefits of suggested system: Formal security analysis implies that the suggested plan is provably secure and meets various search privacy needs. In addition, we design searching result verification plan making the whole search

process verifiable. Performance evaluation demonstrates the efficiency and functionality from the ABKS-UR. We design a singular and scalable approved keyword search over encrypted data plan supporting multiple data users and multiple data contributors [5]. In contrast to existing works, our plan supports fine-grained owner-enforced search authorization in the file level with better scalability for big scale system for the reason that looking complexity is straight line to the amount of attributes within the system, rather of the amount of approved users. Data owner can delegate the majority of computationally intensive tasks towards the CS, making the consumer revocation process efficient and it is more appropriate for cloud outsourcing model. We formally prove our suggested plan selectively secure against selected-keyword attack. We advise a plan to allow authenticity check within the came back search increase the risk for multi-user multi-data-contributor search scenario.

Topological Framework: A reliable authority is unconditionally assumed to manage generating and disbursing public keys, private keys, and reencryption keys. We think that the CS honestly follows the designated protocol, but strangely enough infers additional privacy information in line with the data open to him. Another essential design goal would be to efficiently revoke users in the current system while minimizing the outcome around the remaining legitimate users. However, we result in the whole search process verifiable and knowledge user can tell from the authenticity from the came back Google listing. We formally prove the suggested plan semantically secure within the selective model [6]. A naive option would be to impose the responsibility on every data owner. Consequently, data owner is needed to become always online to quickly respond the membership update request that is impractical and inefficient. Within the search phase, the CS returns looking result combined with the auxiliary information for result authenticity check later through the data user. The machine level operations include System Setup, New User Enrollment, Secure Index Generation, Trapdoor Generation, Search, and User Revocation. For Google listing verification, the hash operation is going to be counted for it's the primary computation cost there. The primary concept of the verification plan would be to permit the CS to come back the auxiliary information that contains the authenticated data structure apart from the ultimate Google listing, where the information user is able to do result authenticity check [7]. When the data user queries a keyword looked before, the CS is only going to return looking result and also the user will verify them by examining the search history.

4. CONCLUSION:

To manage outsourced data in the cloud, we create an authenticated data structure using the flower filters, inverted indices, and hash & signature strategies. Our strategy helps multiple owners to protect and migrate their data independently to the cloud server. Without a reputable online authority, users can create their own search capabilities. The owner-enforced access policy around the index of each file can also introduce fine-grained search authorization. We may then achieve the authentication architecture objectives, i.e., accuracy and integrity. By adding time marks to the associated signatures, freshness may be recognised. Unlike current work, our proposal promotes fine grained owner-enforced file level search permissions with improved scale-up for large-scale applications because look-ahead sophistication lies specifically with the number of attributes within the system and is more compatible with the number of permitted users. We are aware that the owner has a fine-grained search authorization by using the Ciphertext policy-based Clubpenguin-ABE technique of encryption of the file. We develop a search results authentication strategy in order to build trust for the knowledge user inside the recommended stable search system.

REFERENCES:

[1] Wenhai Sun, Student Member, IEEE, Shucheng Yu, Member, IEEE,Wenjing Lou, Fellow, IEEE, Y. Thomas Hou, Fellow, IEEE, and Hui Li, Member, IEEE, "Protecting Your Right: Verifiable Attribute-BasedKeyword Search with Fine-GrainedOwner-Enforced Search Authorizationin the Cloud", ieee transactions on parallel and distributed systems, vol. 27, no. 4, april 2016.

[2] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. 27th Annu. Int. Conf. Adv. Cryptol. Theory Appl. Cryptograph. Techn., 2008, pp. 146–162.

[3] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. 2nd USENIX Conf. File Storage Technol., 2003, vol. 42, pp. 29–42.

[5] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 11, pp. 3025–3035, Nov. 2014.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001, pp. 213–229.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE Conf. Comput. Commun., 2010, pp. 1–9

ITEM STATUS FORECAST METHOD FOR USERS WILLING

Naresh Katkuri[1]., Kancharana Gayathri [2]., V K S Sarayu [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- nareshk501@gmail.com)
2, 3 B.Tech IV Year CSE, (17RG1A05J7, 17RG1A05K7),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

We focus on the speculation task of scoring. But material at user level is not generally available on certain platforms for analysis. Therefore, in web mining, machine learning and natural language analysis, how you can review and how you can relate to social systems reviewers becomes an important issue. According to the user's feeling, if two goods with the same distribution, they have the same status and would be released with the same reviews. The most basic and critical factor for the elimination of consumer expectations is emotion analysis. The opinion in the reviews is important to obtain the status of the commodity. In general, the product may be higher in status in any degree if item reviews show a favorable feeling. We use the feeling of social consumers in our work to deduce evaluations. From reading consumer feedback, we extract product functionality. Then we know the feeling terms used to characterize the characteristics of the goods. Some websites, however, do not often have organized information and each methodology does not exploit unstructured information from users. Experts to identify new guidelines as well as relevant ones. They are able to recommend particular experts to those target customers in accordance with the customer environment by evaluating market ratings. We will primarily like to obtain the product/item/service functionality and certain designated individuals. LDA is also a Bayesian algorithm used to model the links between feedback, topics and vocabulary. We conduct a variety of tests to test consumer feelings for results in our ranking conjecture model. Our approach uses the current Yelp dataset templates to assess results.

Keywords— Ratings, sentiment distribution, item reputation, Reviews, Rating prediction, Recommender system, Sentiment influence, User sentiment

1. INTRODUCTION

In general, the user's attitude towards goods can be explained by feeling. We understand that statistical ratings instead of binary judgments are more important in a variety of realistic situations. We suggest a nostalgic approach to social users and we measure a product/product feeling for each user. Some systems are also proposed to be scalable. For example, we look at the manner in which they have found feeling among the friends of users. The user-based CF formula proposed [1] [2] will potentially be the most popular CF algorithms. The spread of trust remains a key factor in the study of social networking and confidence-based recommendation. Whenever we browse the Internet, we are most interested with people who have written five-star ratings or negative reviews. The theory of confidence networks in social systems is being suggested by Yang et al. Including numerous product analysis considerations including product quality content, review time, product longevity and previously older positive proof. Zhang et al. They present an item classification model that uses weighs to determine the rating score for product review variables. For the opinionated set of text in almost any region, the suggested structure is very general and specific. In an examination of the many topical aspects Wang et al. assess consumer views of a successful organisation. In addition, the interaction between the user and friends creates new names such as interpersonal feeling effect, representing the influence of user buddies within a sentimental position [2].

2. TRADITIONAL DESIGN:

Sentiment analysis could be conducted on three different levels: review-level, sentence-level, and phrase-level. Review-level analysis and sentence-level analysis make an effort to classify the sentiment of a complete review to among the predefined sentiment polarities, including positive, negative and often neutral. While phrase-level analysis make an effort to extract the sentiment polarity of every feature that the user expresses his/her attitude towards the specific feature of the specific product. Zhang et al. propose a self-supervised and lexicon-based sentiment classification

method of determine sentiment polarity of the review which contains both textual words and emoticons. Plus they use sentiment for recommendation. Lee et al. propose a recommender system using the idea of Experts to locate both novel and relevant recommendations [4]. By analyzing the consumer ratings, they are able to recommend special experts to some target user in line with the user population. Disadvantages of existing system: The present work mainly concentrates on classifying users into binary sentiment, and they don't go further in mining user's sentiment. The present approaches mainly leverage product category information or tag information to review the interpersonal influence. These techniques are restricted around the structured data, which isn't always on some websites. However, reading user reviews can offer us ideas in mining interpersonal inference and user preferences.

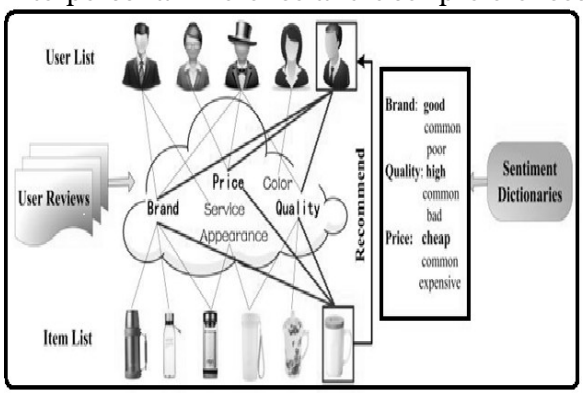


Fig.1.Proposed system structure

3. SENTIMENT-BASED SCHEME:

We advise a sentiment-based rating conjecture method within the framework of matrix factorization. Within our work, we utilize social users' sentiment to infer ratings. First, we extract product features from reading user reviews. Then, we understand the sentiment words, which are utilized to describe the merchandise features. Besides, we leverage sentiment dictionaries to calculate sentiment of the specific user with an item/product. The primary contributions in our approach are listed below: We advise a person sentimental measurement approach, which is dependent on the found sentiment words and sentiment degree words from reading user reviews. We utilize sentiment for rating conjecture. User sentiment similarity concentrates on the consumer interest preferences. User sentiment influence reflects the way the sentiment spreads one of the reliable users. Item status similarity shows the possibility relevance of products [5]. We fuse the 3 factors: user sentiment similarity, interpersonal sentimental influence, and item status similarity right into a probabilistic matrix factorization framework to handle a precise recommendation. The experimental results and discussions reveal that user's social sentiment that people found is really a main factor in improving rating conjecture performances. Benefits of suggested system: Within our paper, we not just mine social user's sentiment, but additionally explore interpersonal sentimental influence and item's status. Finally, we take these in to the recommender system. The objective of our approach is to locate effective clues from reviews and predict social users' ratings. We fuse user sentiment similarity, inter personal sentiment influence, and item status similarity right into a unified matrix factorization frame work to offer the rating conjecture task.

Suggested Implementation: To create the vocabulary, we first of all regard each user's review as an accumulation of words without thinking about an order. Only then do we remove "Stop Words", "Noise Words" and sentiment words, sentiment degree words, and negation words. We extend HowNet Sentiment Dictionary to calculate social user's sentiment on products [6]. The present work mainly concentrates on classifying users into binary sentiment, and they don't go further in mining user's sentiment. Within our paper, we merge the positive sentiment words list and positive evaluation words listing of HowNet Sentiment Dictionary into one list, and referred to it as POS-Words When the sentiment word is preceded by a strange quantity of negative prefix words inside the specified zone, we turn back sentiment polarity. The language like "acclamation", "pleasure", and "happiness" is going to be collected into POS-words of SD, the language like "noise", "stink", and "mistake" is

going to be collected into Neg-words of SD. Based on information theory, large variance means the enormous information. Therefore, the reviews with increased information may have more influence. Within our work, we assume item's status cannot directly reflect its real ratings. We leverage users' sentiment distribution to infer item's status [7]. The proportion figures in every cell would be the relative enhancements of RPS within the various baseline models. It's clearly proven our RPS model outperforms all of the baseline models in every group of Yelp. This experiment shows a sizable amount of differentiation backward and forward types of users, which shows RPS is extremely special and efficient.

4. CONCLUSION:

First of all, we derive product characteristics from the analysis corpus, then we add a tool for evaluating the sentiment of social consumers. Furthermore, 3 sentimental factors are identified. User interest rates are generally constant over a nutshell period such that review user topics will be reflective. The goal is to find successful hints from feedback and to forecast the ratings of social users. It is important to know how to gather useful knowledge from feedback in order to make an accurate decision for a customer. User friends are always trustworthy. If your consumer and condition buddies have common tastes of interest, then Orshe will have the same attitudes to this object. The power of interpersonal feeling is implemented in the first word, which means that the client will trust him/her more when your friend from the customer has apparent likeness and annoyance. In order to purchase decisions, buyers need not only to consider if the system is successful but also how good the goods are. It is often accepted that different individuals may have different tastes for sentimental language. We do a review of the 3 sentimental considerations on Yelp's real world dataset.

REFERENCES:

[1] Xiaojiang Lei, Xueming Qian, Member, IEEE, and Guoshuai Zhao, "Rating Prediction based on Social Sentiment from Textual Reviews", ieee transactions on multimedia, 2016.

[2] Z. Zhao, C. Wang, Y. Wan, Z. Huang, J. Lai, "Pipeline item-based collaborative filtering based on MapReduce," 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, 2015.

[3] Z. Zhao, C. Wang, Y. Wan, Z. Huang, J. Lai, "Pipeline item-based collaborative filtering based on MapReduce," 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, 2015.

[4] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, 2015, pp. 340-352.

[5] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, 2015, pp. 340-352.

[6] B. Wang, Y. Min, Y. Huang, X. Li, F. Wu, " Review rating prediction based on the content and weighting strong social relation of reviewers," in Proceedings of the 2013 international workshop of Mining unstructured big data using natural language processing, ACM. 2013, pp. 23-30.

[7] B. Sarwar, G. Karypis, J. Konstan, and J. Reidl, "Item-based collaborative filtering recommendation algorithms," in Proc.10th International Conference on World Wide Web, 2001, pp. 285-295.

CORRELATION-AWARE EXTRACTION STRATEGY FOR HIGH FRACTIONS OF INFORMATION

Santhosh Kumar Potnuru[1]., Baddam Soujanya [2]., Naramula Swetha [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- santhoshpotnuru@gmail.com)
2, 3 B.Tech IV Year CSE, (17RG1A05J1, 17RG1A05K2),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

This provides an almost real-time plan known as the RTS to help searchable data analysis in the cloud efficiently and cost-effectively. By way of multidimensional attributes, RTS extracts key property information for that category to represent the information in multi-dimensional vectors. An intuitive suggestion was to significantly minimize the number of photos sent by talking instead of all about only one which is most representative, at least until mobile phones have been energy-restricted. In addition to the high difficulty and charges involved, current content-based analysis systems often fail to manage large levels of files efficiently. The proposed RTS technique is applied as a device middleware that operates on existing systems, such as the Hadoop file system, using the general interface of the file system and using the knowledge similarity property. We have a genuine circumstance of world use by evaluating 60 million photos using RTS that are alerted to kids that are lost in a crowded environment in due time. RTS is designed by using correlation-aware haze and manageable flat-structured addressing to harness the correlation properties of information's. To support semantic grouping, RTS benefits from VFS operations. We should use the page cache data to send to the daemon.

Keywords— Real Time Search (RTS), cloud storage, data analytics, real-time performance, semantic correlation

1. INTRODUCTION

The stalidity of the details seriously reduces the need for data due to the inacceptable latency. The importance or value of data inappropriate data analysis signifies the valuable comprehensiveness that can lead directly to economic results in a corporate intelligence application or new technological breakthroughs. Searchable data analysis means the acquisition by querying results of data value/worth such as the location of a valuable document, a correlated process identity, the critical picture, reconstruction machine log, etc. Data analytics usually consume large device inputs such as storage, I/O bandwidth, and high-performance multiform processors for the cloud. In certain cases the effects of stale data analytics may also be deceptive, which can lead to fatal problems[1]. This allows RTS to significantly minimize the latency of associated file recognition processing with a reasonably low accuracy. In comparison to a case where we are talking about the RTS approach and how we are used to upgrading such storage devices, such as the Spyglass and Smart Store. Our conception reduces the overhead calculation of current file identification systems by using locality sensitive hazing. LSH hash tables would potentially result in unequalled loads and impregnable vertical adressing query results due to the variable length of associated lists. The almost-real-time property of RTS makes it possible to classify the correlated files easily and also to reduce the scope of knowledge. RTS embraces many types of analytics that can be applied in searchable storage environments. We compile a huge and actual picture range of over 60 million pictures. The use of semanticized namespace for complex and flexible name space management for ultra deep storage systems is further expanded by RTS. Extensive experimental findings show the efficacy and efficiency of RTS in improving performance. RTS uses a summary representation based on the Blossom filter and has the leading choices for ease of use and convenience.

2. PREVIOUS APPROACH:

MixApart uses an optimised data cache and scheduling approach to correct the data that is stored on enterprise storage infrastructure by using MapReduce calculations. The front cache layer allows the performance of neighbourhood storage required by analysis. The shared back-end storage allows the management of data[2]. In order for Spyglass to map the name hierarchy into a multi dimensional K-D tree and use

multilevel versioning and partitioning to preserve coherence, he uses the location of a file namespace and the warped distribution of metadata. Glance, a just-in-time sampling device, is able to deliver reliable solutions without previous knowledge for aggregate and top-k questions. Present machine drawbacks: In addition to being extremely dynamic and paid, current content-based analytical methods often fail to manage massive file levels effectively. Our great complexity regularly leads to very sluggish loading and unbelievably high and sometimes inappropriate latency. The stalidity of the details seriously reduces the need for data due to the inacceptable latency. Current methods to search for and interpret unstructured data rely upon any portion of information files depending on the framework. As a result of the long delay of information systems and the resultant stalemate of records, the value/real value of information is diminished and ultimately overturned[3].

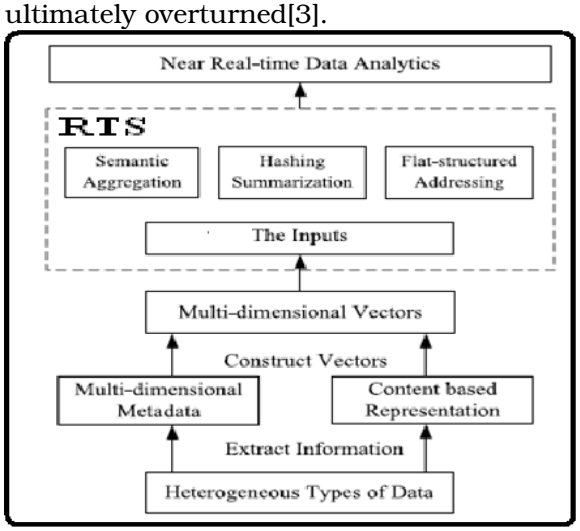


Fig.1.Proposed framework

3. FINE-GRAINED METHOD:

Furthermore, this text, which can be searched for, is interpreted to acquire a data value / value by way of queried results, such as a valuable record, a correlated process-ID, a main picture, a reconstruction machine log etc. We advise a unique near-time approach for the analyses of large volumes of data known as RTS, which aims to process this data effectively in real time. The important principle behind RTS is to explore and use the correlation property through enhanced haze and flat-structured correlation management to significantly decrease the processing delay of parallel inquiries, although an acceptably limited loss of precision[4] occurs. In machine architecture and finishing computation, the estimated plan's legitimate time efficiency is still widely understood. In turn, RTS moves on to deliver powerful data analytics at a dramatically higher processing speed through the easy blend of current strategy. We hope to make the following contributions for near-real-time data analytics through the research concerning the RTS methodology.

Methodology: With respect to the motives, we consult. Based on the researchers, the principal factors are double. This is further compounded by the repeated disc I/Os and network transmissions. Secondly, there are periodic device crashes in some applications resulting in re-computations which significantly increase latency. In reality, it was also formerly important to combine forensic picture evidence of personal and technical origins. Many file systems or their tracks vary in real-time from multi-dimensional attributes. Affinity poorly refers to semantile similarity generated by multi-dimensional file attributes that do not, however, contain only temporal or spatial location[5]. It is demonstrated that RTS is a helpful platform that supports real-time data analysis applications nearly in real time. It will be a hacking connection knowing to locate the correlated files by hash-computing, such as locality-sensitive hacking. With multi-dimensional attributes, RTS extracts the main property information of a given category to represent these data in multi-dimensional vectors. One essential feature is that without hierarchy, the namespace is flat. To represent the namespace accurately, RTS uses multi-dimensional attributes to consider semantical associations instead of single-dimensional. Current structures can be changed to increase efficiency.

Methods and Framework: There is a lot of similar multimedia images within the cloud. We advise to utilize a crowd-based aid, i.e., personal images that may be freely utilized, to recognize useful clues. e can rapidly have the clues suggesting if the missing child had ever made an appearance round the Big Ben. High-resolution cameras offer high picture quality and multiple angles. according to our observations and real-world reports, users have become more and more prepared to share their sightseeing images because of the shared interests and also the easy internet access. Within the SA module, RTS employs locality sensitive hashing to capture correlated features that identify similar images. RTS includes two primary functional modules, i.e., big information systems and semantic correlation analysis. The area-efficient representation enables the primary memory to contain more features. Generally, two similar images imply they contain many identical features. To do accurate and reliable matching between different views of the object or scene that characterize similar images, we extract distinctive invariant features from images [6]. An incorrect positive implies that different images are put in to the same bucket. An incorrect negative implies that similar images are put into different buckets. Unlike conventional directory based hierarchy, RTS take advantage of the VFS operations to aid semantic grouping. We are able to have the data from page cache to help transmit towards the daemon. We implemented a RTS prototype from the use situation on the 256-node cluster. RTS hence leverages the verification and responses from users to assist determine the query precision. This paper proposes an almost real-time plan, known as RTS, to aid efficient and price-effective searchable data analytics within the cloud. Among the key parameters may be the metric R that regulates the way of measuring approximate membership. The LSH-based structures could work well if R is roughly comparable to the space between your queried point q and it is nearest neighbors [7]. The query latency of RTS is a lot shorter than the other schemes and stays roughly. Since RNPE leverages simple but error-prone tags to recognize similar images, her cheapest precision. PCA-SIFT, however, uses compact feature vectors and performs dimensionality reduction. RTS leverages its near-duplicate identification method to considerably reduce the quantity of images to become transmitted.

4. CONCLUSION:

Our conception reduces the overhead calculation of current file identification systems by using locality sensitive hazing. LSH hash tables would potentially result in unequalled loads and impregnable vertical addressing query results due to the variable length of associated lists. RTS's idea is to investigate and utilize semantic correlations by correlation-aware hacking and handling of flat-structured solutions to dramatically reduce the latency of processing while at the same time achieving reasonable limited data loss research precision. This paper suggests an almost in real time strategy called RTS to promote cost-effective and efficient cloud searchable data analysis.

REFERENCES:

[1] Yu Hua, Senior Member, IEEE, Hong Jiang, Fellow, IEEE, and Dan Feng, Member, IEEE, “Real-Time Semantic Search Using ApproximateMethodology for Large-Scale Storage Systems”, ieee transactions on parallel and distributed systems, vol. 27, no. 4, april 2016.

[2] T. Ahonen, A. Hadid, and M. Pietikainen, “Face description with local binary patterns: Application to face recognition,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[3] A. Andoni and P. Indyk, “Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions,” Commun. ACM, vol. 51, no. 1, pp. 117–122, 2008.

[4] Y. Ke and R. Sukthankar, “PCA-SIFT: A more distinctive representation for local image descriptors,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2004, pp. 506–513.

[5] S. Kavalanekar, B. Worthington, Q. Zhang, and V. Sharda, "Characterization of storage workload traces from production Windows servers," in Proc. IEEE Int. Symp. Workload Characterization, 2008, pp. 119–128.
[6] X. Tan and B. Triggs, "Enhanced local texture feature sets for face recognition under difficult lighting conditions," IEEE Trans. Image Process., vol. 19, no. 6, pp. 1635–1650, Jun. 2010.
[7] S. Lakshminarasimhan, J. Jenkins, I. Arkatkar, Z. Gong, H. Kolla, S.-H. Ku, S. Ethier, J. Chen, C. S. Chang, S. Klasky, R. Latham, R. Ross, and N. F. Samatova, "ISABELA-QA: Query-driven analytics with ISABELA-compressed extreme-scale scientific data," in Proc. Int. Conf. High Perform. Comput., Netw., Storage Anal., 2011, pp.1–11.

SHIELDING PERCEPTIVE I/O INFORMATION USING RENOVATION PROCEDURE IN OPEN NETS

Kalevar Spurthi[1]., Bombothula Navya Laxmi [2]., Thadaka Swetha [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- spurthi91@gmail.com)
2, 3 B.Tech IV Year CSE, (17RG1A05L1, 17RG1A05L3),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

We advise the decomposition of LP Computation into public LP solvers beyond the customer's cloud and LP parameters. Straight-line programming is definitely an algorithmic and statistical methodology to improve the first-time results and refine engineering of various computer parameters. It has been widely used for testing and improving real-world systems/ models in many engineering fields including packet routing, flow management, data centre power control, and so on. The main problem with protection, though, is how to secure the data processed and generated during calculation for your customers. The effective outsourcing of large, relevant straight line programming calculations (LP) was studied in this article focused on engineering and optimization tasks. In order to verify the calculation result, we analyze the LP main duality theorem and define the necessary and adequate problems that must be met with the right results. Either heavy cloud crypto graphical calculations or various complex protocols are involved in current approaches or in the enormous problems of networking. Our mechanism makes significant saves on cloud customers from secure LP outsourcing, as it only takes time to solve a standard LP query.

Keywords— Confidential data, computation outsourcing, optimization, cloud computing, linear programming.

1. INTRODUCTION

To control unintended information disclosure, secure data must be encrypted before outsourcing offers full cloud protection. The outsourcing of LP estimation to LP solvers operating across the cloud and the LP criteria of the client is clearly broken down by our system. Outsourcing cloud computing is a key advantage. Addresses are often reported in outsourcing workloads[1], such as financial reports for companies, private analyses, personal health information, etc. This flexibility allows one to gain information on the required safety/efficiency compromise in relation to general circuit representation with a more comprehensive summary of LP calculations. Yet customers do not know anything about the operational data in the cloud. In fact, this style of design may ensure that users carry out less operations using a process instead of finalising the measurement themselves directly. Buyers should find cloud support otherwise, there is no excuse. The use of FHE operations and negative sizes of circuits which cannot be used to create original and encrystallic loops is extremely problematic though, in the normal estimation of this general method might not be possible. This general approach helps one to find appropriate solutions for such programming problems in contrast to circuit representation at higher abstraction levels. In this paper we are exploring technically successful methods to safely externalise direct calculations (LP). Straight-line programming is definitely an algorithmic and computing strategy to improve and refine engineering for the first time the results of different device parameters. It has been widely used for research and modifications of real-world systems/models in many areas of engineering, such as packet processing, flow management, data control, etc. The flexibility of these decompositions allows one to grasp the abstract of the LP equations more easily than the representation for this practical efficiency of the general circuits. A key advantage of this higher level of problem processing technology is the ability to directly reproduce the latest lp solver and applications from a cloud server. We use the fact that the transformed LP problem solving the cloud server makes sense to validate the results. We examine the critical theory for duality and the piecemeal building of the subsidiary LP problem to decide certain problems necessary and sufficient to satisfy the correct outcome. Comprehensive examination of defence and experimental results show that the design of our mechanism

is instantly possible. This approach is extremely useful for verificating performance and brings additional costs to cloud servers and customers near zero.

2. TRADITIONAL DESIGN:

Recent researches in cryptography as well as in theoretical IT groups are making constant progress in 'safe outsourcing of expensive calculations.' The ultimate effect of protected calculation outsourcing continues to be illustrated, according to Yao's disruptive circuits and Gentry's breakthrough emphasis on full-homomorphic file encryption (FHE) preparation, as it is technically feasible to symbolise the calculation with an encrypted combinational Boolean circuit which can be valued with crypted private data. Frikken has a clearly safe procedure to multiply the secret outsourcing matrix [3]. While this work approaches its previous sense of server expectation and measurement efficiency, the high overhead communication can be disadvantageous. According to secrete discussion technology, all scalar operations are extended to polynomials in the original matrix multiplication and have an enormous overhead. Present machine drawbacks: Due to the very complexities of FHE working and gloomy circuit sizes, which cannot be used to create initial and encrypted circuits, the current mechanism for regular calculations could not even be similar to realistic. In summary, virtually powerful mechanisms are now lacking with immediate activities for healthy cloud storage.

3. ADVANCED TOPOLOGY:

Within this paper, we study practically efficient mechanisms for secure outsourcing of straight line programming (LP)computations. Straight line programming is definitely an algorithmic and computational tool which captures the very first order results of various system parameters that needs to be enhanced, and it is necessary to engineering optimization. Particularly, we first formulate personal information of the client for LP problem as some matrices and vectors. This greater level representation enables us to use some efficient privacy-preserving problem transformation techniques, including matrix multiplication and affine mapping, to change the initial LP problem into some random one while protecting the sensitive input/output information. Benefits of suggested system: It's been broadly utilized in various engineering disciplines that evaluate and optimize real-world systems/models, for example packet routing, flow control, power control over data centers, etc. The computations made by the cloud server shares the same time frame complexity of presently practical algorithms for solving the straight line programming problems, which helps to ensure that using cloud is economically viable. The experiment demonstrates the immediate functionality: our mechanism can invariably help customers get more tasks completed than 50% savings once the sizes from the original LP troubles are not very small, while presenting no substantial over mind around the cloud.

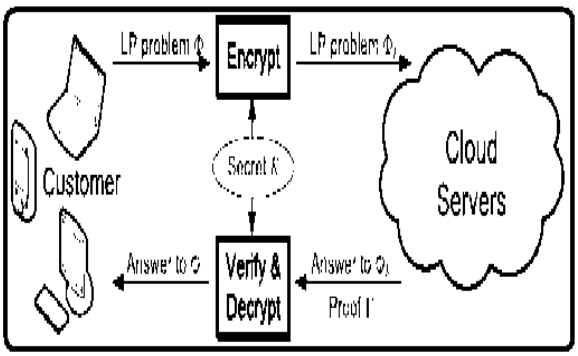


Fig.1.Block diagram of proposed system

Overview: At greater abstraction levels, more details concerning the computations becomes public to ensure that security guarantees become less strong. But more structures become available, and also the mechanisms be efficient. At lower abstraction levels, the structures become generic, but less details are open to the cloud to ensure that more powerful security guarantees might be achieved at the expense of efficiency [4]. Cloud-computing enables a financially promising paradigm of computation outsourcing. Particularly, by formulating private LP problem as some matrices/vectors, we develop efficient privacy-preserving problem transformation techniques,

which permit people to transform the initial LP into some random one while protecting sensitive input/output information.

Design Framework: Within this framework, the procedure on cloud server could be symbolized by formula ProofGen and also the process on customer could be organized into three algorithms (KeyGen, ProbEnc, ResultDec). Observe that our suggested mechanism shall never make use of the same secret key K for 2 different problems. We first study within this subsection a couple of fundamental techniques and reveal that the input file encryption according to them along may lead to an unsatisfactory mechanism. However, case study can give insights about how a more powerful mechanism ought to be designed. Because of the wide use of LP, like the estimation of economic revenues or personal portfolio holdings, the data in objective function c and optimal objective value cT x may be sensitive and want protection, too. To do this, we apply constant scaling towards the objective function, i.e. a genuine positive scalar g is generated at random included in file encryption keyK and c is substituted with gc. Basically, it implies that although it's possible to alter the constraints to some different form, there is no need the achievable region based on the restrictions can change, and also the foe can leverage similarly info to achieve understanding from the original LP problem. We advise to secure the achievable region of F by making use of an affine mapping around the decision variables x [5]. This design principle is dependent on the next observation: ideally, when we can arbitrarily transform the achievable section of problem F in one vector space to a different and the mapping function as secret key, there's not a way for cloud server to understand the initial achievable area information. Observe that within our design, the workload needed for purchasers around the result verification is substantially less expensive than solving the LP problem by them, which ensures the truly amazing computation savings for secure LP outsourcing. Therefore, the end result verification method not just must verify an answer when the cloud server returns one, but must also verify the instances once the cloud server claims the LP issue is infeasible or unbounded. We'll first present the proof G the cloud server ought to provide and also the verification method once the cloud server returns an ideal solution, after which present the proofs and also the means of another two cases, because both versions is made upon the prior one. We first think that the cloud server returns an ideal solution y. To be able to verify y without really solving the LP problems, we design our method by seeking some necessary and sufficient problems that the perfect solution must satisfy. We derive these conditions in the well studied duality theory from the LP problems. The strong duality from the LP problems claims that if your primal achievable solution y along with a dual achievable solution result in the same primal and dual objective value, then both of them are the perfect solutions from the primal and also the dual problems correspondingly [6]. Clearly, this auxiliary LP problem comes with an optimal solution because it has a minimum of one achievable solution and it is objective function is gloomier-bounded. The duality theory signifies that this situation is the same as that FK is achievable and also the dual problem of FK, is infeasible. We currently evaluate the input/output privacy guarantee underneath the aforementioned ciphertext only attack model. Offline guessing on problem input/output doesn't bring cloud server any advantage, since there's not a way to warrant the validity from the guess. Hence, polynomial running time foe has minimal opportunity to succeed. However, it's not yet obvious exactly what the underlying connection backward and forward LP problems F and FK is and just how that relationship may benefit our mechanism design.

Enhanced Technology: Additionally, we discuss the way the uncovered results may affect the potential information leakage on some kind of special cases, and just how we

are able to effectively address them via lightweight techniques. For that three customer side algorithms KeyGen, ProbEnc, and ResultDec, it's straight-forward the most time-consuming operations would be the matrix-matrix multiplications in problem file encryption formula ProbEnc. Within our experiment, the matrix multiplication is implemented via standard cubic-time method, thus the general computation overhead is O(n3). For cloud server, its only computation overhead would be to solve the encrypted LP problemFK in addition to generating the end result proof G, each of which match the formula ProofGen [7]. When the encrypted LP problem FK is associated with normal situation, cloud server just solves it using the dual optimal solution because proof G, that is usually easily available in the present LP solving algorithms and incurs no additional cost for cloud. Thus, out of all cases, the computation complexity from the cloud server is asymptotically just like to resolve an ordinary LP problem, which often requires greater than O(n3) time.

4. CONCLUSION:

The flexibility of such decomposition helps one to consider the more abstraction of LP formulas for this practical output than the general circuit representation. This type of safe and practical computer design, respects data security, reliability and productivity for input and outputs, officialises the issue of secure outsourcing of LP computations for the very first time. Through intentionally decomposed the outsourcing of LP to publicly available solvers and records, our mechanism's design is capable of exploring appropriate security/efficiency constraints by higher level LP computation than the general system representation. This form can be paired with an extra close-to-null overhead in the overall mechanism. We have also established problem approaches which empower people to secretly turn the LP into a random LP while protecting sensitive input/output data.

REFERENCES:

[1] Cong Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Jia Wang, Member, IEEE, “Secure Optimization Computation Outsourcingin Cloud Computing: A Case Studyof Linear Programming”, ieee transactions on computers, vol. 65, no. 1, january 2016.

[2] C. Wang, K. Ren, and J. Wang, “Secure and practical outsourcing of linear programming in cloud computing,” in Proc. IEEE INFOCOM, 2011, pp. 820–828.

[3] W.Du and M. J. Atallah, “Secure multi-party computation problems and their applications: A review and open problems,” in Proc. New Secur. Paradigms Workshop, 2001, pp. 13–22.

[4] R. Gennaro, C. Gentry, and B. Parno, “Non-interactive verifiable computing: Outsourcing computation to untrusted workers,” in Proc. 30th Annu. Conf. Adv. Cryptol., Aug. 2010, pp. 465–482.

[5] O. Catrina and S. De Hoogh, “Secure multiparty linear programming using fixed-point arithmetic,” in Proc. 15th Eur. Conf. Res. Comput. Security, 2010, pp. 134–150.

[6] P. Golle and I. Mironov, “Uncheatable distributed computations,” in Proc. Conf. Topics Cryptol.: The Cryptographer’s Track RSA, 2001, pp. 425–440.

A SLANTED BOOLEAN MANEUVER METHOD FOR FINEST ROUTING

Prasanthi Gundabattini[1]., Bhanuri Sravani [2]., Nallanagula Bhargavi [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- gprashanthi81@gmail.com)
2, 3 B.Tech IV Year CSE, (17RG1A05J2, 17RG1A05K1),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

In a random collection of network nodes, trivial protected communications allows any node to maintain n-1 keys in pairs of symmetrical encrypting situations, whereas n-1 public key with uneven cryptography, where n refers to the number of network nodes. Each node finds the underlay path length connected with its overlay neighbors during the network service process by having basic route specifications. The hidden pair keys are in the critical pool for key pre-distribution schemes that is constructed according to symmetric cryptography principles. We apply to the network layer in this paper because of the underlying layer as well as the layer because of the overlay layer. Our proposed choice would effectively be to answer to an LP problem by relaxing all Boolean restrictions in the original problem. In solving the Boolean LP problem, the effectiveness of our formula does not surpass that of resolving the relaxed LP problem though ensures that the perfect solution is known. In addition to weighted or unweighted, we noted the key advantage of our formula as being the potential in virtually every graph to solve the ideal routing problem. Assess network efficiency, safety and consumption properties using the proposed formula for symmetrical and inconsistent main pre-distribution methods running on top of protocols of routing on-demand. We use three main methods of pre-distribution, i.e., 2-UKP, SST, PAKP, which will operate on the ad-hoc if the distance vector routing protocol is necessary, to measure success in our proposed form.

Keywords— LP problem, Overlay Routing, Underlay Routing, Linear Optimization, Shortest Path, Directed Graphs, Pre-Distribution.

1. INTRODUCTION

It is noted that a two layer formula to find the underlining path following a matching overlay path is essential for the routing by using the main pre-distribution schemes. Special algorithms are needed to find optimal stable overlay paths in safe routing techniques with key pre-distribution algorithms[1] [2]. The text is clearly decrypted and easily encrypted by the intermediary nodes on the overlay route and the encrypted message is only being used by all kinds of other nodes involved. A stable routing formula, optimising underlay and overlay routes by key pre-dealing strategies, is proposed as the main contribution, but does not include clear trust in other network nodes. The main contribution. We have placed various uneven and symmetric main pre-distribution schemes [3] in order to determine the efficiency and protection strength of the proposed formula. We see our action as a safe and operational solution to main delivery network routing applications. When an assailant breach many nodes, several connections can become unsecured, the main downside to the essential probabilistic pre-dispensation. Our work proposed proposes a lightweight solution that eliminates the hardware and central server requirements along with many routing domains, to the detriment of keeping a limited number of keys per node and minimizes an extra fee for file encryption. Liu and Ming are proposing to store vicariate polynomials rather than keys which require neighboring nodes to have at least one common polynomial. Incomplete balanced block architecture really is a complementary design approach used in core pre-distribution schemes. Each block represents an essential ring assigned to a node. BIBD places v separate key items from the key pool in b blocks. Overall, primary pre-distribution systems are not modular and would like an enormous amount of room for storage [4].

2. CLASSIC DISTRIBUTION SCHEME:

The majority of the key pre-distribution schemes pick the keys at random but there are many others that attempt for selecting keys in smarter ways. Key pre-distribution schemes are classified into deterministic and probabilistic algorithms. Both in groups, each network node is pre-packed with several keys selected from the key pool within the initialization phase. Choi, Zhu, C¸ amtepe, and

Ruj propose different deterministic key pre-distribution schemes [5]. Eschenauer and Gligor propose the very first probabilistic key pre-distribution formula by which each set of neighboring nodes possess a common key having a specific probability. Disadvantages of existing system: Deterministic key pre-distribution schemes aren't scalable and want an extremely large space for storage. The primary drawback to the fundamental probabilistic key pre-distribution is when an assailant compromises several nodes, many links might be potentially made insecure.

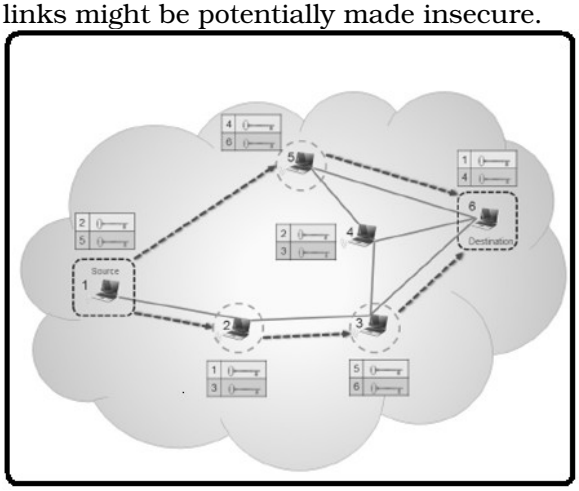


Fig.1.Proposed system framework

3. ENRICHED SCHEME – LP MODEL:

The primary contribution of the paper is proposing a safe and secure routing formula jointly optimizing underlay and overlay pathways using key pre-distribution schemes although not requiring explicit trust of other network nodes. More particularly, the contributions of the paper are: Modeling a network using key pre-distribution schemes with directed and weighted graphs, Proposing a Boolean LP problem for optimal overlay routing within the resulting network graph, Analytically lowering the Boolean LP problem to some relaxed LP problem and therefore solving the Boolean LP in polynomial time, and Evaluating network performance, security, and consumption characteristics from the suggested formula for symmetric and uneven key pre-distribution methods operating on the top of on-demand routing protocols [6]. Benefits of suggested system: We model a network having a weighted directed graph by which all edges and vertices their very own cost. A safe and secure routing formula for that modeled graph utilizing a Boolean LP problem. Employed for secure routing in almost any network using any key pre-distribution plan. Experimental results reveal that our formula improves network performance and enhances network security.

Routing Overlay: You should understand that each hop within an overlay path may contain several underlay hops. The very best path may be the path which both security and gratification are optimally measured. Selecting a higher vertex cost produces a greater cost for extended overlay pathways. we model the issue having a Boolean LP problem after which propose a means to solve this issue in polynomial time, no worse compared to time complexity connected with solving the relaxed LP problem without Boolean constraints. Hence, we advise that every node stores a lookup table that contains details about stored keys. Furthermore, we advise to help keep the price of each edge within the lookup table. We observe that the price of all vertices is identical representing to buy a intermediate understanding-file encryption step. The second signifies that a worldwide advance understanding from the underlay network topology isn't needed for the whole process of our suggested method. However, the assumption is the cryptographic network topology is famous. Within the situation of PAKP method, there's no considerable improvement because of applying our suggested routing formula. This really is alluded that routing is dependent on the shortest overlay path in the source node towards the destination and also the high vertex cost over a underlay hop cost. Accordingly, how big routing packets is elevated [7]. In comparison, PAKP doesn't need to send any other information in the routing packets. To be able to compensate from the faster speed of symmetric cryptography compared to uneven cryptography, we pressure each set of nodes to agree with a pairwise key for file encryption and

understanding within the PAKP method. A greater quantity of intermediate understanding-file encryption steps increases the prospect of an foe node being able to access messages.

4. CONCLUSION:

We shape the question of safe routing and propose a straight line (LP) Boolean problem to achieve the optimum direction. Many techniques allow you to solve Boolean and integer problems with LP. Based on our suggested form, each node is pre-packed by two randomly chosen keys along with a search table in the network initialization process. A stable and safe routing algorithm using the Boolean LP problem for this modeled graph. Used with every primary pre-distribution strategy for safe routing in most networks. In the new safe communications environment, key pre-distribution algorithms have recently become an important solution to key control. In many lately proposed symmetric and unequal methods of pre-distribution, we use our proposed algorithm. When an assailant breach many nodes, several connections can become unsecured, the main downside to the essential probabilistic pre-dispensation.

REFERENCES:

[1] Mohammed Gharib, Student Member, IEEE, HomayounYousefi'zadeh, Senior Member, IEEE,and Ali Movaghar, Senior Member, IEEE, "Secure Overlay Routing Using Key Pre-Distribution:A Linear Distance Optimization Approach", IEEE Transactions on Mobile Computing 2016.

[2] M. e. a. Gharib, "A novel probabilistic key management algorithm for large-scale manets," in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, March 2013, pp. 349–356.

[3] A. Vannelli, "An adaptation of the interior point method for solving the global routing problem," Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, pp. 193–203, Feb 1991.

[4] M. e. a. Gharib, "Expert key selection impact on the manets' performance using probabilistic key management algorithm," in Proceedings of the 6th International Conference on Security of Information and Networks, ser. SIN '13. New York, NY, USA: ACM, 2013, pp. 347–351.

[5] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," Mobile Computing, IEEE Transactions on, vol. 5, no. 2, pp. 128–143, Feb 2006.

[6] M. Huson and A. Sen, "Broadcast scheduling algorithms for radio networks," in Military Communications Conference, 1995. MILCOM '95, Conference Record, IEEE, vol. 2, Nov 1995, pp. 647–651 vol.2.

[7] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security, ser. CCS '03. New York, NY, USA: ACM, 2003, pp. 52–61.

A PROPOSAL TO AUTOMATIC REVOKE DELEGATION BY THE DATA OWNER

Jonnalagadda Sravani[1]., A. Bhavana [2]., K. Praneetha [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- sravanij691@gmail.com)
2, 3 B.Tech IV Year CSE, (18RG5A0501, 18RG5A0503),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

A digital healthcare record product is a unique technology that makes healthcare more convenient. In this paper we present a single original cryptographic feature, named as the conjunctive search keyword, which is a type of time based SE plan, with the designated tester and timing. A unique, searchable encryption file plan is designed to help stable conjunctive keyword search and supported delegation feature. The SE plan is a technology to integrate security safety and good functionality, which would be of enormous importance in the e-health records system. The SE plan is a technology. Unlike current systems, the work can timing enabled proxy re-encoding and efficient revoking of the delegation. The protection and confidentiality of private sensitive information will be the main worries of consumers who could prevent further implementation and widespread acceptance of the systems. It may encourage patients to assign limited rights of access within a brief period of time to other individuals to conduct search functions over their data. The size and decryption of the encrypted documents of the delegate may be regulated. The contrast and detailed simulations show a low estimation and overhead storage. For this proposed re-dtPECK scheme, we devise a system model along with a protection model, to prove that the plan is competent and protected in the regular model. The experimental findings and safety analyses show that our plan is much more secure in comparison with current cloud-based solutions..

Keywords— Searchable encryption, time control, conjunctive keywords, designated tester, e-health, resist offline keyword guessing attack.

1. INTRODUCTION

The biggest barrier to large-scale systems implementation will be the strong security and privacy issues. The PRE approach could be extended to the proxy re-file encryption. Microsoft Health Vault and Google Health, for instance, are introduced with many realistic patient-centered Electronic Health Record systems. Health data gathered in a data centre might include personal data that would allow the persons or firms that are entitled to benefit from their shop[1] to possible leakage and disclosure. The server is able to transform the encrypted patient index into a re-encrypted form that the delegate may display. A plausible solution to solve this dilemma will be to encrypt all his data with a new key, which would cost even more. The revoking of the delegate in a scalable scale is probably even more complex. In this paper we attempt to resolve the problem by suggesting a novel method for automatically withdrawing the delegation after a period previously specified by the data holders. A unique, searchable encryption file plan is designed to help stable conjunctive keyword search and supported delegation feature. The proposed strategy is officially proven safe against chosen keyword attacks. Preset timing of owner-compliant delegation is enabled. The owner has the power to determine multiple successful access times for different users as he appoints his right of delegation. A very efficient time span may be represented with the start and shutdown time by the data holders. The timeline T is baked in the re-encrypted ciphertext by using a proxy server re-file encryption formula. This is the proxy reencoding feature that has been enabled. A conjunctive search plan for keywords with designated proxy encryption tester and schedule is recommended.

2. CONVENTIONAL METHOD:

Public key file encryption plan with keyword search (PEKS) enables a person to look on encrypted information without decrypting it that is appropriate to boost the safety of Electronic health record systems. In certain situations, someone might want to behave as a delegator to delegate his search to a delegate, who is able to be his physician, without revealing their own private key. The proxy re-file encryption (PRE) method could be brought to match the requirement. The server could convert the encrypted index from the patient right into a re-encrypted form which

may be looked through the delegate. However, one other issue arises once the access right is distributed. Once the patient recovers leaving a healthcare facility or perhaps is used in another hospital, he doesn't want the non-public data to become looked and utilized by his previous physicians any longer. A potential method of solve this issue would be to re-secure all his data with a brand new key, that will bring a significantly greater cost. It will likely be more difficult to revoke the delegation in a scalable size [2]. Disadvantages of Existing System: The intense security and privacy concerns would be the overriding obstacle that stands when it comes to wide adoption from the systems. Within the traditional time-release system, time seal is encapsulated within the ciphertext in the very start of the file encryption formula. It indicates that users including data owner are restricted when period.

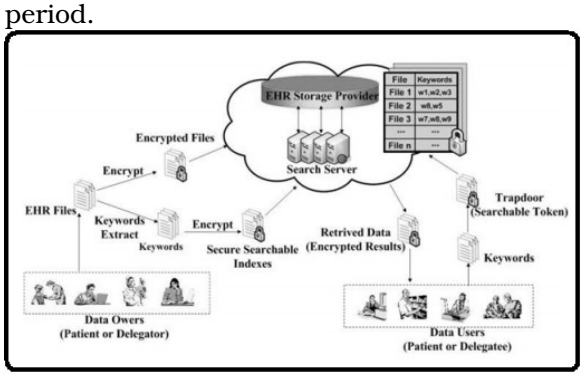


Fig.1.System architecture

3. NOVEL ENCRYPTION:

Within this paper, we try to solve the issue having a novel mechanism suggested to instantly revoke the delegation immediately after some time designated through the data owner formerly. We design a singular searchable file encryption plan supporting secure conjunctive keyword search and approved delegation function. In contrast to existing schemes, the work is capable of timing enabled proxy re-file encryption with effective delegation revocation. Owner-enforced delegation timing preset is enabled. Distinct access period of time could be predefined for various delegates [3]. The suggested plan is formally demonstrated secure against selected-keyword selected-time attack. Benefits of Suggested System: The good thing about the suggested product is that there's virtually no time limitation for that data owner since the time details are baked into the re-file encryption phase. The information owner is competent to preset diverse effective access periods of time for various users as he appoints his delegation right. We formally define the conjunctive keyword search having a designated tester and also the timing enabled proxy re-file encryption function. Then, we describe a concrete Re-dtPECK plan having a detailed workflow and derive the correctness from the plan. The Re-dtPECK plan includes following algorithms by having an indicator? When its value is 1, the delegation function is going to be activated. Otherwise, the proxy re-file encryption won't be enabled. Within the system, the Electronic health record documents of the sufferers are encrypted with a symmetric file encryption formula and also the symmetric secret is encapsulated using the patient's public key pea through the key encapsulation mechanism. The algorithms concentrate on the searchable keywords file encryption and also the timing controlled delegation function. The delegator Rib transmits out a delegation notice towards the reliable 3rd party, time server, proxy server, data server and delegate Rj. The signature could be verified using the public key of Ri. The delegation request might be rejected when the signature is forged. The authority delegation is recognized largely by proxy re-file encryption mechanism. The proxy server take advantage of the re-file encryption answer to transform the ciphertext encrypted by delegator's public key into another form, which may be looked through the delegate using their own private key. To have time controlled access right revocation, the predefined time details are baked into the re-encrypted ciphertext having a time seal. With the aid of time seal, the delegate has the capacity to produce a valid delegation trapdoor by TrapdoorR formula. When the time information hidden within the re-encrypted ciphertext is sporadic with this within the

delegation trapdoor, the equation in TestR formula won't hold. The individual them self won't be restricted through the effective period of time since the limitation is created within the delegation phase as opposed to the original file encryption phase. You will find six entities to have fun playing the interactive process together with a reliable 3rd party (TTP). For example, the Veterans Health Administration (VHA) is assumed to operate like a TTP, who's reliable by clinics, hospitals, patients and doctors. A delegator should be Joe, who's a chronic heart failure patient. The Electronic health record files of Joe are stored on the data server within the cloud inside a protected form. Joe visited Hospital A for that cardiac treatment since February. first, 2014. He wants to designate the cardiologist Dr. Donne from Hospital A to become his delegate for convenient Electronic health record data access [4]. Since Joe intends to transfer to Hospital B after June first and that he hopes that Dr. Donne can't inquiry his Electronic health record that point on. Then, Dr. Donne is granted a period-restricted authority to gain access to the protected health information (PHI) from the patient Joe. Time server (TS) will produce a time seal for Dr. Donne to make sure that they can use of Joe's PHI throughout February. first- May, 30st, 2014. The proxy server (PS) is accountable to secure Joe's PHI to some re-encrypted form to ensure that Dr. Donne can explore individual's records together with his own private key. In phase 1, the TTP initializes the machine by executing Global Setup formula and generates the worldwide parameters. In phase 2, Electronic health record files are created during Joe's therapeutic process. The encrypted Electronic health record indices and documents are going to be generated while using dPECK formula and stored in the cloud data server. Within this system, the signature formula won't be specified. But there's essential around the formula the signature plan ought to be strongly unforgivable. The notice is going to be rejected when the signature fails the verification. If it's verified true, the TTP runs ReKeyGen formula to develop a re-file encryption key and send it towards the PS secretly. The TS runs Time Seal formula to develop a time seal for delegate. When Joe's PHI information is utilized through the Dr. Donne, the PS will run Re-dtPECK formula to encapsulate the effective period of time into re-encrypted ciphertext. When the moment isn't in compliance using the effective period of time, the PS won't perform the re-file encryption operation for Dr. Donne. When the delegation indicator? equals to at least one, phase 3 is going to be performed. Joe transmits a delegation notice towards the TTP, PS, TS, delegate and knowledge server plus a signature signed by Joe. The effective delegation duration of PHI access delegation for delegate is specified. After finding the query, cloud server runs the delegation test formula [5]. The TS runs Time Seal formula to develop a time seal for delegate. When Joe's PHI information is utilized through the Dr. Donne, the PS will run Re-dtPECK formula to encapsulate the effective period of time into re-encrypted ciphertext. With this plan, the details are protected using a strong file encryption primitive. The indexes from the conjunctive keywords are encrypted through the dPECK or Re-dtPECK algorithms before submitted towards the cloud server. The company couldn't recover the plaintext from the encrypted data. The keyword extraction from Electronic health record is controlled through the patient and encrypted in your area with patient Ri's own secret key. However, the outdoors attacker couldn't decide concerning the ciphertext of certain keywords and time with no server's private key despite the fact that all of the trapdoors for that other keywords and occasions can be found. IND-KGA guarantees the attackers such as the server attackers and outdoors attackers couldn't discover the relationship between your given trapdoor and also the challenge keywords despite the fact that other trapdoors for delegator and delegate could be acquired. This is because the exam formula could be run when the keyword trapdoor and ciphertext are acquired. In PEKS schemes without designated tester, the exam formula could be operated by

any attacker. Within this work, the exam formula is only able to be performed through the data server using his private key, the solid concept of "designated tester". The suggested Re-dtPECK is going to be in contrast to other relevant schemes based on these indicators. A simulation result with an experimental test-bed can also be presented to appraise the performance of Re-dtPECK plan. Thus, the suggested plan has various helpful functions and it has more powerful security functionality than individuals of the majority of the existing searchable file encryption schemes [6]. We've evaluated the suggested Re-dtPECK plan by applying critical factors with an experimental work bench, such as the system global setup, the important thing generation, the re-file encryption key generation, the trapdoor generation and also the test algorithms.

4. CONCLUSION:

To our best degree, it is currently the first searchable encryption of files using the proxy re-file encryption feature that is available and also the named HER cloud record storage tester. We also proposed a unique Re-dtPECK Strategy in this paper to explain the timing of an automated delegate cancellation of the privacy-restrictive keyword search process for the electronic health record-cloud storage. It can also provide the quest of conjunctive keywords and resist attacks by keywords. The approach allows only the tester to monitor the existence of such keywords. Unlike other traditionally searchable systems for file encryption, performance analyses mean that our suggested plan, alongside its greater security, is capable of high calculation and storage efficiency. Furthermore, after a defined period of usefulness, the delegate can automatically miss the access and check authority. The coordination and overall computation from the proposed option for almost every real-life applications scenario has been demonstrated in our simulation performance.

REFERENCES:

[1] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.

[2] X. A. Wang, X. Huang, X. Yang, L. Liu, and X. Wu, "Further observation on proxy re-encryption with keyword search," J. Syst. Softw., vol. 85, no. 3, pp. 643–654, 2012.

[3] Yang Yang and Maode Ma, Senior Member, IEEE, "Conjunctive Keyword Search With DesignatedTester and Timing Enabled Proxy Re-EncryptionFunction for E-Health Clouds", ieee transactions on information forensics and security, vol. 11, no. 4, april 2016.

[4] L. Guo and W. C. Yau, "Efficient secure-channel free public key encryption with keyword search for EMRs in cloud storage," J. Med. Syst., vol. 39, no. 2, pp. 1–11, 2015.
[5] J. W. Byun and D. H. Lee, "On a security model of conjunctive keyword search over encrypted relational database," J. Syst. Softw., vol. 84, no. 8, pp. 1364–1372, 2011.
[6] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.

INDEX SWITCHING TO PREVENT DATA DYNAMICS BY ENHANCING MODEL

Konda Janardhan[1]., Chintapatla Asritha [2]., Mallisetty Srimanya [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- kondar15@gmail.com)
2, 3 B.Tech IV Year CSE, (17RG1A05J6, 17RG1A05J8),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract:This paper offers a public audit strategy with support for data dynamics and equal conflict arbitration. Cloud consumers no longer physically have their data, which makes it impossible to protect the credibility of the outsourced data. Recently proposed structures such as "proven record ownership" and 'experiments of irretrievability' are made to tackle this problem, but they are not sufficiently backed by data mechanics to audit static archive data. Moreover, hazard models typically presume that a true data owner focuses on a deceptive cloud provider when consumers may misbehavior. We particularly design a catalogue switch to remove the cap on index use in tag calculations in current schemes and to manage data dynamics in an efficient way. The safety review reveals that our scheme is demonstrably safe and the success assessment shows the overhead complexities of details and resolution of disputes. We broaden current threat models and introduce an idea for the exchanging of signatures to establish equal arbitration procedures in order to address the justice issue, so that all disputes can be equally resolved.

Keywords: Integrity auditing, public verifiability, dynamic update, arbitration, fairness.

1. INTRODUCTION:

Since users no longer have their data physically and thus lose direct knowledge access, the direct use of standard cryptographic primitives such as hash or file encryption will lead to many security loopholes[1]. Initially, previous audit systems typically need CSP to establish a deterministic proof, allowing access to the complete computer file to verify credibility. Next, some audit systems ensure that the data owner only wants the non-public response to conduct the auditing task is privately verifiable. Third, PDP and PoR aim to inspect seldom modified static data, thereby having little support for data dynamics. Data audit systems will help cloud users to assess the integrity without downloading any of the centrally stored data in your region known as block less verification. But from a broad point of view. However, more security risks may arise from direct extensions to these static data oriented systems to facilitate dynamical updates. For each update, we assign a new tag index to increase the mapping among tag indices and block indices for that operating block[2]. In order to deal with the justice of audit, we have added another arbitrator to our model of hazard, which is a conflict arbitration specialist institute, which is trusted and played by both data owners and the CSP. In accordance with our programme, we deliver justice guarantees and disputes. Current research generally suggests that a true data owner has an innate bias towards cloud users in their security models.

2. MODEL TRADITIONAL:

Existing audit schemes aim to use the index of a block in its tag calculation to authenticate disputed blocks. However, block indices which shift, and then tags from these blocks should be recomputed if we insert or remove a block. Because of the high overhead computing, this is very inappropriate. In current public audit systems, hazard models primarily rely on delegating auditing work to a 3rd-party auditor (TPA) to discharge customer overhead wherever possible. These designs do not take justice seriously into account, however, since they typically take a true owner against an entrusted CSP. Disadvantages: Cloud users no longer have their data physically and are no longer secure.

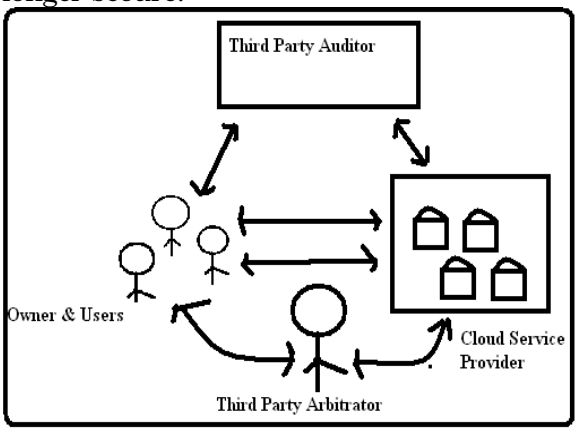


Fig.1.Framework of proposed model

3. IMPLEMNTATION:

Lately suggested schemes for example "provable data possession" and "proofs of irretrievability" are made to address this issue, but they're made to audit static archive data and for that reason insufficient data dynamics support. Furthermore, threat models during these schemes usually assume a genuine data owner and concentrate on discovering a dishonest cloud company even though clients might also misbehave. This paper proposes an open auditing plan with data dynamics support and fairness arbitration of potential disputes. Particularly, we design a catalog switcher to get rid of the limitation of index usage in tag computation in current schemes and get efficient handling of information dynamics. To deal with the fairness problem to ensure that no party can misbehave without having to be detected, we further extend existing threat models and adopt signature exchange idea to create fair arbitration protocols, to ensure that any possible dispute could be fairly settled. Advantages: Concentrate on discovering a dishonest cloud company even though clients might also misbehave. More security. It is simple for any third-party arbitrator to discover the cheating party. Clouds users depend around the CSP for data storage and maintenance, plus they may access increase their data. To ease their burden, cloud users can delegate auditing tasks towards the TPAU, who periodically performs the auditing and honestly reports the end result to users. The CSP makes gain selling its storage ability to cloud users, so he's the motive to reclaim offered storage by deleting rarely or never utilized data, as well as hides loss of data accidents to keep a status [5]. We extend the threat model in existing public schemes by differentiating between your auditor (TPAU) and also the arbitrator (TPAR) and putting different trust assumptions in it. Our design goal is, Fair dispute arbitration: to permit a 3rd party arbitrator to fairly settle any dispute about proof verification and dynamic update, and discover the cheating party. Our dynamic auditing plan with public verifiability and dispute arbitration includes the next algorithms. Therefore, disputes backward and forward parties are inevitable to some extent. Within our design, we have no additional requirement around the data to become stored on cloud servers. Within our construction, tag indices are utilized in tag computation only, while block indices are utilized to indicate the logical positions of information blocks. In implementation, a worldwide monotonously growing counter may be used to produce a new tag index for every placed or modified block. To be sure the correctness from the index switcher and additional the fairness of dispute arbitration, signatures around the updated index switcher need to be exchanged upon each dynamic operation. However, if parallelization strategy is accustomed to optimize the tag generation and proof verification in the client side, then your access from the index switcher can be a bottleneck of performance. A fundamental truth is that whenever the customer initially uploads his data towards the cloud, the cloud must run the Commitment to determine the validity of outsourced blocks as well as their tags, and later on their signatures around the initial index switcher are exchanged. An easy strategy is to allow the arbitrator (TPAR) make a copy from the index switcher [6]. Furthermore, since the change from the index switcher is because data update operations, the CSP can re-construct the most recent index switcher as lengthy as necessary update information are delivered to the CSP upon each update, which helps the CSP to determine the client's signature and generate their own signature around the updated index switcher. The safety of the protocol depends on the safety from the signature plan accustomed to sign the index switcher, that's, all parties only has minimal probability to forge a signature signed using the other party's private key. Once the client finds failing of proof verification throughout an auditing, he contacts the TPAR to produce an arbitration. To attain stateless arbitration in the TPAR, throughout arbitration, all parties needs to send his form of the index switcher towards the TPAR for signature verification. Within our

arbitration protocol, all parties must send his signature around the latest metadata to another party. We proceed by including several models of update and signature exchange. Now we evaluate the problem in which the signature exchange cannot be normally finished. To optimize looking here we are at tag indices, we sort the indices of challenged blocks before searching. However, data update and dispute arbitration involve the computation and verification from the signature around the index switcher. Thus, computing or verifying the signature around the index switcher must read its content in the file. However in cloud atmosphere, remotely stored data might not simply be read but additionally be updated by users that are a common requirement. To get rid of the index limitation of tag computation in original PDP plan and steer clear of tag re-computation introduced by data dynamics. In implementation, we write the information from the index switcher right into a apply for storage.

4. CONCLUSION:

We distinguish block indices and tag indicators from each other, and create a catalogue switch to help keep block tag index mapping such that tags are avoided by block upgrade operations, which lead in minimal additional overhead, as shown by our performance assessments. to remove index use limitations in tags calculation and to effectively provide data dynamics. The aim of this article will be to include a public verifiable honesty audit strategy, effective information dynamics and the resolution of equal disputes. We do this in accordance with the principle of sharing metadata signatures on each update operation by creating arbitration protocols. Our tests illustrate the effectiveness of our current strategy, which offers a fair total sum for dynamic updating and conflicts. In the meantime, given the possible misbehavior of both clients and the CSP in auditing and information updates, we are expanding the present threat model in current research to include an equal conflict settlement between clients and the CSP, which is essential for the implementation and promotion of cloud audit schemes.

REFERENCES:

[1] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” in Proc. 17th Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT98), 1998, pp. 591–606.

[2] HaoJin, Hong Jiang, Senior Member, IEEE, and Ke Zhou, “Dynamic and Public Auditing with Fair Arbitrationfor Cloud Data”, ieee transactions on cloud computing 2016.

[3] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced storages in clouds,” in Proc. ACM Symp. Applied Computing (SAC 11), 2011, pp. 1550–1557.

[4] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and verifiably encrypted signatures from bilinear maps,” in Proc. 22nd Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT03), 2003, pp. 416–432.

[5] T. S. Schwarz and E. L. Miller, “Store, forget, and check: Using algebraic signatures to check remotely administered storage,” in Proc. IEEE Intl Conf. Distributed Computing Systems (ICDCS 06), 2006, pp. 12–12.

[6] Z. Hao, S. Zhong, and N. Yu, “A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability,” IEEE Trans. Knowledge and Data Eng., vol. 23, no. 9, pp. 1432–1437, 2011.

AN EXTERNAL AUDITOR IN DEALING WITH THE IN-DEPTH CYBER DEFENSE OF OPEN NETWORKS

Valavajjula Tejaswi[1]., Chandupatla.Asritha [2]., Mulakanoor Chandana [3]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- valavajjulatejaswi@gmail.com)
2, 3 B.Tech IV Year CSE, (17RG1A05J3, 17RG1A05L2),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

We work on how to make the most straightforward changes possible for the user. We also propose a whole new paradigm called a cloud storage audit, where main updates are checked. This paradigm will allow key updates to be safely outsourced from the approved party and thus minimize the important customer upgrade burden. In addition, our design also enables customers to check the authenticity of the hidden cryptographic keys issued by the OA. Especially in many public auditing concepts we leverage the outsourced auditor; let him act as an approved party inside our situation to make him responsible for both storage audit and safe key updates on the resistance to key disclosure. Only when uploading new files to the cloud does the customer download the encrypted secret key in the OA. The approved party keeps the customer's encrypted secret key for cloud storage audit and updates it in all time under the encrypted condition. The customer downloads and decrypts the encrypted secret key to the accepted party just as he needs new data to be downloaded to the cloud. OA must only have an encrypted type of secret key to the customer in our design for carrying out any of these problematic tasks. OA must only keep an encrypted version of the customer's secret key in our design when performing each of these troubling customer tasks. We formalize this paradigm's importance and protection sort.

Keywords: Outsourced Auditor (OA), outsourcing computing, cloud storage auditing.

1. INTRODUCTION:

With a verifiable outsourcing of main upgrades, we develop the very first cloud storage audit protocol. These guidelines rely on numerous aspects such as high quality cloud storage audits, identity security, protection of identities, complex data processes, discussion of information and other factors. Through updating the user's hidden keys regularly, Yu et al. created a cloud storage auditing protocol with key disclosure resilience. Outsourcing computing has lately become very appealing and extensively investigated. We advise a whole new paradigm called the cloud storage audit, where main changes are checked outsourced. One critical protection issue is how the confidentiality of data kept in the cloud can be checked effectively. Recently, several cloud storage audit protocols have been proposed[1] to solve this issue. This introduces new local pressures for this customer, so the customer must still perform the essential upgrade format to make the hidden main step. However, some new needs must be met to achieve this aim. Data storage is one of the most important cloud computing facilities in the world. Although cloud storage offers consumers great benefits, it poses new challenges for security. First, it must not be clear from an authorised group who carries out external customer computing for key changes that the real hidden key for cloud storage auditing is used. Recently, it is also proposed and researched how to resolve the critical exposure problem in the setting of cloud storage audits. To resolve this challenge, current solutions all need customers to upgrade their hidden keys at all times, which will eventually create new local burdens for consumer, particularly for people who have restricted computing outlets, such as mobile phones. Key exposure tolerance is a critical issue in many security systems for comprehensive cyber protection. If not, the brand-new vulnerability to defence will be brought about. Therefore, only an encrypted hidden key for the customer for cloud storage audit can remain with the approved group. Next, as the authorised outsourcing group knows only the encrypted hidden keys, key changes under the encrypted situation should be done. Third, to recover the true secret key in the encrypted edition which is contained in the accepted faction, it ought to be extremely effective for this client. With verification of the outsourcing of main changes, We formalise the meaning and protection style of the cloud storage audit protocol. In the formalised

security model, we demonstrate the protection in our protocol and defend its success in specific terms[2]. Lastly, the customer will be able to verify the validity from the encrypted secret key following the client retrieves it in the approved party. The purpose of this article is to design a protocol to audit cloud storage that can meet the needs of key updates outsourcing.

2. CONVENTIONAL DESIGN:

Key-exposure resistance happens to be an essential problem for in-depth cyber defense in lots of security applications. Lately, how to approach the important thing exposure issue in the settings of cloud storage auditing continues to be suggested and studied. To deal with the task, existing solutions all require client to update his secret keys in each and every period of time, which might inevitably generate new local burdens towards the client, especially individuals with limited computation sources for example cell phones. The issue is non-trivial naturally. When the client's secret key for storage auditing is uncovered to cloud, the cloud has the capacity to easily hide the information loss occurrences for maintaining its status, even discard the client's data rarely utilized to save the space for storage. Disadvantages: In existing system, it enquires the customer to update his secret keys in each and every period of time, which might inevitably generate new local burdens towards the client and fewer security.

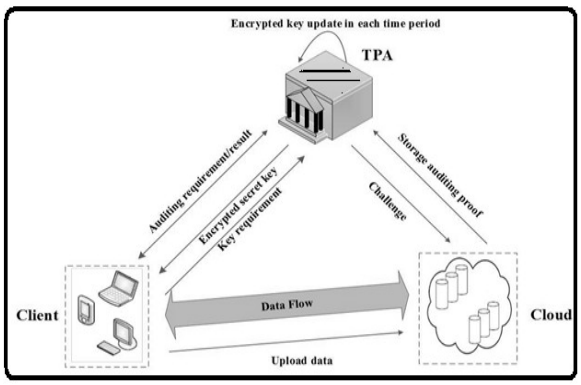


Fig.1.Proposed structure.

3. FORMALIZED SECURE DESIGN:

Within this paper, we focus regarding how to result in the key updates as transparent as you possibly can for that client and propose a brand new paradigm known as cloud storage auditing with verifiable outsourcing of key updates. Within this paradigm, key updates could be securely outsourced with a approved party, and therefore the important thing-update burden around the client is going to be stored minimal. Particularly, we leverage the 3rd party auditor (TPA) in lots of existing public auditing designs; allow it to act as approved party within our situation, making it responsible for both storage auditing and also the secure key updates for key-exposure resistance. Advantages: key updates could be securely outsourced with a approved party, and therefore the important thing-update burden around the client is going to be stored minimal. Supplying more security. We formalize the meaning and also the security type of the cloud storage auditing protocol with verifiable outsourcing of key updates. The safety proof and also the performance simulation reveal that our detailed design instantiations are safe and effective. Each one of these salient features is carefully designed to help make the whole auditing procedure with key exposure resistance as transparent as you possibly can for that client [3]. It can make our protocol secure and also the understanding operation efficient. Meanwhile, the TPA can complete key updates underneath the encrypted condition. T in the approved party and decrypts it just as he want to upload new files to cloud. Additionally, the customer can verify the validity from the encrypted secret key. Cloud storage auditing protocol with verifiable outsourcing of key updates. The customer can verify the validity from the encrypted secret key as he retrieves it in the TPA. The safety type of the cloud storage auditing protocol with verifiable outsourcing of key updates. We use three games to explain the adversaries with various compromising abilities who're from the security from the suggested protocol. Game 1 describes an foe, which fully compromises the OA to obtain all encrypted secret keys. Game 2 describes an

foe, which compromises the customer to obtain DK, attempts to forge a legitimate authenticator in almost any period of time. Game 3 offers the foe more abilities, which describes an foe, which compromises the customer and also the OA to obtain both Ask and DK previously period j, attempts to forge a legitimate authenticator before period of time j. The OA plays two important roles: the very first is to audit the information files kept in cloud for that client the second reason is to update the encrypted secret keys from the client in every period of time. The OA can be viewed as like a party with effective computational capacity or perhaps a service in another independent cloud. You will find three parties within the model: the customer, the cloud and also the third-party auditor (OA). The customer has the files which are submitted to cloud. The entire size these files isn't fixed, that's, the customer can upload the growing files to cloud in various time points. The cloud stores the client's files and offers download service for that client [4]. Traditional file encryption strategy is not appropriate since it helps make the key update hard to be completed underneath the encrypted condition. Besides, it will likely be even more complicated to allow the customer using the verification capacity to guarantee the validity from the encrypted secret keys. To deal with these challenges, we advise look around the blinding technique with homomorphic property to efficiently "encrypt" the key keys. We make use of the same binary tree structure to evolve keys that has been accustomed to design several cryptographic schemes [5]. This tree structure could make the protocol achieve fast key updates and short key size. One problem we have to resolve would be that the OA should carry out the outsourcing computations for key updates underneath the condition the OA doesn't be aware of real secret key from the client. Our security analysis afterwards implies that such blinding technique with homomorphic property can sufficiently prevent adversaries from forging any authenticator of valid messages. Therefore, it will help to make sure our design goal the key updates is as transparent as you possibly can for that client. To Get Rid Of the Encrypted Secret Key Verification from the Client, when the client isn't in urgent have to know if the encrypted secret keys downloaded in the OA are correct, we are able to remove his verifying operations making the cloud carry out the verification operations later. Within this situation, we are able to delete the VerEKey formula from your protocol. Whether it holds, then your encrypted secret key should be correct. In this manner, the customer doesn't need to verify the encrypted secret keys immediately after he downloads it in the OA. Within the designed Sys Setup formula, the OA only holds a preliminary encrypted secret key and also the client holds a understanding key which is often used to decrypt the encrypted secret key. Within the designed Key Update formula, homomorphic property helps make the secret key capable of being updated under encrypted condition and makes verifying the encrypted secret key possible. We assess the performance from the suggested plan through several experiments which are implemented with the aid of the Pairing-Based Cryptography library. We compare the important thing update time on client side between your both schemes. Once the client really wants to upload new files towards the cloud, it must verify the validity from the encrypted secret key in the OA and recover the actual secret key [6]. We demonstrate time from the challenge generation process, the proof generation process, and also the proof verification process with various quantity of checked data blocks. Within our plan, the communicational messages comprise the task message and also the proof message.

4. CONCLUSION:

When downloading new cloud files, the user must just retrieve the encrypted hidden key in the OA. In this article, we research how key cloud storage audit changes with key exposure resilience can be delegated. The authenticity of the cryptographic secret key can be checked when retrieved by the recipient in the TPA. This protocol outsources the main changes to the OA and therefore to this customer is clear.

The systematic safety data and the efficiency simulation of the proposed strategy are presented. Existing scheme doesn't like the checked outsourcing of main changes by auditing procedure. See secret client key without file encryption has been used by 3rd Party. The OA should perform outsource calculations for the main changes in compliance with the condition that the OA is not aware of the client's actual hidden key. Download the encrypted secret key by customer. With different quantities of regulated data blocks, we show the period from processes of challenge generation, method of proven generation and proof verification. The communications include the mission letter, and also the evidence message, in our strategy. We propose the first protocol for cloud storage audits that can be tested for main changes. In addition, it just sees the encrypted version of the hidden key to the client, which can be verified by the client when downloading them in the OA by using the encrypted secret keys.

REFERENCES:

[1] C. Guan, K. Ren, F. Zhang, K. Florian, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), 2015, pp. 203–223.

[2] B. Wang, B. Li, and H. Li Oruta, "Oruta: Privacy-preserving public auditing for shared data in the cloud," IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan./Mar. 2014.

[3] J. Yu, F. Kong, X. Cheng, R. Hao, and G. Li, "One forward-secure signature scheme using bilinear maps and its applications," Inf. Sci., vol. 279, pp. 60–76, Sep. 2014.

[4] Jia Yu, Kui Ren, Fellow, IEEE, and Cong Wang, Member, IEEE, "Enabling Cloud Storage Auditing With VerifiableOutsourcing of Key Updates", ieee transactions on information forensics and security, vol. 11, no. 6, june 2016.

[5] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[6] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," Int. J. Inf. Secur., vol. 4, no. 4, pp. 277–287, 2005.

DESIGNING A DELEGATION SERVICE FOR DATA OWNER IN SOCIAL OPEN NETS

Anumolu Anuradha[1]., K. Sneha [2]., Samatham N Gayathri [3]., Velagala Srinedhee[4]
1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- anuradha.anu503@gmail.com)
2, 3, 4 B.Tech IV Year CSE, (16RG1A0545, 17RG1A05K5, 17RG1A05K9),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT:

In the cloud publications, this paper focuses on proxy-focused data uploading and remote data integrity management. Customers are relieved from storage management burdens, access to common data with independent geographical areas, etc. using the public cloud network. This paper depends on the results of the studies of proxy encryption, identity-based public key cryptography and remote cloud data integrity. Our proposed ID-PUIC protocol is effective by using public-key identity based cryptology, so the administration of the certificate is removed. ID-PUIC is a completely novel, proxy-oriented, cloud-based data uploading and remote dataset management model. The manager is restricted to connecting to the network so that he can defend from collusion in the study. Nevertheless, a proposed ID-PUIC protocol can also carry out private remote controls, remote control of data integrity and public remote controls, as approved by the original client. But the legitimate business of the boss will be analysed throughout. For the ID-PUIC protocol we have a structured device model and safety model. We then developed the very first concrete ID-PUIC protocol in accordance with the bilinear pairings. Our ID-PUIC protocol is proven to be safe within the random oracle paradigm.

Keywords: Proxy public key cryptography, remote data integrity checking, cloud computing, identity-based cryptography.

1. INTRODUCTION:

To help more customers process their data in public cloud sites, new security issues must be addressed [2]. After the client has been set to use machines, he delegates his representative to process and upload his results. Cloud computing meets the needs of application over the last few years and is growing fast. Increasingly, consumers are therefore searching for the remote cloud storage infrastructure to store and process their results. Effective and scalable can be our ID-PUIC protocol. The proposed ID-PUIC protocol will execute private remote data integrity inspections, delegated remote data integrity checks and public remote data integrity checks according to the original customer authorization. However, remote data integrity control of public cloud storage can also be a critical security condition. Remote data integrity tests can be used to reassure cloud users to store their data intact. Thus, ID-PUIC protocol will be studied according to public identity-based cryptography and public key proxy encryption. The manager is restricted to connecting to the network so that he can defend from collusion in the study. But the ethical business of the boss continues in the analytical era. When you produce a lot of details, who will help you filter this information? If these results cannot be handled on time, the manager risks a monetary loss. Public controls will be subject to the risk of data degradation. The difficult administration of certificates can be rid of identity-based public encryption. The proxy-orientated data upload and remote data integrity inspection based on identification is far more enticing to increase performance. This paper focuses on proxy-based data uploading and remote data integrity checking in public cloud locations[2]. Our proposed ID-PUIC protocol is effective by using public-key identity based cryptology, so the administration of the certificate is removed. ID-PUIC is a completely novel, proxy-oriented, cloud-based data uploading and remote dataset management model. The manager must delegate the proxy to process his results, for example his assistant, in order to prevent the situation. However, the manager does not hope anyone will verify the integrity of remote data. For the ID-PUIC protocol we have a structured device model and safety model. We then developed the very first concrete ID-PUIC protocol in accordance with the bilinear

pairings. The original client will connect with computers to assess remote data integrity in our proposed ID-PUIC protocol. Effective and provenly stable should be the working ID-PUIC protocol. Performance measurement should be carried out according to correspondence and calculation overheads. We formalise the protection sense of an ID-PUIC protocol to address these safety needs.

2. EXISTING SYSTEM:

In public places cloud atmosphere, most clients upload their data to Public Cloud Server (Computers) and appearance their remote data's integrity by Internet. Once the client is definitely an individual manager, some practical problems may happen. When the manager is suspected to be involved in to the commercial fraud, he'll be removed through the police. Throughout analysis, the manager is going to be limited to connect to the network to be able to guard against collusion [3]. But, the manager's legal business goes on throughout analysis. Whenever a large of information is generated, who are able to help him process these data? If these data can't be processed just over time, the manager will face losing economic interest. To avoid the situation happening, the manager needs to delegate the proxy to process its data, for instance, his secretary. But, the manager won't hope others be capable of carry out the remote data integrity checking. Public checking will incur some danger of dripping the privacy. For instance, the stored data volume could be detected through the malicious verifiers. Once the submitted data volume is private, private remote data integrity checking is essential. Even though the secretary is able to process and upload the information for that manager, he still cannot look into the manager's remote data integrity unless of course he's delegated through the manager. We call the secretary because the proxy from the manager. In PKI (public key infrastructure), remote data integrity checking protocol will work the certificate management. Once the manager delegates some entities to do the remote data integrity checking, it'll incur considerable overheads because the verifier will look into the certificate if this checks the remote data integrity. Disadvantages of Existing System: In PKI, the considerable overheads range from heavy certificate verification, certificates generation, delivery, revocation, renewals, etc. In public places cloud-computing, the finish devices might have low computation capacity, for example cell phone, iPod, etc.

3. PROPOSED SYSTEM:

In public places cloud, this paper concentrates on the identity-based proxy-oriented data uploading and remote data integrity checking. By utilizing identity-based public key cryptology, our suggested ID-PUIC protocol is efficient because the certificate management is eliminated. ID-PUIC is really a novel proxy-oriented data uploading and remote data integrity checking model in public places cloud. We provide the formal system model and security model for ID-PUIC protocol [4]. Then, in line with the bilinear pairings, we designed the very first concrete ID-PUIC protocol. Within the random oracle model, our designed ID-PUIC protocol is provably secure. In line with the original client's authorization, our protocol can realize private checking, delegated checking and public checking. Benefits of Suggested System: The concrete ID-PUIC protocol is probably safe and effective using the formal security proof and efficiency analysis. We provide the formal definition, system model, and security model [4]. Then, a concrete ID-PUIC protocol was created while using bilinear pairings. The suggested ID-PUIC protocol is provably secure in line with the hardness of computational Diffie-Hellman problem. In line with the original client's authorization, our protocol can realize private checking, delegated checking and public checking. We advise a competent ID-PUIC protocol for secure data uploading and storage service in public places clouds. Bilinear pairings technique makes identity-based cryptography practical. Our protocol is made around the bilinear pairings. We first evaluate the bilinear pairings. The concrete ID-PUIC

protocol is probably safe and effective using the formal security proof and efficiency analysis. However, the suggested ID-PUIC protocol may also realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking in line with the original client's authorization. Our suggested ID-PUIC protocol satisfies the non-public checking, delegated checking and public checking. Our contributions will also be appropriate for that scenario of hybrid clouds, in which the proxy may be treatable because the private cloud from the original client. Motivated through the application needs, this paper proposes the novel security idea of ID-PUIC in public places cloud. We advise a competent ID-PUIC protocol for secure data uploading and storage service in public places clouds. Bilinear pairings technique makes identity-based cryptography practical. Our protocol is made around the bilinear pairings. We first evaluate the bilinear pairings. Then, the concrete ID-PUIC protocol was created in the bilinear pairings. Finally, in line with the computation cost and communication cost, we provide the performance analysis from two aspects: theoretical analysis and prototype implementation. This concrete ID-PUIC protocol comprises four procedures: Setup, Extract, Proxy-key generation, TagGen, and Proof. To be able to show the intuition in our construction, the concrete protocol's architecture is portrayed [5]. First, Setup is conducted and also the system parameters are generated. In line with the generated system parameters, another procedures are carried out. Within the phase Extract, once the entity's identity is input, KGC generates the entity's private key. Especially, it may create the private keys for that client and also the proxy. Within the phase TagGen, once the data block is input, the proxy generates the block's tag and uploads block-tag pairs to Computers. Within the phase Proxy-key generation, the initial client produces the warrant helping the proxy create the proxy key. Within the phase Proof, the initial client O interacts with Computers. With the interaction, O checks its remote data integrity. First, we provide the computation and communication overhead in our suggested ID-PUIC protocol. Simultaneously, we implement the prototype in our ID-PUIC protocol and evaluate it is time cost. Then, we provide the versatility of remote data integrity checking within the phase Evidence of our ID-PUIC protocol. Finally, we compare our ID-PUIC protocol using the other up-to-date remote data integrity checking protocols. To be able to show our protocol's practical computation overhead, we've simulated the suggested ID-PUIC protocol by utilizing C programming language with GMP Library and PBC library. Thus, we simply think about the communication cost that is incurred within the remote data integrity checking [6]. Our suggested ID-PUIC protocol satisfies the non-public checking, delegated checking and public checking. Our contributions will also be appropriate for that scenario of hybrid clouds, in which the proxy may be treatable because the private cloud from the original client. Upon finding the original client's instruction, the non-public cloud will communicate with the general public cloud and finished the information uploading task. The safety in our ID-PUIC protocol mainly includes the next parts: correctness, proxy-protection and enforceability.

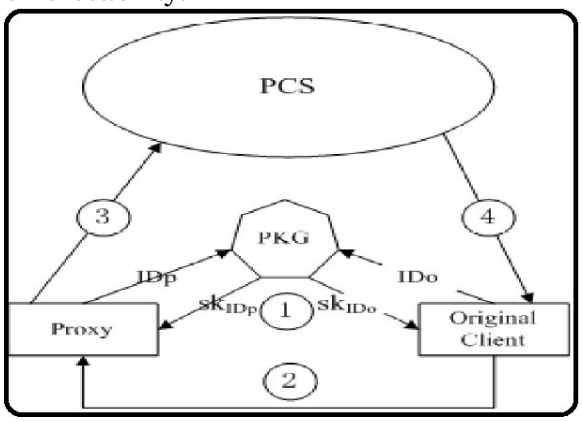


Fig.1.Proposed system

4. CONCLUSION:

The text formalizes the device architecture and security model of ID-PUIC. Then, with the help of bilinear pairing technology, the very first practical protocol was created. In some

particular situations, the owner of the information can only log into the public cloud server. The owner of the information may assign to the third party, such as the proxy, the information processing work. The remote data integrity management protocol should be effective, on the other hand, to make it ideal for finishing devices that are power constrained. With structured security and efficiency analytics, the concrete ID-PUIC protocol is likely secure and reliable. The overall costs in PKI vary from the authentication of heavy certificates, the development, distribution, cancellation, renovation of certificates, etc. The non-public server receives the proxy and the permission from the original client for your original client to communicate with the private cloud. Public cloud storage can offer low computing ability on finishing devices like mobile phones, ipads, etc. In the case, the private/public key pair would come from the non-public cloud.

REFERENCES:

[1] J. Zhang, W. Tang, and J. Mao, "Efficient public verification proof of retrievability scheme in cloud," Cluster Comput., vol. 17, no. 4, pp. 1401–1411, 2014.

[2] Huaqun Wang, Debiao He, and Shaohua, "Identity-Based Proxy-Oriented Data Uploading andRemote Data Integrity Checking in Public Cloud", ieee transactions on information forensics and security, vol. 11, no. 6, june 2016.

[3] E. Zhou and Z. Li, "An improved remote data possession checking protocol in cloud storage," in Algorithms and Architectures for Parallel Processing (Lecture Notes in Computer Science), vol. 8631. Berlin, Germany: Springer-Verlag, 2014, pp. 611–617.

[4] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Trans. Services Comput., vol. 5, no. 2, pp. 220–232, Apr./Jun. 2012.

[5] P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," Chin. Sci. Bull., vol. 59, no. 32, pp. 4201–4209, 2014.

[6] B. Lynn, "On the implementation of pairing-based cryptosystems," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2008.

SECURED DATA TRANSMISSION IN WIRELESS AND PORTABLE STORAGE DEVICES THROGH WI-FI NETWORK

Dr. Archek praveen kumar[1]., V.Uma devi[2]., M.Devarshini[3]., G.Kavya[4]., M.Kavya [5]

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: archekpraveen@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The world of wireless is changing rapidly. The analytics and development technologies listed below promise to provide value-added services to additional users in less time. The secure transfer of knowledge has become a serious problem, especially in the education system. In order to ask questions during exams, you need a fast and reliable system with the right system. During this project, a safer and faster approach to direct finishing is planned to complete the transfer of knowledge. This method collects information from a device and transmits it securely to another device over a wireless network. The secure information material, which is mainly based on a microcontroller, is transmitted via WI-FI electronic devices. By misapplying wireless technology, we tend to design our communications as reliable and wireless. As part of this project, we usually offer users distributed authentication, which provides instant access to the network without manual interaction. It maintains the quality of the terminals at the access points and at the same time protects the operator's infrastructure from external attacks. User information sent over the wireless connection is protected from psychological phenomena by the IPSec protocol. With this technique, questions can be easily passed before the exam begins if an authorized person from the main workplace or university sends them to the school. At the same time, information is encrypted throughout the entire transmission to protect access to another user's information. In addition, the system provides for confirmation of receipt of documented information about mobile devices.

Keywords— USB module, cloud, Wi-Fi module, etc.

1. INTRODUCTION

Advanced communication technologies have made it possible to work with information systems in completely different ways. A job information system is a system that collects data at one end and passes it on to the other. These square devices typically measure handheld or mobile devices, are lightweight, battery operated, and can store telemetry information. As part of this work, it is planned to create an innovative system of associate degrees in response to the receipt of information and its transmission around the world through a secure environment. Wireless technology, i.e. H. WI-FI is used throughout this system to transfer information securely. This method is used in all areas, especially in the field of education management. The information you send is stored on a mobile USB (Universal Serial Bus) device and connected to the system. The system microcontroller reads the information and sends it to the server via WI-FI. The server sends information to the recipient. This is where the server stores information that improves security. Send information directly to the recipient via WI-FI. Thus, the examination board questionnaire will be sent directly to the director or head of the training center with a high degree of confidence. In addition, a digital display (Liquid Crystal Display) is connected to the system, which shows the operating status of the system. Users send information around the world without disclosing it anywhere. This can be used in intensive distributed domain applications for synchronous remote transmission of information.

2. LITERATURE SURVEY

In fact, there are several wireless technologies in the world: each has its own advantages, none of them is perfect. You just need to answer the question, "Which technology is best for my application?" I hope this has helped you better understand popular wireless technologies for WI-FI, their strengths and weaknesses. Additional issues beyond this technology area are unit prices, ease of integration, and security. We are seeing a significant improvement in overall flexible pricing and easy integration with several new products, each with wireless connectivity, which is a trend. Pricing and integration efforts should be further considered in the context of specific applications. Security aspects of WI-FI applications include supported features of individual protocols as well as accessory and code issues.

3. METHODOLOGY USED

Wi-Fi technology conforming to the IEEE 802.11 standard has been developed as a wireless replacement for the preferred wired LAN IEEE 802.3. As such, it was built for web ownership from day one. While Wi-Fi technology primarily determines the data link layer of a local area network, people who claim to be victims of Wi-Fi implicitly imply that they also use TCP / IP for web ownership. The Wi-Fi AP is used in most homes these days, but it is used in most offices, schools, airports, convenience stores and retail stores. The tremendous success of Wi-Fi is primarily due to the exceptional capabilities of programs outside of the Wi-Fi Alliance and the growing market demand for simple, affordable Internet access. Wi-Fi is already built into all new laptops, tablets, good phones and TVs. The next step of Wi-Fi is connecting to the Internet for the new age of things. Wi-Fi networks have a network topology and the access point is the web gateway. Most Wi-Fi networks use a pair of 4 GHz bands. Wi-Fi can work even in the 5 GHz band, which has additional channels and a zone with a higher data transfer rate. Since the variation for 5 GHz indoor radios is shorter compared to a 4 GHz pair, five gigahertz per second is mainly used in business applications along with multiple access points to confirm adequate Wi-Fi coverage. In short, Wi-Fi is the most widely used wireless web technology today. High performance and complexity have been major stumbling blocks for IoT developers, but new semiconductor devices and modules are lowering many barriers and transforming Wi-Fi integration into growing IoT devices and applications.

Proposed functional diagram:

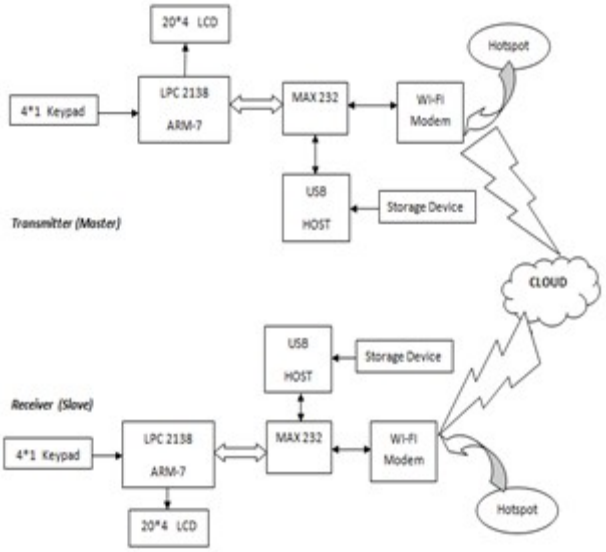


Figure 1. The proposed system

DESCRIPTION OF THE FUNCTIONAL DIAGRAM:

The basic block diagram of wireless secure data transmission between portable storage devices over a WI-FI network is shown in the figure above. This diagram mainly consists of the following main blocks.

1) ARM 7 LPC 2138
2) MAX 232
3) USB Host
4) LCD Display
5) WIFI Modem
6) Power Supply
7) Keypad

4. SCHEME USED

At the end of the transfer, the microcontroller reads the information stored in the first device and sends it to the server via the WI-FI module. The server starts communicating with another WI-FI module and sends the information to the second USB device at the end of the receiver. In this way, knowledge is transferred wirelessly between 2 free USB sticks in completely different fields. The display device used here is a liquid crystal display with 16 x 2 characters per line to indicate the operating conditions of the system. It consists of programming the microcontroller and optimizing the circuit as

an onboard system. The organizational structure of the program is as follows:
Transmission:

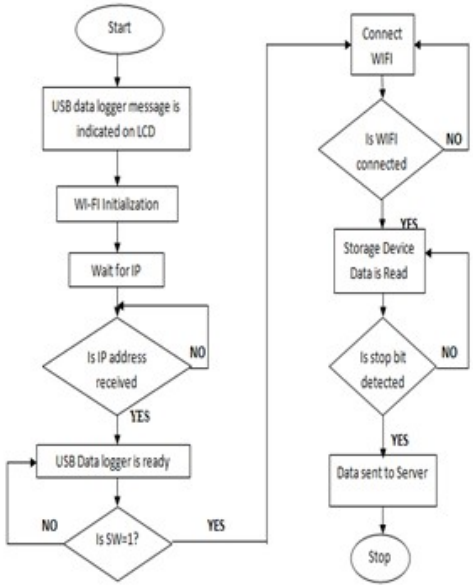


Figure 2. Organizational structure of the emission department
Reception:

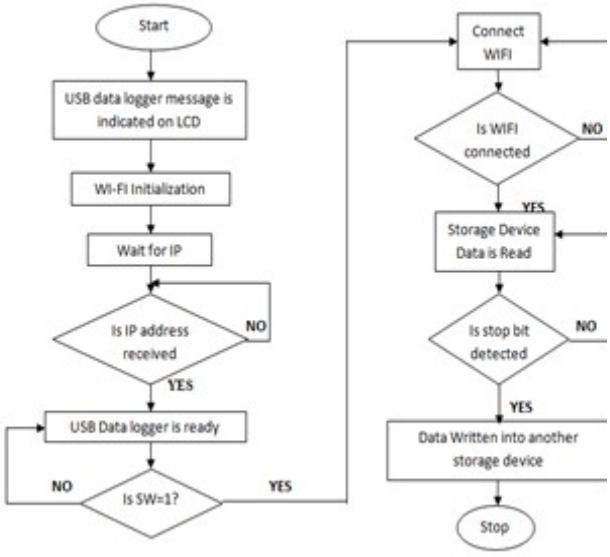


Figure 3. Recipient organization chart

5. RESULT AND DISCUSSION

This article mentions an example for the purpose of remote sensing and transmission operation of serial communication methods. The rule for this job applies only to the transfer of text files or documents. The required changes are created as part of the rule and can be applied to the sending and receiving of transfer files. Since it uses an ARM processor, the rule is less complicated. Compared to a microcontroller, the ARM processor consumes much less power (3.3 volts). This example will be used to develop a portable device the size of a USB device that the user can carry around. The address for processing operational information in the (Internet Protocol) format of the device makes it more secure.

6. CONCLUSION

With this technology, information is transmitted over long distances, which simplifies programming and makes ARM design possible even for complex applications. The hardware complex includes printed circuit boards (printed circuit boards) in all integrated circuits with all the necessary elements. For example, ARM seven LPC 2138, MAX232, LAN module, keyboard. Together we tend to measure the planning unit 2 of this technique as a square. One can act as a master and the other as a slave. LAN Modules are a means of transferring knowledge over the cloud. The cloud storage tag name is available for each disk throughout the entire schedule. Together, the system provides cryptography and confirmation of the state of knowledge, and the result is also displayed on an alphanumeric display, and the transmitted data can also be recorded at the receiver end.

REFERENCES

1. O'Brien K, Salyers D.C, Striegel A.D, Poellabauer C ”Power and performance characteristics of USB flash drives, World of Wireless, Mobile and Multimedia Networks”11th IEEEInternational Symposium.June-2008 and also published in International Journal of Advanced Computer Science and Applications.
2. Anuj Kumar, I. P. Singh, and S. K. Sud “Design and Development of Multi-Channel Data Logger for Built Environment “, Proceedings of International Multi-Conference of Engineers and Computer scientists 2010 Vol II ,IMECS 2010 ,Hong Kong,PP:993-998.
3. Remple, T. B. , Qualcomm, San Diego, CA, USA , June 2003 "USB on-the-go

interface for portable devices", Consumer Electronics, IEEE International Conference, ICCE. 2003.

4. ShyamSadasivan, " An Introduction to the ARM CORTEX – M3 Processor", October 2006.
5. Sifeng Zhang, Keli Zhang, Ping Cao, Yanfang Wang. "Design and Realization of Remote Synchronous Data Transmission System Based on Distributed Architecture of Serial Concurrent Bus". IEEE proceedings of the 9th International Conference on Electronic Measurement & Instruments. Beijing, China, Aug.2009, Volume 3 PP: 358-362.

AUTOMATED BILLING SYSTEM FOR SHOPPING CART USING BARCODE AND IMAGE PROCESSING TECHNIQUE IN LABVIEW

Dr I. Selvamani [1]., M.Tejasree[2]., M.Srilakshmi[3]., G.Aruna[4]., M.Kavya [5].,

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: i.selvamani@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0443, 17RG1A0442, 17RG1A0428, 17RG1A0423), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— A mall is a place where almost all city dwellers go shopping for everyday needs such as groceries, clothing, electrical appliances, etc. Shopping malls are very common in big cities compared to cities. The area of these malls is also very large, so shoppers can make their spacious purchases without overloading. All products in the mall are barcoded. Barcode is the oldest technology we have been using for years. Each product has a barcode that is attached to the back of the product. Carts are commonly used in shopping malls for shopping. As we all know, it takes a long time for the crowd to go to the checkout counters for final settlement. Customers will also not know the price and quantity of items they have added to their cart. In this article, we will create a system to solve this problem by automatically invoicing the shopping cart itself, getting detailed information about the cost of each product and counting the number of products placed in the shopping cart, modifying the functionality of the shopping cart, or adding an existing barcode system that becomes a cost effective system.

Keywords— barcodes, ID, Raspberry Pi, webcam, LCD screen, beep, switch, Lab VIEW

.

1. INTRODUCTION

A shopping center is a place where you can find almost any product. Almost weekends of the week are great for shopping in these malls. Shopping malls are very common in big cities compared to cities. The area of these malls is also very large, so shoppers can make their spacious purchases without overloading. As the city and technology improve, the infrastructure of these shopping centers improves on this basis. [2] Updating these malls with technology is also very important as customers are also expecting an improved version of Cozy. All products in the mall are barcoded. Barcode is the oldest technology we have been using for years. Each product has a barcode that is attached to the back of the product. These barcodes require line-of-sight, which is one of the drawbacks. It is also very slow in terms of speed. As we all know, when we enter shopping malls, we must take a cart with us so that we can leave the desired products. After placing all the products requested by the customer, he must go to the counter to pay the bill. If there are many people queuing at the billing counter, we will have to wait in line until we can make the final payment. There, the invoice manager scans the barcode of each product and then issues the final invoice, which takes a long time. In addition, it is labor-intensive on accounting counters. [3] If the total value of the products exceeds the customer's budget, the buyer must recall the products so that they equal the total value of the products, which is very frustrating. Hence, there are some problems with the existing barcode system.

Customers are unhappy with waiting longer queues. [4]

It takes a lot of human strength, and it's expensive.

There is no information on the total cost of products.

To overcome these problems, we have proposed a design that avoids these problems. We have developed a design that performs automatic invoicing, reduces customer time, is less labor intensive, and therefore less expensive. [5] Plus, customers don't have to stand in long lines. We also solved the problem of informing the buyer about the total cost of the product before going to the checkout, which also brings satisfaction to the buyer.

2. PROPSED SYSTEM

2.1 Billing Unit

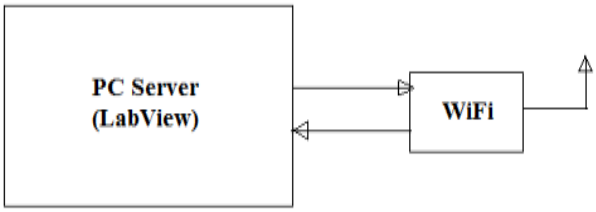


Fig. 1: Billing Unit

The metering unit consists of a PC that acts as a server on which LabVIEW is used to start shopping cart accounting. LabVIEW acts as a single server at the designated mall, using or having access to all carts. Wi-Fi is used to return decoded barcode and ID values to the Raspberry Pi. In addition, the program is written in LabVIEW, i.e. the file write is programmed and from there the data is written back to the Raspberry Pi file, so that from there it goes to the LCD screen and shows all the details of that particular product for the customer's display purposes.

2.2 Trolley Unit

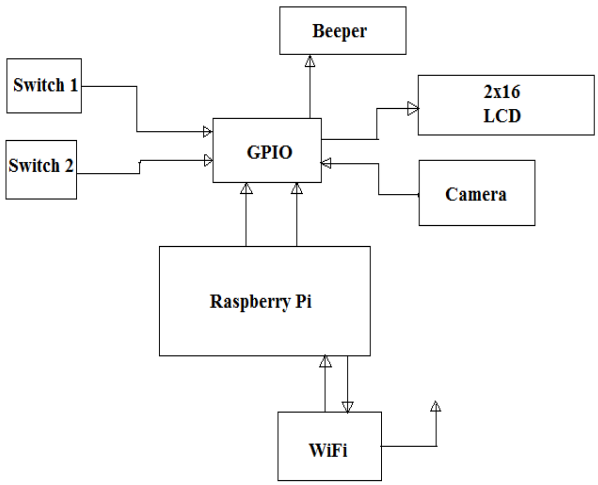


Fig. 2: Trolley Unit

In this device, the Raspberry Pi is connected to a camera. A button is used that, when pressed, clicks on the product barcode image, adds the product value to the total invoice amount, and displays it on the LCD screen. The beep is also used to beep after clicking on the barcode image to notify customers that they can add a product to their cart.

3. DESCRIPTION OF THE SOFTWARE

It is a server that is used for network purposes to exchange files or folders between the Raspberry Pi and other devices such as a PC or laptop. We have used this software at the account level so that it does all the decoding of the barcode and product ID. Only here we have various techniques for decoding and obtaining product information. Before making a purchase, the basket number is checked against the product number database. If they match, then the specific buyer is granted permission to purchase. When a customer buys a product, they have to click a button to indicate that they are adding a product and therefore a value must be added. Then the buyer must first hold the item in front of the camera. A beep will sound to indicate that the camera has captured an image of the barcode ID and can now be added to the cart.

While the camera clicks on the barcode and product ID image, the image captured by the camera is transmitted to the Raspberry Pi. The image is sent from the Raspberry Pi to the PC (LabVIEW) using Samba software, which is used for networking purposes between the Raspberry Pi and the PC. There, in LabVIEW, you need to specify the path to the corresponding folder in which the images that you clicked will be saved. Authentication is done automatically when the image file is loaded in the folder path. The barcode and ID are then decoded using pattern and barcode recognition techniques located at the checkout.

As soon as the image is in the file path, authentication starts automatically. This means that the image is loaded into the program and its work is done. The decoded value is checked internally against the product database, which will already be stored in system memory. All product information will be stored in a barcode and ID based database along with all information such as product name, price and weight.

4. RESULTS AND DISCUSSION

This is the product database against which the decoded barcode value is compared. In the database, we would store all product details such as barcode value, name, product weight

and cost. Depending on this, details are displayed on the LCD screen.

Database of the products

Bar Code No	Unique ID	Product Name	Cost of the products
0000	0000	0000	0000
8901216812338	511	Kamasutra Deo Spray	250
4005808163588	241	Nivea Deoderant	199
8901052087808	223	Tetley Green Tea	90
8901396184003	269	Harpic Toilet Rim	57
8901207018268	245	Meswak Toothpaste	120
8901531300015	793	Boroline	32
8902442208636	996	Navneet 300 pages Notes	110
8901030475580	788	Tresemme Conditioner	171
8906057531301	346	Medimix 3 packs	95
8904187000711	110	Fash Facewash	130
8906067520012	111	D-Free Anti Dandruff	110

Fig. 3: Product database

In the next step after capturing the product barcode image, the barcode value must be decoded using the barcode recognition method. This is how it looks when recognizing a barcode.

The file path in the picture is the path to the picture, the barcode of which we want to check. That is why we have to show the way every time.

The split barcode is the value of the recognized barcode. A sample image is nothing more than a matching identifier.

Fig. 4: Barcode and ID recognition

An index is nothing more than a barcode and id positions in a database table. Based on the discovery, we get the index number, and based on the index number, we get the product details.

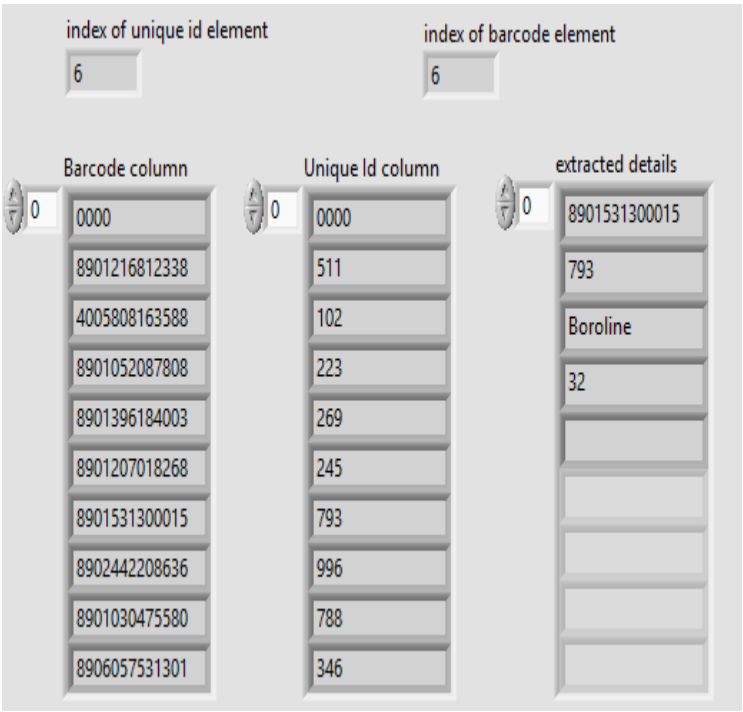


Fig. 5: Parts removed from the product

This extracted information should be printed on the final invoice as a reference to the customer. Once the product information has

been retrieved, it should be returned to the Raspberry Pi by writing code called writing to a text file in LabVIEW. This detail is then displayed on the LCD screen for the convenience of the buyer.

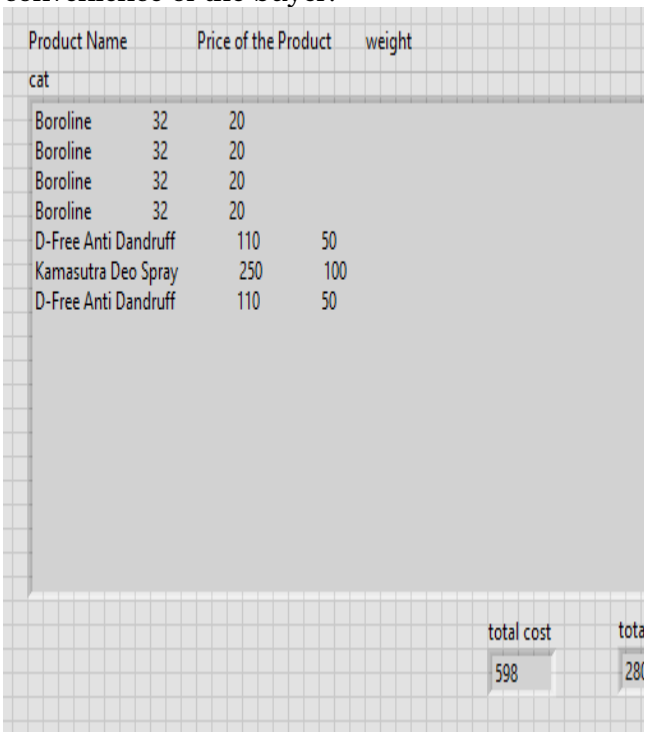


Fig. 6: Final score

This final bill is then sent to the Raspberry Pi for display on an LCD screen to make life easier for the buyer.

Fig. 7: Show product details

5. CONCLUSION & FUTURE WORK

Barcode is the oldest technology we have been using for years. Each product has a barcode that is attached to the back of the product. Carts are commonly used in shopping malls for shopping. As we all know, it takes a long time for the crowd to go to the checkout counters for final settlement. Customers will also not know the price and quantity of items they have added to their cart. In this article, we will create a system to solve this problem by automatically invoicing the shopping cart itself, getting detailed information about the cost of each product and counting the number of products placed in the shopping cart, modifying the functionality of the shopping cart, or adding an existing barcode system that becomes a cost effective system. For safety reasons, set up a platform near the mall exit to check the total weight of the products. Applying the IOT concept on the billing counter so that the total amount of purchases made in shopping malls is sent to the head office for accounting purposes.

REFERENCES

1. Galande Jayshree, Rutuja Gholap, Preeti Yadav, P.R.E.C. Loni, Ahmednagar, “RFID Based Automatic Billing Trolley”, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014).
2. Murulidhara N, SreeRajendra, “Automated Shopping and Billing with Product Inventory Management System”, July 2015 | IJIRT | Volume 2 Issue 2 | ISSN: 2349-6002.
3. Mrs.Meenakshi M.E., Joshiba Amali.S, Divya P.M, “Smart Trolley and Automatic Billing”, International Journal of Advanced Research in Biology Ecology Science and Technology(IJARBEST), Vol. I, Special Issue I, August 2015 in association with Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai.
4. Udita Gangwal, Sanchita Roy, Jyotsna Bapat, International Institute of Information Technology – Bangalore, “Smart Shopping Cart for Automated Billing Purpose Using Wireless Sensor Networks”, Sensorcomm 2013: The Seventh International Conference on Sensor Technologies and Applications.

5. S. Sainath, K. Surender, V. Vikram Arvind Final Year, Department of Computer Science and Engineering Hindustan University Chennai, India, J. Thangakumar, Ph.D. Assistant Professor, Department of Computer Science Hindustan University, Chennai, India, "Automated Shopping Trolley for Super Market Billing System", International Conference on Communication, Computing and Information Technology (ICCCMIT-2014).

PERFORMANCE ANALYSIS AND NETWORK LIFESPAN IMPROVEMENT IN WSN USING ARTIFICIAL BEE COLONY ALGORITHM BASED SENSOR DEPLOYMENT TECHNIQUES

Ch. Keerthi[1]., G.Bharani[2]., J.Lasyavi[3]., M.Sana[4]., S.Yeshwitha[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (: krith@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0424, 17RG1A0432, 17RG1A0446, 17RG1A0454),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Wireless sensor networks are composed of power-limited nodes and are used to collect useful information in the field. At WSN, it is important to efficiently collect information. If nodes are randomly initialized, not all nodes can be used efficiently, reducing the life of the network. In this article, we will implement an artificial bee colony algorithm to properly deploy sensor nodes and calculate network lifespan based on the upper limit for this configuration. Simulation results show that artificial colony works better compared to random and heuristic use to improve web life.

Keywords— wireless sensor network, provisioning, scheduling, upper limit, network lifespan

.

1. INTRODUCTION

A wireless sensor network is nothing more than a collection of a large number of sensor nodes. Each sensor node consists of sensors, actuators, memory and transceivers. Network coverage and lifespan are the two main critical wireless sensor network issues that we will focus on in this article. The coverage area should ensure that all targets in the area of interest are tracked with the required degree of reliability. Typically, coverage answers questions about the quality of service (monitoring) that a particular sensor network can provide. There are multiple POIs in a given target coverage region and the sensors must cover all points. Sensors collect data by tracking targets in their detection area. Thanks to the technologies currently available, the sensors are powered by batteries. Due to battery limitations, extending the life of the wireless sensor network is a critical issue. In the case of coating problems, the expiration date is the time during which all targets or areas are continuously covered. There are two main modes for the sensor radio on the network: active and standby. Sleep means the radio of the sensor turns off when there is no activity, if it is active, it means the radio is on and the active sensors can detect the environment. The sensor can only work in one mode at a time. Standby power consumption is 0 . 03W is much less than active, which ranges from 0.38W-0.7W. In this article, we will implement an artificial bee colony algorithm for providing sensor nodes in a wireless sensor network and compare its result with heuristic and random initialization methods.

2. PROPOSED METHOD

The proposed method consists of implementing the ABC (artificial bee colony) algorithms and comparing the results of the ABC algorithm with a random provisioning algorithm and a heuristic provisioning algorithm.

Random arrangement:

A large number of sensor nodes are randomly placed in a controlled area, which is difficult to access. Inadvertent deployment affects the life of the network in the WSN because this deployment method does not provide the coverage required.

Heuristic use:

This method provides more efficient results than a random implementation. This method moves the sensor to cover a large number of targets. This allows a large number of roofing sets to be formed. To do this, first randomize all nodes and move all inactive nodes to the least tracked node. Now move all the nodes to the center of the targets they cover. In addition, the closest target needs to be identified and the node will again be placed in the middle of those shared targets. If the knot can also cover this new target, the knot can move. If not, skip this step and finally calculate the ceiling.

The effectiveness of heuristic provisioning is clear from the flowchart shown in Figure 1.

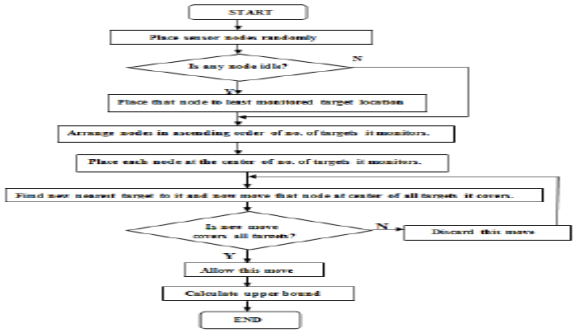


Fig. 1 Flow chart of heuristic support

3. RESULTS OF SIMULATION.

Simulations to analyze the performance of random, heuristic, and ABC initialization are performed first in an area of 300 mx 300 m and then scaled down to 400 mx 400 m.For two zones in the region, the ABC comparison with randomization and heuristics is obtained by changing the following parameters. The simulation is done with Matlab1012a.

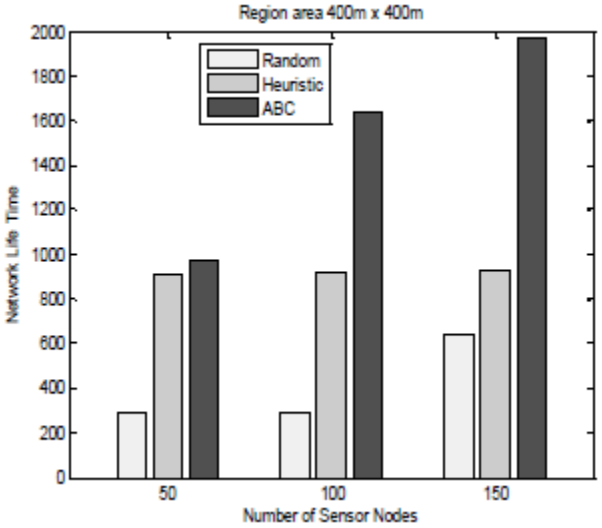
Sr. No.	Specification	Value
1	Region area	300m X 300m and 400m X 400m
2	Number of Targets	30, 40 and 50
3	Number of sensor node	50,100, 150
4	Sensing Range	30m to 50m
5	Sensor node battery power	1000 units

Table -1: Table of technical characteristics

Case I. Performance analysis for changing the number of sensor nodes.

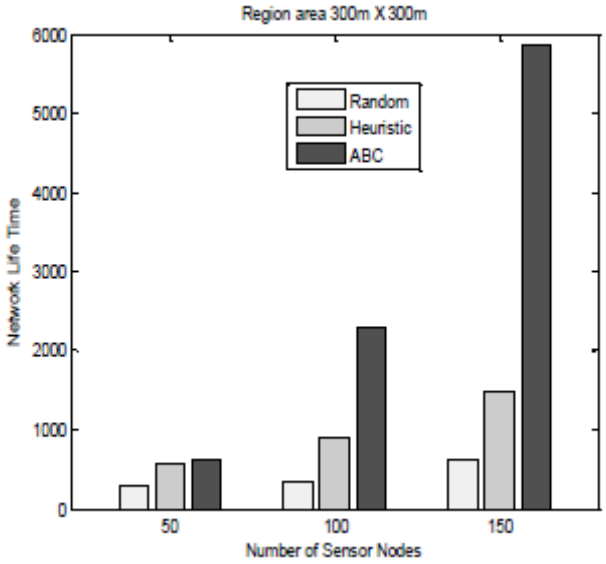
Number of heads = 25

Sensing node detection range = 50 m



Graph -1 : Effect of changing sensor nodes

Sr. No.	Area (Sq. meter)	Range (meter)	No.of Sensors	No.of Targets	Network Lifetime		
					Random	Heuristic	ABC
1	100	20	50	25	298	1226	5054
2	150	20	50	25	299	887	2635
3	200	20	50	25	280	554	868
4	250	20	50	25	274.6	588	658
5	250	20	75	25	279.6	896	2454
6	250	20	100	25	304	1122	3320

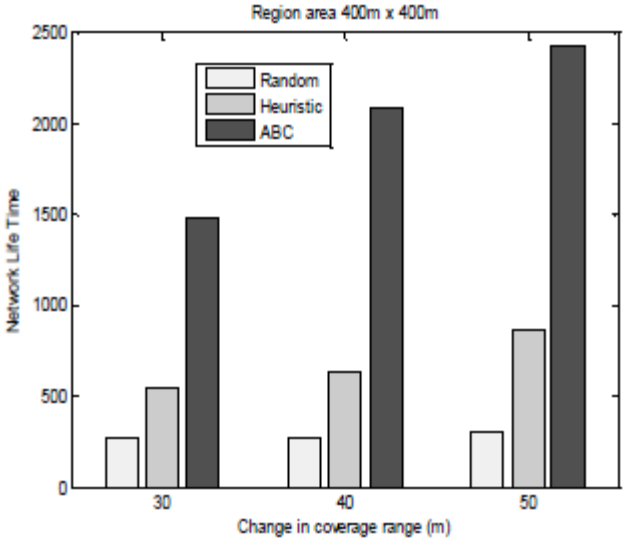


Graph -2 : Effect of changing sensor nodes

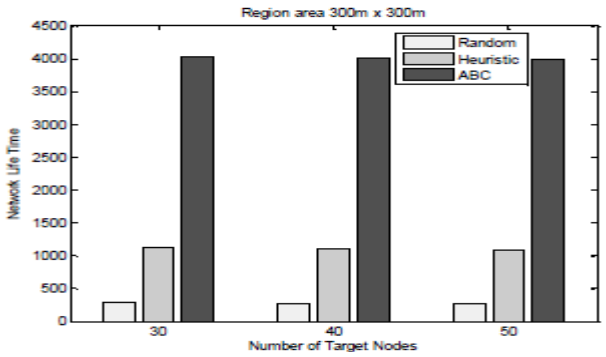
Case II: Performance analysis for changing the coverage area (detection) of sensor nodes such as 30 m, 40 m and 50 m.

Number of sensor nodes = 100

Number of heads = 25



Graph -3 : Effect of changing the detection area



Graph 4 : Effect of changing destination nodes

Table -2: Impact on network life with 20 m detection Vary

6. DISCUSSION OF THE RESULTS

The ABC performance is significantly better than the random and heuristic delivery shown in all charts. This is an improvement in one of the performance metrics of a wireless sensor network using such techniques to deploy sensor nodes in a WSN. The simulation results also show that as various WSN parameters change, the performance of the ABC implementation algorithm becomes more and more efficient compared to the basic heuristic and random implementation algorithm.

As the area of the region increases, while other parameters of the WSN remain constant, the life of the network decreases, as shown in all three cases. As the area of the area increases, the sensor nodes will become more dispersed in use. Consequently, the number of sensor nodes covering the target is reduced. Because of this, the coverage kits that provide the required coverage are also reduced, which affects the lifespan of the network.

As in this situation, there is a possibility that more sensor nodes can cover the target. Due to this, a large number of roofing games will be formed. Having more coverage sets in the WSN during planning will improve the life of the network. The same results are obtained by increasing the detection area of the sensor nodes. Because as the detection range of the sensor node increases, more targets that are close to most targets can enter the range sensor node. Thus, case II shows this improvement in network life as the detection range of the sensor node increases.

7. CONCLUSION

In this article, we discuss the performance of artificial, heuristic and random algorithms for initializing bee colonies. The network survives the longest when the ABC algorithm is used to implement sensor nodes in a wireless sensor network. Although WSN changes other parameters compared to other implementations, the ABC implementation algorithm is superior in all situations. Future work is to investigate the performance of thin-provision scheduling algorithms to extend the life of the network with the required target coverage.

REFERENCES:

1. K. Dasgupta, M. Kukreja, and K. Kalpakis, " Topology-aware placement and role assignment for energy-efficient information gathering in sensor networks", in Proc. IEEE ISCC, 2003, pp. 341–348.
2. T. Nieberg, J. Hurink, and W.Kern, "Approximation schemes for wireless networks" ,ACM Trans .Algorithms, vol. 4,no. 4, pp. 49:1–49:17, Aug. 2008.
3. M. Cardei, M. T. Thai, Y. Li, and W. Wu, "Energy-efficient target coverage in Wireless sensor networks" , in Proc. 24th Annu. Joint Conf. IEEE INFOCOM, Mar. 2005, pp. 1976–1984.

4. S. Mini, S. K. Udgata, and S. L. Sabat,"Sensor deployment in 3-D terrain using artificial bee colony algorithm", in Proc. Swarm, Evol. Memetic Comput., 2010, pp. 424–431.
5. K. Kar and S. Banerjee, "Node placement for connected coverage in sensor networks", in Proc. Model. Optim. Mobile, Ad Hoc Wireless Netw.,2003, pp.556–563.
6. V. Raghunathan. C. Schurgers, S. Park, and M. B. Srivastava , "Energy-Aware Wireless Micro sensor Networks", IEEE Signal Processing Magazine.19 (2002), pp.40-50.
7. S. Mini, Siba K. Udgata, and Samrat L. Sabat" Sensor Deployment and Scheduling for Target Coverage Problem in Wireless Sensor Networks", IEEE SENSORS JOURNAL,VOL.14, NO. 3, MARCH 2014.

MODIFIED ANT COLONY OPTIMIZATION USING A WEIGHTED HEURISTIC AND PHEROMONE MATRIX FOR IMAGE EDGE DETECTION

Dr. I. Selvamani[1]., G.Chandralekha Maheshwari[2]., G.Nithisha reddy[3]., A.Annapurna[4]., J.Gayatri[5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: i.selvamani@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0421, 17RG1A0420, 17RG1A0401, 17RG1A0431), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Image edge detection is a technique that allows you to segment an image into gaps, noting sudden changes in intensity. Ant colony optimization is a Meta heuristic approach based on the feeding behavior of ants. This article proposes a modified ACO algorithm for image edge detection by double updating the pheromone matrix and using a weighted heuristic. This method can be seen as an improvement on the original ant system. The approach presented in this article helps to deal with broken edges in an image and makes it more efficient than other traditional edge detection methods.

Keywords— edge detection, pheromone matrix, ant colony optimization, weighted heuristic, Otsu threshold.

1. INTRODUCTION

Image processing is an operation that takes an image as input and produces an output, which can be an image or a set of parameters associated with an image. One of the most common and difficult problems in image processing is edge detection. Edge represents the edge properties of objects in an image and appears as an abrupt change in intensity from one pixel to another in the image. Image edge detection is an important part of image analysis and processing. This is a preprocessing step in a series of feature extraction applications. So far, various methods have been proposed for capturing the contours of an image. Some of them are Sobel, Pruitt, Laplacian and Canny operators. Ant colony optimization is another approach based on the natural foraging behavior of ants. Traditional approaches to edge detection are computationally expensive because these operations are performed on every pixel in the image.

ACO is a probabilistic method that seeks to find an optimized solution to the boundary detection problem through guided search in the solution space by constructing a pheromone matrix. In the ACO algorithm, ants move through the search space, a graph of nodes and edges. The movement of ants is controlled by transition probabilities, which reflect the probability that an ant will move from one particular node to another. This value is influenced by heuristic and pheromone information.

The algorithm consists of three main steps. The first is the initialization process. The second is an iterative build and update process that aims to build the final pheromone matrix. The creation and update process is performed multiple times, once per iteration. The final step is a decision-making process in which margins are determined based on the final pheromone levels. This article made some changes to the existing ACO approach that resulted in better quality edges detected in the image, which is important for various object detection applications.

2. LITERATURE SURVEY

ACO is based on feeding ant communities. Ants, individually, are simple-minded living creatures. In the wild, a solitary ant cannot effectively communicate or search for food, but as a group it is smart enough to find and gather food for its colony. This collective intelligent behavior is the inspiration for this evolutionary technique (ACO algorithm). The introduction of ant strategies adds another dimension to the realm of computing. Ants communicate using a chemical called pheromone. During travel, the ant deposits a constant amount of pheromone, which can be

tracked by other ants [2]. In their search for food, ants tend to follow tracks with a higher concentration of pheromones. The pheromone deposited by the ants evaporates. The general procedure for the ACO algorithm.

The initialization step is performed at the very beginning. At this stage, the necessary initialization procedures are performed, for example B. set the parameters and assign the initial values of pheromones.

3. PROPOSED EDGE DETECTION BASED ON ACO ALGORITHM

In the proposed algorithm, two changes were made to the original ACO approach. The model used to describe the proposed work is an image in which each pixel represents both a node and an edge in the diagram. Ants move from one pixel to another based on heuristic information determined by local fluctuations in intensity. The components of transition matrices and pheromones are also associated with image pixels.

The first difference from the algorithm above is the method for determining heuristic information. Weights are used to compute a heuristic value. As the ant moves away, the weight decreases. This provides additional neighborhood information for calculating the transition probability. The initial matrix of pheromones in the proposed approach is set by the value 1 / (M 1 M 2), which allows ants to explore pixels other than edge pixels. Another change in the ACO algorithm is related to two updates to the pheromone matrix, rather than one update step in many other approaches in this area.

3.1 Initialization process

During the initialization process, each ant is assigned a random position on the M 1 × M 2 image . The initial value of each element in the pheromone array is set equal to the constant τ init, which is small but not zero. In addition, the matrix of heuristic information is built on the basis of local changes in the intensity values in accordance with equation 1. The heuristic information is determined during initialization, since it depends only on the pixel values in the image and is largely constant.

$$\eta\, i, j = V\, c\, (i, j) \,/\, V\, max \quad (1)$$

V c (i, j) is a function acting on a local group of pixels, as shown in FIG.

V max is the maximum change in intensity in the entire image, which is used as the normalization factor. V c (i, j) depends on the neighbors of the pixel (i, j).

3.2 Decision making process

This is a very important process as it takes into account the results of the previous steps to determine if each pixel has a border. First, an iterative method is used to compute the threshold T to obtain edge information. This threshold is used for the pheromone matrix. To convert an intensity image to a binary image, a normalized intensity value in the range [0, 1] is considered. Using the initial threshold, the histogram is divided into two parts. Calculates the average of the gray values associated with the foreground pixels and the sample average of the gray values associated with the background pixels. This new threshold is taken as the average of the two samples.

This process is repeated based on the new threshold until the specified value stops changing. The initial limit is the average value of the pheromone matrix. Each index value in the pheromone array is split so that it is less than the initial threshold value or greater than the threshold value.

Based on these two categories, an average is calculated, which is the new threshold. As mentioned above, this process is repeated until the threshold is constant.

The approach described here is known as the Otsu threshold technique [8]. The entire process of edge detection using the proposed technique is summarized in FIG.

```
Do initialization procedures
for each iteration n = 1:N do
  for each construction_step l = 1:L do
    for each ant k = 1:K do
      Select and go to next pixel
      Update pixel's pheromone (local)
    end
  end
  Update visited pixels' pheromones (global)
end
```

Figure 4: Image edge detection using modified ACO algorithm

4. EXPERIENCE AND RESULTS

Based on the methodology proposed in the article, experiments were carried out with some test images. The ACO algorithm was implemented in C and the program was run on a system with an Intel Core i5 and 4GB of RAM. Processing time for a 256 × 256 image is approximately 2.8 seconds.

The results obtained for the two test images are shown in the following figures. Other traditional edge detection approaches were applied to the same image to compare the results.

Fig 1: Test image 1

Fig 2: Test image 2

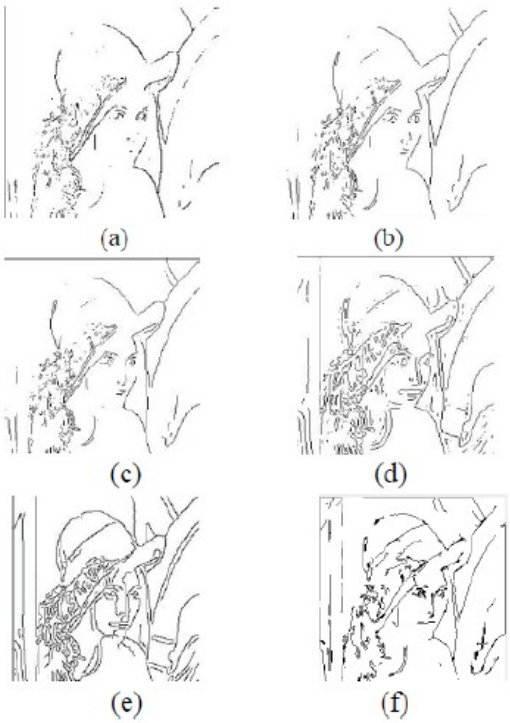


Fig 3: Edge Detection on Test image 1 (a) Roberts
(b) Sobel (c) Prewitt (d) Laplacian (e) Canny (f) Proposed ACO approach

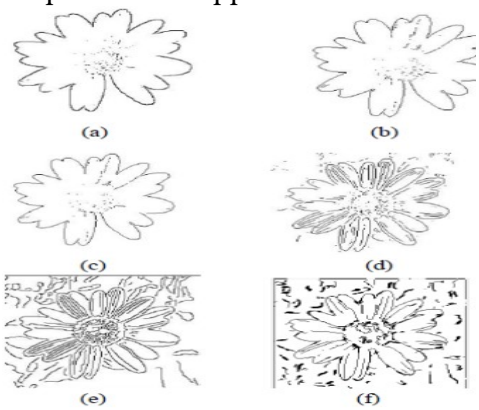


Fig 4: Edge Detection on Test Image 2 (a) Roberts
(b) Sobel (c) Prewitt (d) Laplacian (e) Canny (f) Proposed ACO approach

Edge Detection Technique	Results
Sobel operator	Edges are thicker, may or may not be discontinuous
Roberts operator	Prominent discontinuities, Thickest edges
Prewitt operator	Thin edges with discontinuities
Laplacian operator	Better than Sobel, Prewitt and Roberts. Malfunctioning occurs at corners and curves
Canny operator	Complex to implement but good for noisy images
Proposed ACO approach	Thin and clear edges, Simple to implement, Higher execution speed, Continuous edges

Table 1: Comparative Analysis of Edge Detection Techniques

5. CONCLUSION

This article presents an image edge detection method based on an improved and modified ant colony optimization method. Some changes to the original focus make edge detection more accurate as the processing speed increases. In addition, the modified algorithm handles bad edges without errors. According to experiments performed on test images using both the ACO algorithm and conventional edge detection operators, the results are summarized in Table 1. It can be clearly seen that the quality of the edges detected by the proposed ACO is superior. to other techniques.

REFERENCES

1. M. Dutta and P. Rai, " Image Edge Detection Using Modified Ant Colony Optimization Algorithm based on Weighted Heuristics ", International Journal of Computer Applications, Vol. 68 – No. 15, pp. 5 – 9, 2013.
2. C. Gupta and S. Gupta, " Edge Detection of an Image based on Ant Colony Optimization Technique ", International Journal of Science and Research, Vol. 2 – No. 6, pp. 114 – 120, 2013.
3. J. Li and P. Xiao, " An Improved Ant Colony Optimization Algorithm for Image Extracting ", International Conference on Apperceiving Computing and Intelligence Analysis, 2010.
4. C. C. Chen and D. S. Lu, " Edge Detection Improvement by Ant Colony Optimization ", Elsevier PatternRecognition Letters, Vol. 29 – No. 4, pp. 416 – 425, 2008.
5. M. Dorigo and T. Stutzle, " Ant Colony Optimization ", IEEE Computational Intelligence Magazine, Vol. 1, pp. 28 – 39, 2006.
6. H. N. Pour, E. Rashedi and S. Saryazdi, " Edge Detection using Ant Algorithms ", Soft Computing, Vol. 10, pp. 623 – 628, 2006
7. M. Batouche and S. Ouadfel, " Ant Colony System with Local Search for Markov random field image segemntation ", IEEE International Conference on Image Processing, pp. 133 – 136, 2003.
8. N. Otsu, " A Threshold Selection Method from Gray – Level Histograms ", IEEE Transactions on Systems, Man and Cybernetics, Vol. 9 – No. 1, pp. 62 – 66, 1979.
9. M. Nayak and P. Dash, " Edge Detection Improvement by Ant Colony Optimization Compared to traditional Methods on Brain MRI Image ", Communications on Applied Electronics, Vol. 5 – No. 8, pp. 19 – 23, 2016.
10. P. Thukaram and S. J. Saritha, "Image Edge Detection Using Improved Ant Colony Optimization Algorithm ", International Journal of Research in Computer and Communication Technology, Vol. 2 – No. 11, pp. 1256 – 1260, 2013.

DESIGN OF MTM SECURITY CHIP FOR MOBILE DEVICES USING HUMMINGBIRD ALGORITHM

B. Sneha Priya[1]., K.Naga ramya[2]., D.Manasa[3]., S.Swaroopa[4]., B.Ananya[5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: budhasnehapriya@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0404, 17RG1A0415, 17RG1A0453, 17RG1A0406), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The goal of this article is to protect mobile devices. Usually, hackers or other software easily break into mobile devices by updating the ROM. The main goals of the article are to protect mobile devices from software and to protect hardware devices from hackers. The hardware is called an MTM (Mobile Trust Module) chip. This chip is connected to a mobile device. Through I / O interfaces, UART and various I / O devices. The chip size should be as small as possible for mobile devices. It also offers additional features via software. It has its own software and is easy to use, so the user can protect their mobile devices from threats. In this article, we will implement hardware security devices that provide security through hardware and software.

Keywords— MTM Chip, Hummingbird Algorithm, Security Chip, IC Chip Card.

1. INTRODUCTION

Today, we all use electronic devices to store confidential data, but a hacker can easily hack it using software as well as using mobile phones. Theft of laptop computers is on the rise. To do this, we implement a chip protection system that protects devices from theft. In this article, we will implement hardware security devices that provide security through hardware and software. Checks if the user is using their own devices or if the device belongs to another user. Check the password entered by the user through the hardware security app. This password is verified by the equipment and confirmed by the user. If the password is correct, then and only then the user will be able to use their mobile devices, or, if the password is incorrect, the equipment will indicate that the password is incorrect, turn off the phone and say that the user will not correct. The microcircuit is the minimum possible and can be integrated into mobile devices or other electronic devices.

2. LITERATURE SERVEY

Recently, we have seen a meteoric rise in mobile devices, almost everyone has to bring their devices as their own [1]. Obviously, the benefits of BOYD are that employees feel more comfortable and satisfied with their devices, and employers save money by not having to pay for expensive devices and data plans. BOYD companies aim to increase flexibility. The convenience and portability of the devices will satisfy your employees' workflow, increasing their productivity. For example B. Spam messages, fake caller ID and MMS sender ID. After that, the study will take care of the security of mobile devices [2], since a mobile phone can only be protected by various communication components via GPS, GSM and network layer, but BOYD cannot be secure, and data can be stored in the cloud, and only observations from clouds. Data corruption and execution is in progress, but data can be corrupted offline even if a trusted module is to be started [3]. In mobile computing, data can be protected by hardware devices, and the security of the algorithm used to encrypt the data is 3DES, AES and SHA-1 for the speed of security operations for these 10 Mbps and 1154 Mbps AES required. The machine cycle is 1616 for 128 bits as well as 128 keys. AES and SHA-1 use a separate code for encryption and decryption. It was developed exclusively on a hardware basis; this type of interface lacks a software interface [3]. Technological advances in computers, communications and networking are transforming traditional desktop computing into mobile devices. It is expected that by 2018 there will be more than 2 billion smartphone users worldwide. The growing dependence on these devices inevitably means an increase in the amount of sensitive data stored on this platform. Unfortunately, the portability of mobile devices also makes them vulnerable to theft [4]. As more and more features are added

to mobile phones, mobile phone security is a growing concern among mobile phone players (malicious code is transmitted to mobile devices). Security concerns are exacerbated as these advanced features stimulate and increase the potential for security attacks [5]. The problem is compounded by the fact that initially, when designing wireless devices, security was not a priority. DRM (data privacy and digital rights management) agents have strict security requirements. Therefore, the first step in ensuring the resilience of wearable devices and smartphones to various types of attacks is to provide a general security architecture, design taking into account security requirements and reliable software layers [6].

3. PROPSED SYSTEM OF DESIGN CHIP MTM

3.1 MTM Chip Material

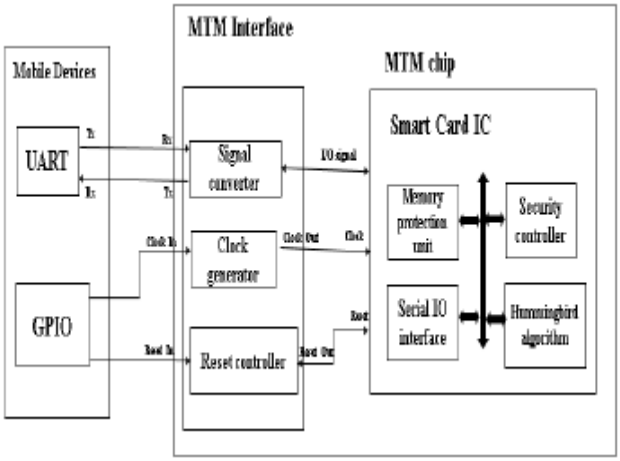


Fig. 1: Hardware architecture of the proposed MTM chip

The MTM chip [7] consists of an interface and a smart card IC. The integrated smart card circuit consists of a memory protection block to protect the memory from external threads that may occur with external software. The stored password can be protected by this memory protection unit. The security check can be used to provide security with the Hummingbird algorithm. The Hummingbird algorithm uses the same code for encryption and decryption [8]. Serial I / O interfaces are used for serial communication between mobile devices and the MTM chip for correct communication. Communication between the UART, the universal asynchronous transceiver and the I / O signal can be done via half-duplex communication. It is transferred from the UART code to the individual converter, through which it is then transferred to the IC of the smart card. The GPIO output is sent from the general purpose input when the clock is triggered to the clock at 1250 baud on the smart card IC. The same GPIO sends signals to the reset controller to reset the circuits if the data or code is wrong. When the IC is not in use, the clock is internally disabled to minimize power consumption.

3.2 Proposed MTM Chip Software

Three blocks are considered in software architecture: the first is mobile devices, the second is the functional block of the microcircuit, and the third is the command processing block. At startup, the password matches the configurable private keys transmitted by mobile devices, which are the first block through the UART I / O interfaces to the working block of the chip. The operating unit of a microcircuit consists of a cryptographic coprocessor and I / O interfaces. The cryptographic coprocessor encodes all data and is transmitted to the operating system of the microcircuit.

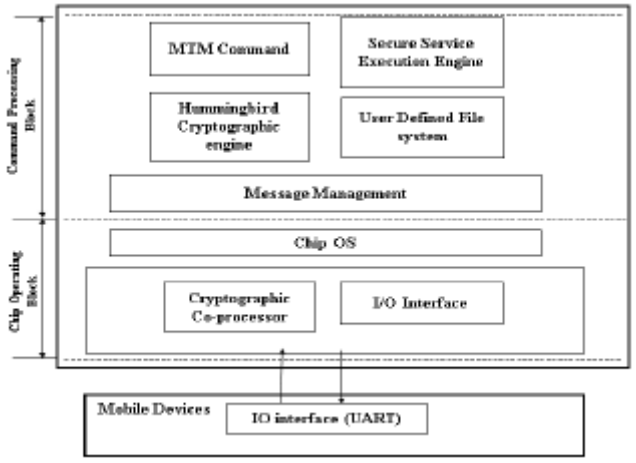


Fig. 2: Software architecture of the proposed MTM chip

If the data from the Secure Service Runtime Engine does not match, the e-mail control sends a message to the chip operating system that the password does not match, and therefore cancels the execution. If the

password does not match a second time, execution returns a second time. Thus, mobile devices are disabled and we can no longer perform any processes and the device is safe.

4. IMPLEMENTATION WORK AND RESULTS

So far in this article, we are writing the Kolibri cryptocode into the Xilinx Spartan 3. To verify the codes, we interact with the mobile phone with the Spartan 3 via a Bluetooth device.

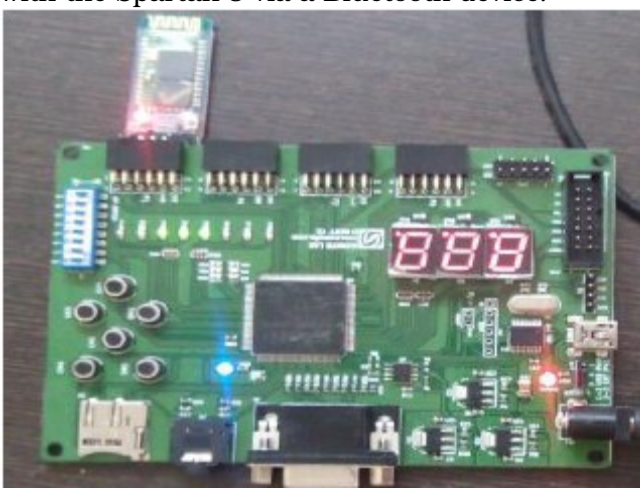


Fig. 3: Screenshot of hardware implementation

The Spartan 3 kit has a data transfer rate of 622 Mbps or more per I / O. It also offers a cost-effective, high-performance logic solution for mainstream consumer-facing applications. Use USB to write logic codes on the kit. When the LED is flashing, the kit and Bluetooth device are ready to use. We verify this code with BT Simple Terminal software. When Bluetooth and the Bluetooth device of the cell phone are paired. Then the operation begins. We give the user a password with a private key with 4 different digits like A, B, C, D. When we enter these 4 different codes, signals from bluetooth devices to Spartan 3kit will be transmitted according to the Kolibri cryptographic process, den Sent codes are verified and the output is sent to the mobile phone via Bluetooth. If the code is correct, "Y" will be displayed, and if the code is incorrect, "N".

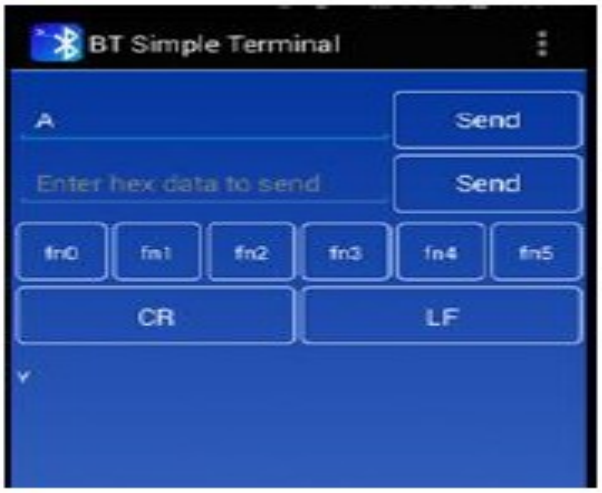


Fig. 4(A): Entered password for screenshot 'A'

Fig. 4(B): Password entered for Screenshot 1.

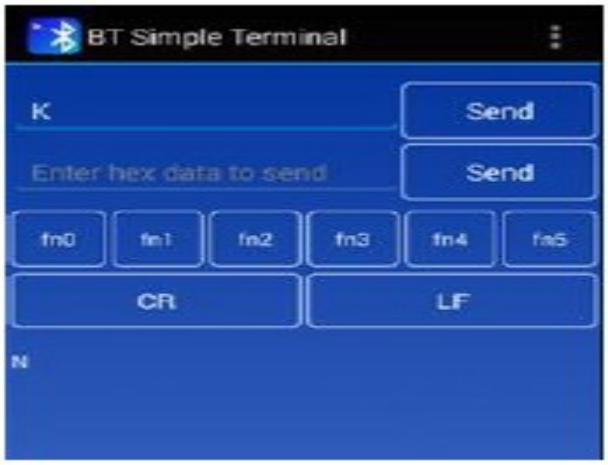


Fig- 4(C): password was entered for screenshot 'K'

Figure (B), (C) If we enter an incorrect password, the letter "N" indicates that the password is incorrect and is verified by a cryptographic algorithm.

5. CONCLUSION

Thus, this document provides security for various portable and portable devices. The Hummingbird algorithm is efficient for encrypting and decrypting user private keys.

REFERENCES

1. Ashkenazi, D. Akselrod "Platform Independent Overall Security Architecture In Multi-processor System-on-chip Integrated Circuits For Use In Mobile Phones and Handheld Devices," ELSEVER, Science Direct, Computer and Electrical Engineering, vol.33, pp.407-424, 23 July 2007
2. M. Rabbani, R. Ramprakash, M. tech Students, "Design of Hummingbird Algorithm for Advanced Crypto Systems," IJEDR, vol.2, Issue 1, ISSN 2321-9939, 2014
3. Hongil Ju, Youngsae Kim, Yongsung Jeon, and Jeongnyeo Kim, "Implementation of a Hardware Security Chip for Mobile Devices," IEEE Consumer Electronics, vol. 61, no.4, pp305-700, 4 Nov 2015
4. Y. Wang, J. Wei, and K. Vangury, "Bring Your Own Device Security Issues and Challenges," in Proc. The 11th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, pp. 80-85, Jan. 2014.
5. M. L. Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," IEEE Communications surveys & tutorials, vol. 15, no. 1, pp. 446-471, Mar. 2013.
6. M. Kim, H. Ju, Y. Kim, J. Park, and Y. Park, "Design and implementation of mobile trusted module for trusted mobile computing, "IEEE Trans. Consumer Electron., vol. 56, no. 1, pp. 134-140, Feb. 2010.
7. Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, Ke Chen "A Survey on touch dynamics authentication in mobile devices," ELSEVIER Science Direct, computer & security, vol.59, pp.210-235, 18 Mar.2016.
8. Carlin Covey, Mark Redman, Thomas Tkacik "An Advanced Trusted Platform for Mobile Phone Devices," ELSEVIER, Science Direct, Information Security Technical Report, vol. 10, pp.96-104, 2005

RASPBERRY PI BASED AFFORDABLE AND RELIABLE TEMPERATURE LOGGING SYSTEM

R. Srinivas[1]., K.Richa[2]., CH.Sai priya[3]., S.Swaroopa[4]., B.Ananya[5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: srinivasr.@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0437, 17RG1A0410, 17RG1A0435, 17RG1A0436), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— All laboratories need a temperature measurement and monitoring system. Instead of logging each reading with an analog device, it is better to use on-site digital data logging. Temperature data are read from the sensor and saved in an Excel file. In our laboratory, this setup offers a very good alternative to existing analog thermometers. The Raspberry Pi temperature sensor kit offers an affordable and reliable temperature measurement solution.

Keywords— Raspberry Pi, temperature logger, low cost temperature measurement system, Linux, Python, Ubuntu.

1. INTRODUCTION

Temperature measurement is the result of the development of thermometers. The thermometer output is usually indicated by calibrated reading marks. The problem arises at the laboratory level. If in an experiment we need to measure temperature over a long period of time, the recording complexity increases. The temperature must be recorded continuously and the system must also be monitored during this period. Therefore, it was decided to build a temperature recorder as an alternative to existing configurations. The aim of this study is to create a universal and inexpensive temperature recorder with constant power. In this article, we explain how to create a temperature logger with a Raspberry Pi. Raspberry Pi models can perform general computing and are therefore the most preferred candidates for introducing students to general computing and computer programming [1]. Ping, L et al. , [2] explained the temperature test system developed by DS18B20. Shinde, PA et al. , [3] discussed the implementation of the DS18B20 in a vehicle monitoring system using a Raspberry Pi. The Raspberry Pi can be used as an embedded system for any measuring lens [4, 5]. For this project we used a Raspberry Pi 2 Model B [6] and a DS18B20. We use the Python programming language for coding.

2. REQUIRED COMPONENTS

1. We will implement our experimental setup with the following components
2. Raspberry Pi 2 Model B.
3. DS18B20
4. network cable
5. Cutting board for bread
6. connection cable

3. EXPERIMENTAL SETUP

The temperature measurement setup is created with the Raspberry pi. We started the Raspberry Pi with Noobs [7], which contains the Raspbian Jessie with the Pixel operating system [8].

The micro USB connector is DC powered. The monitor is powered by an external power supply. We can now access the entire system through this graphical user interface. We prefer to work in the terminal. With the help of the terminal itself, we can control the entire system, even if we have superuser rights. Superuser access is provided with the "sudo" comment [9]. With the comment "sudo raspi-config" activate ssh [10] and the I2C console.

These changes took effect after a system reboot. Update is required after reboot. We are using the Aptitude package manager. This is the front end of the Advanced Packaging Tool (APT) [11]. The apt-get update, as well as the comments on the apt-get update, were done using sudo.

3.1 Connecting the DS18B20 temperature sensor

The DS18B20 digital thermometer provides temperature measurement from 9 to 12 bit Celsius and has an alarm function with user programmable non-volatile high and low setpoints. The DS18B20 communicates over a single-wire bus, which by definition requires

only one data line (and ground) to communicate with a central microprocessor. In addition, the DS18B20 can be powered directly over the data line ("interference current"), so no external power supply is required [2, 12]. It measures temperatures from -55 ° C to + 125 ° C. With an accuracy of ± 0.5 ° C from -10 ° C to + 85 ° C. The DS18B20 temperature sensor connects to the Raspberry pi-connected system.

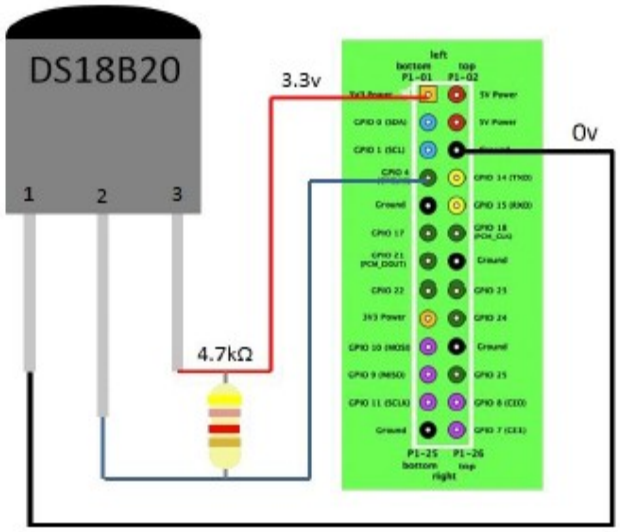


Figure 1: DS18B20 temperature sensor connected to Raspberry Pi

Figure 1 explains the instrumental structure of the temperature recorder. On DS18B20, pin 1 is connected to Rpi ground. Pin 2 is connected to GPIO 4, and pin 3 is connected to 3.3 V. We inserted a 4.7 kΩ resistor between pins 2 and 3 of the DS18B20.

3.2 Python software code

The code is required to connect the DS18B20 device to the Raspberry Pi, receive data, and display the results. To do this, we will implement Python code. Python is a simple and powerful language. Python is a popular object-oriented language that is used for both stand-alone programs and multi-field scripting applications. In this project we are using Python 2.7 [13].

We import libraries of time, globe and operating system.

```
import os
import glob
Import time
os.system('modprobe w1-gpio')
os.system('modprobe w1-therm')
base_dir = '/sys/bus/w1/devices/'
device_folder = glob.glob(base_dir + '28*')[0]
device_file = device_folder + '/w1_slave'
def read_temp_raw():
f = open(device_file, 'r')
lines = f.readlines()
f.close()
return lines
def read_temp():
lines = read_temp_raw()
while lines[0].strip()[-3:] != 'YES':
time.sleep(0.2)
lines = read_temp_raw()
equals_pos = lines[1].find('t=')
if equals_pos != -1:
temp_string = lines[1][equals_pos+2:]
temp_c = float(temp_string) / 1000.0
temp_f = temp_c * 9.0 / 5.0 + 32.0
return temp_c, temp_f
while True:
print(read_temp())
time.sleep(1)
```

3.3 Integrated system

To set up a temperature sensor, we need to integrate the hardware and software code into the Raspberry Pi. After starting up the Raspberry Pi, the Python code runs. This process can be done through the terminal or through the graphical user interface. When the Python code was run in the Python console, the temperature measurement data was saved in a separate Excel file. The measured output is retrieved for the subsequent calculation process.

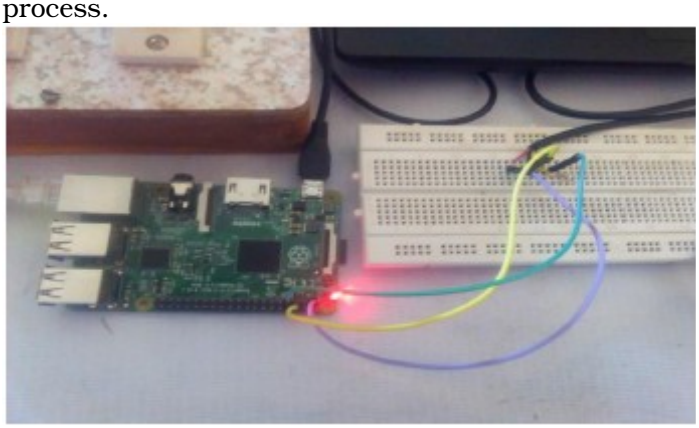


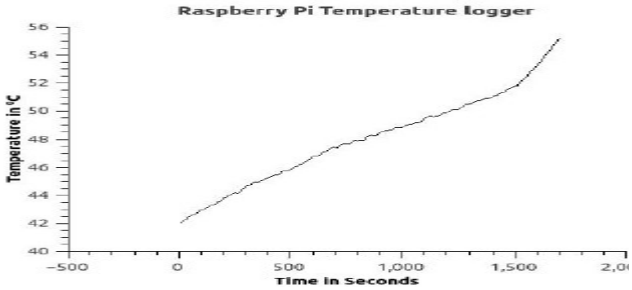
Figure 2 Raspberry Pi Connected to DS18B20

4. RESULTS AND DISCUSSION

We designed a temperature logger with DS18B20 and Raspberry Pi. Running a Python script saved the output to a specific file.

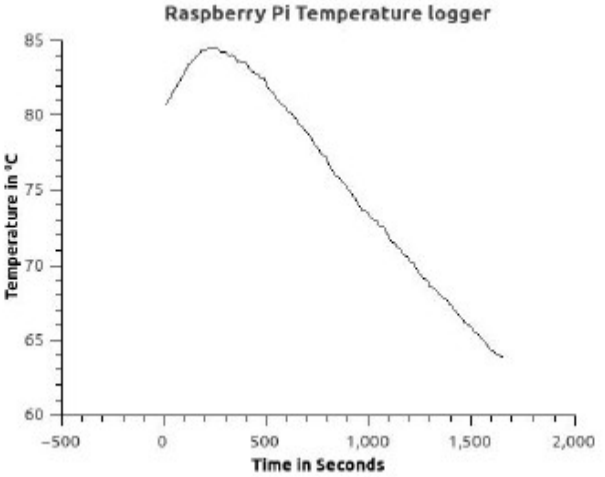
Temperatures were measured for different areas.

For the first set of experiments, we analyzed the water temperature for 1700 seconds, or about 29 minutes. Initially, the shaker was set to increase the temperature gradually. After 1500 seconds, the shaker was set to further increase the range. The output is written and the graph is written.



Graph -1: Raspberry Pi Temperature Logger - Increase Mode

In graph I, we can analyze the temperature rise data. After 1500 seconds, the temperature rises rapidly, indicating that the sudden temperature rise caused by the stirrer is affecting the linearity of the data. The small peaks in this diagram explain that temperature fluctuations are very small due to the open environment. The temperature rise rate is 0.0071850 ° C per second.



Graph -2: Decreasing mode of the temperature recorder

In this series of experiments, we configured our system to record water temperature data for 290 seconds (~ 5 minutes) in incremental mode. The recorded output is displayed graphically. This graph shows the temperature rise at the beach. There are several small peaks in this graph which indicate that the measured data is not significantly affected by the environment. If the measuring range is small, small deviations will also affect the output.

From the graph, we calculated that the rate of temperature rise is 0.02700 ° C per second.

5. CONCLUSION

Analyzing these different results, we conclude that the temperature recorder created with the Raspberry pi is working correctly. The consistency of the output is also maintained. From the above results, you can see that the environment plays an important role in the linearity of the output. These fluctuations are caused by heat loss to the environment. These effects can be minimized by an isolated system. Measurement data in the highest clock range is also a factor in the linearity of the output. From the graphs, we conclude that the upper time domains produce linear output. The temperature recorder was built with a Raspberry Pi and the results are discussed here. The Raspberry Pi temperature logger can be used as an inexpensive temperature measurement device. When the output is extracted into an Excel file, the data can be used for manipulation processes.

REFERENCES

1. Shinde, P. A., & Mane, Y. B. (2015, January). Advanced vehicle monitoring and tracking system based on Raspberry Pi. In Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on (pp. 1-6). IEEE.
2. Molloy, D. (2016). Exploring Raspberry Pi: Interfacing to the Real World with Embedded Linux. John Wiley & Sons.
3. Ping, L., Yucai, Z., Zeng, X., & Ting-fang, Y. (2007, May). A design of the temperature test system based on grouping DS18B20. In Industrial Electronics and Applications, 2007. ICIEA 2007. 2nd IEEE Conference on (pp. 188-191). IEEE.
4. Upton, E., & Halfacree, G. (2014). Raspberry Pi user guide. John Wiley & Sons.

5. Membrey, P., & Hows, D. (2015). Learn Raspberry Pi 2 with Linux and Windows 10. Apress.
6. Pi, R. (2015). Raspberry pi 2 model b. Online]. Tillgänglig: https://www. raspberrypi. org/products/raspberry-p3-model-b/[Använd 10 02 2016].
7. Negus, C. (2010). Linux Bible 2010 Edition: Boot Up to Ubuntu, Fedora, KNOPPIX, Debian, openSUSE, and 13 Other Distributions (Vol. 682). John Wiley & Sons. Chapter 8
8. Ylonen, T., & Lonvick, C. (2006). The secure shell (SSH) protocol architecture.

REVERSIBLE IMAGE WATERMARKING FOR PROTECTING ONLINE DATA VULNERABILITY AND COPYRIGHT INFRINGEMENT BASED ON HISTOGRAM SHIFTING TECHNIQUE

CH.Rajkumar[1]., K.Naga ramya[2]., T.Rohitha[3]., K.Dhana lakshmi[4]., M.Pravalika[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: chunchurajkumar@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0433, 17RG1A0458, 17RG1A0434, 17RG1A0441), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Digital watermarks are a form of data masking technology. It is a method of embedding information (i.e. watermarks) in multimedia data (images, audio or video) so that subsequently the embedded watermark can be extracted from the watermarked data for content protection or authentication. Among the various types of digital watermark designs, a reversible watermark has recently become a research hotspot. Over the past decade, several reversible watermarking schemes have been proposed to protect images containing confidential content, such as medical or military images, that, if modified, could affect their interpretation. These methods allow the user to restore the original image exactly from the watermarked version by removing the watermark. The difference between a watermark image and a cover image is the distortion caused by the masking process. Note that while the recovery phase ensures that the original main image is completely restored, it is desirable that the distortion caused by data masking be kept as low as possible. However, if the reversibility property weakens the invisibility restrictions, it can also interrupt data protection. In fact, after removing the watermark, the image is not protected. While it is possible to remove the watermark, you need to make sure that it is invisible, as most applications are very interested in keeping the watermark on the image for as long as possible.

Keywords— reversible watermark, histogram change.

1. INTRODUCTION

In recent years, the dramatic increase in the use of digital content has created issues such as online data vulnerability and copyright infringement. One of the most important solutions is the digital content watermark. However, watermarks can damage confidential information that is present in the cover order, and therefore it may not be possible to accurately restore the cover order on the receiving side. A reversible watermark, also known as a lossless watermark, allows you to fully extract embedded information as well as completely restore coverage. Therefore, a double-sided tattoo can be considered as a special case of a tattoo.

In the last decade, reversible watermark has undergone a great wave of experimentation in its field, as there is a great need to restore the original image after extraction of the watermark, which is found in various applications such as law enforcement, medicine and the military industry. visualization systems. It is important to restore the original image without distortion. Encoding an identification code in a digitized music, video, picture, or other file is called a digital watermark.

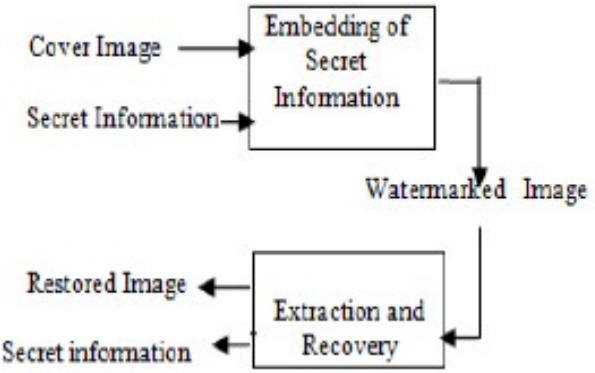


Figure 1: Basic watermarking scheme for reversible images

A general frame depicting a reversible watermark is shown in Figure 1. The sender embeds sensitive information into the cover image so that the recipient can retrieve the embedded message as well as obtain the cover image.

2. SCOPE AND RELATED RESEARCH

The reversible watermark has undergone a great wave of experimentation in its field over the past decade, as it becomes necessary to restore the original working image after removing watermarks in various applications such as police, medical and military imaging systems. It is very important to restore the original image without distortion. The reversible watermark can be divided into three categories: reversible watermark based on lossless compression, reversible watermark

based on differential expansion, and reversible watermark based on histogram shift. Lossless data compression reversible watermarking schemes utilize image coding redundancy. They compress the image data so that it takes up less space and uses the remaining space to embed the watermark data. These schemes usually require a high level of computational complexity, and their capabilities are relatively small.

The histogram shift method was first used by Ni et al. [four]. This chart uses the zero and maximum points (or minimum points if the zero point is not available) from the image histogram and changes the values between these points. While this method was effective, some additional information had to be conveyed to the recipient separately from the watermark image. This method is very simple, but inefficient.

3. DESCRIPTION OF THE SYSTEM

Various methods have been developed over the years, each with its own merits and demerits. It can be seen that the image watermarking techniques developed so far still pose a distortion problem to some extent. To reduce the distortion of the watermark image from the original grayscale image, it is proposed to develop a histogram shift method for a reversible watermark.

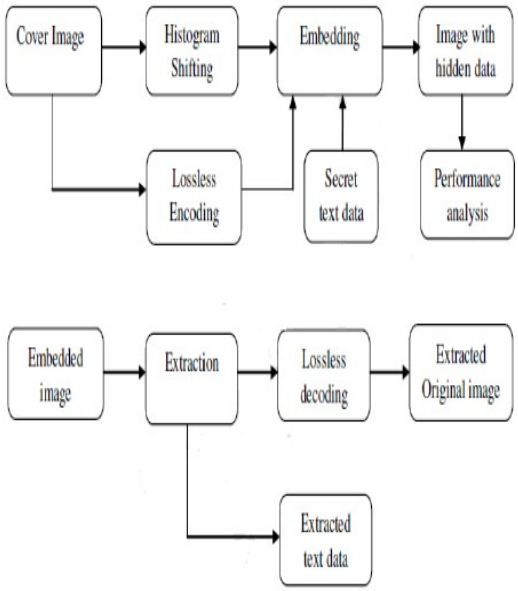


Fig. 2: Functional diagram of a watermark with a reversible image

A block diagram of a reversible image watermark is shown in FIG. In the process of reversibly modifying the watermark histogram, the sender embeds the watermark into the original image using a lossless input technique so that we get a watermark image. After receiving the suspicious image / watermark, the watermark removal scheme retrieves it. After extracting the message from the watermarked image, an exact copy of the original image is obtained. Note that we are more interested in minimizing distortion during manipulation, although the distortion caused by masking is completely reversible. With existing algorithms for shifting the histogram interval, the distortion of the watermark image of the original image depends on the number of pixels between the maximum and zero points of the image. Here, the maximum point acts as a "key point", that is, the pixel value used to embed the watermark. Therefore, it should be possible to reduce distortion by reducing the number of pixels between the cue point and zero point by choosing an appropriate cue point. In our proposed scheme, we find the zero point of the resulting histogram. We then select the pixel value as the key point (not necessarily the maximum point) so that its frequency is greater than or equal to the size of the watermark (that is, the number of bits in the watermark that will be integrated), and in addition, the number of pixels must be between at least the selected pixel value and zero point. If the given image does not contain a zero point, the gray level value corresponding to the minimum number of pixels is selected as the zero point, as in the case of existing histogram interval plots.

4. RESULTS & DISCUSSIONS

In this lesson, you will discuss the results of a reversible image watermark based on the histogram shift technique using MATLAB. These results are used to design the system.

The following figures show an example of the input image and the resulting output image. As it was mainly aimed at reversible image watermarking by integrating histogram shift technique, extraction process and parameter

calculation. The results are used to design the system.

For example, we take a sample image as the source image when we start the program. Displays the main window, original image, histogram of the original image, histogram intervals, offset histogram, and offset display histogram one image at a time. A watermark is required for process integration. Integrate the watermark into the original image and display the watermark image. Calculates PSNR, MSE and BPP of the watermark image. Thereafter, the watermark is extracted from the watermark image and the original image is restored. It also displays the histogram of the originally reconstructed image and calculates the PSNR and MSE of that image. The last window is shown in Figure 3.

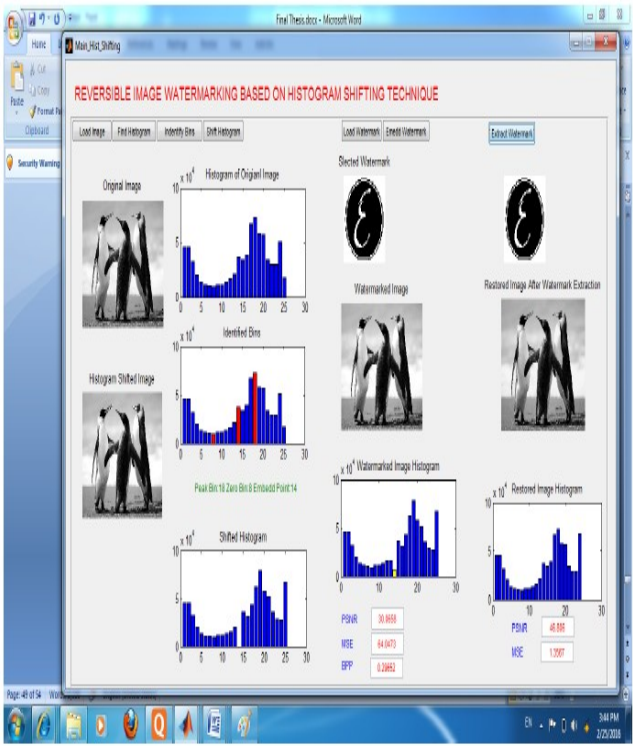
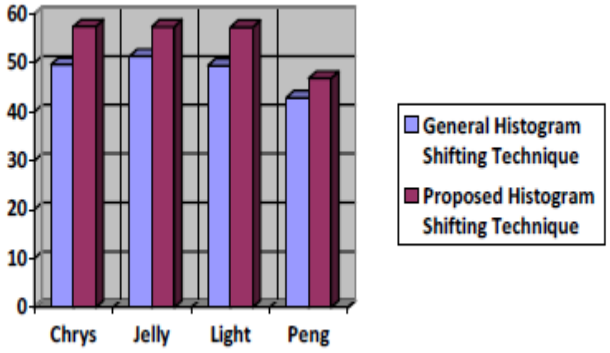


Fig. 3: Result window

After including the method and the result of the extraction method for various input images, Tables 1 and 2 are shown respectively. Two reversible watermark algorithms based on the histogram shift method compare the proposed histogram shift method with the previous histogram method. Experimental results from four standard test images show that the PSNR of the proposed scheme is improved. Figure 1 shows a graphical representation of the comparison.



Gig 4: Graphical representation of the comparison

5. CONCLUSION

Shifting the histogram area is a reversible tattoo technique known for its simplicity of calculations. Here I have suggested a method for switching the histogram tray to minimize the distortion of the cover image depending on the size of the embedded watermark. The proposed scheme is supplemented by the optimal choice of the integration point on the coverage frame rate histogram. This process greatly reduces the number of pixels that move when a watermark is embedded. These improvements significantly reduce the distortion of the cover image, as shown by our experimental results. This article describes the basic mechanism of a reversible watermark. While reviewing the main articles in this area, let's briefly discuss the development and benefits of various histogram offset reversible watermarking techniques. Methods based on changing histogram reduce the size of additional data and are semi-fragile or reliable.

REFERENCES

1. M. R. Rahimi, H Dyanali, M. Arabzadeh, " A Reversible Data Hiding Scheme Based on Maximum Histogram Gap of Image Blocks", 2011 1st International eConference on Computer and Knowledge Engineering (ICCKE), pp. 86-90,Oct. 2011.
2. Z. Ni, Y. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Transactions on Circuits and Systems

for Video Technology, vol. 16, no. 3, pp. 354–362, Mar. 2006.

3. C. D. Vleeschouwer, J.E. Delaigle, B. Macq, "Circular interpretation of histogram for reversible watermarking", IEEE Fourth Workshop on Multimedia Signal Processing, pp. 345–350, Oct. 2001.
4. G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens, C.Roux, "Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting", IEEE Transaction on Information and Security, Vol. 8, No. 1, pp. 111-120, Jan. 2013.
5. F. Bao, R. H. Deng,B.C.Ooi, andY. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. Inf. Technol. Biomed., vol. 9, no. 4, pp. 554–563, Dec. 2005.

MULTIPLE CONFIGURABLE FLR POWER RAILS TO MINIMIZE HEAT DISSIPATION AND SILICON AREA IN NANOPADS

K. Surekha[1]., G.Shivani[2]., T.Laxmi Priya[3]., S.Mounika[4]., CH.Manisha[5].,

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: surekhakorudu413@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0427, 17RG1A0457, 17RG1A0455, 17RG1A0411), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— To overcome the limitations in terms of power distribution, silicon surface area, quiescent current and minimum required efficiency, a multi-rail FLR is offered. This FLR uses two 1.8V and 3.3V rails with an overall 40% energy efficiency improvement when operating at low voltage (1.0V) compared to a 3-rail (3rd generation) V solution. The architecture is optimized for operation at low voltage (e.g. 1.0 V), with 80% of the current coming from the 1.8 V rail. The contribution of this lower voltage rail to the output current decreases significantly as the output voltage approaches 1.5 V, at this 3.3V rail provides most of the power. Note that there is no current limiting mechanism in the power supplies for this circuit. This article provides a complementary solution where one suggested rail can be selected to minimize heat dissipation and silicon area. The proposed solution uses a silicon region similar to that reserved for power transistors, with busbars reduced to handle only half of the solution's maximum current load. This architecture benefits from a configurable control loop, power supply, and ground offset. The principle is that if a lower output voltage is required on the NanoPad, the 1.8 V rail is triggered for a maximum theoretical efficiency of 55% to 83% (1.0 and 1.5 V output).

Keywords— FLR, configurable power rail, NanoPad, voltage regulator.

1. INTRODUCTION

The solution proposed in Figure 1 is a silicon zone similar to the one reserved for power transistors, in which the power is reduced to cope with only half the maximum polarization current capacity of the previous solution. The principle is that if a lower output voltage is required on the NanoPad, a theoretical performance of 55% to 83% is set for the 1.8 V rail (output voltages 1.0 and 1.5 V).

One of the problems with multiple busbar systems is the possibility of blocking. To avoid possible blocking, protective transistors (switches) have been added. With these transistors, only one bus can be switched on at a time. In particular, transistors M14 must turn off when VOUT is greater than the bypass voltage VDDn. M14 is disconnected using the VBASE voltage that is dedicated to M13 and M14 and which also powers the loop. A controller with an appropriate supply voltage to earth provides static polarization.

When the VDDn bus is running, the M13-M14 (VBASE) packages are installed on the VDDn. If they do not work, the blocks with the highest voltage Vdd1 are polarized.

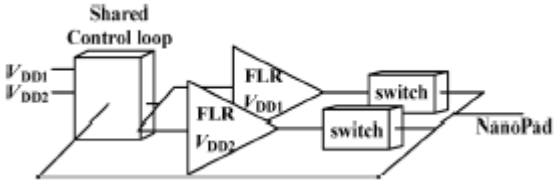


Fig. 1 FLR multi rail sharing a configurable common control loop

II. IMPLEMENTATION OF SYSTEM

This section describes the implementation of the voltage regulator circuit for the multi-rail power supply and the suggested inputs / outputs. Conforms to a two-wire busbar that can be expanded to a lane configuration with multiple energy sources. The proposed architecture integrates two separate fast charge controllers that operate with two power supplies (1, 8 and 3.3 V). It is possible to control one FLR at the same time using the same voltage feedback loop. Switches and massive dynamic bias have also been added to prevent jamming and provide good isolation from a non-working FLR. The current total budget can be divided by the number of installed electric rails. In our particular case, a possible total current of 110 mA is shared between 2 power rails that occupy the same silicon surface. This multi-rail power supply regulator uses a common reference voltage generated in each unit cell via a tunable bandgap in the main stage (Figure 1). This bandgap based on the voltage reference

nominally generates the same voltage across the silicon wafer to create a constant operating voltage at Vout as temperature increases or as slow oscillations (kHz) occur in power supplies.

A. Multi-rail voltage control loops

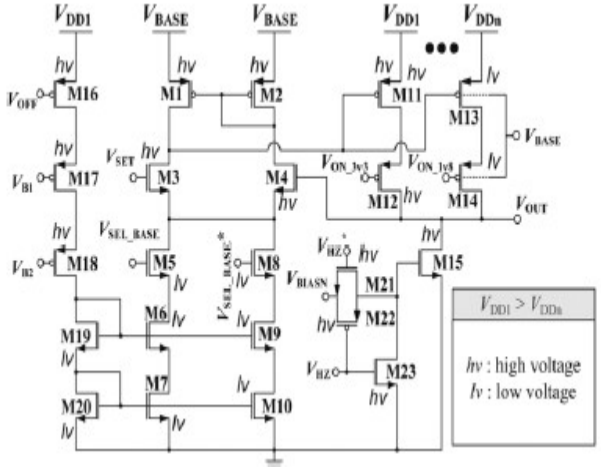


Fig. 2. Transistor level of multiple configurable FLR power rails

The controller can be configured to use either of the two implemented power rails, rated for 1.8 V and 3.3 V, to limit the power consumed in the digital system.

The proposed design uses a hierarchical topology to minimize quiescent current and silicon surface consumption by sharing as many common circuits as possible. Each unit cell uses a master-slave topology. With reference to Figure (3), the upper module uses the reference voltage (Vset) together with 16 NanoPads. The Fast Charge Controller (FLR) (Figure 1.3), built into every NanoPad, uses the VSET to set the output voltage between 1.0 V and 2.5 V. In addition, the VSET sets the digital I / O voltage levels. This method results in a reduction in silicon surface area by sharing a digital I / O fast charge regulator to provide a variable voltage (VSET) power supply, avoiding power stage duplication to power the E / S Digital s.

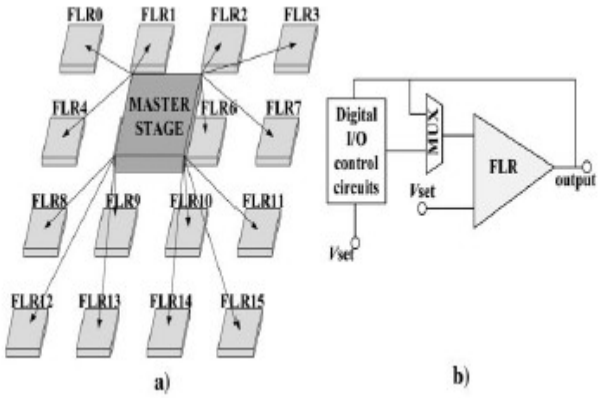


Fig. 3 (a) Proposed master-slave topology in which the scene master supplies 16 fast charge controllers (FLRs) with a common reference voltage. (b) Integrated digital I / O, where the feedback signal is controlled by a host computer or digital I / O control circuits.

However, a control circuit needs to be added to distribute this regulated power between the digital I / O and the load. This is done at the cost of I / O speed and FLR response time, as the gate adds significant parasitic capacitance.

3. SYSREM DISCRIPTION

We need to design a global distribution network operating on all-metal VDD and VSS. Secondly, we need to choose the right cables so that they can withstand the required currents. Third, we must ensure that the temporary behavior of the distribution network does not cause problems for the logic that drives it. With all of these issues in mind, we need to address two types of power outages:

• IR reduces steady-state currents;
• The transient current drops.

The H-tree is a very regular structure that allows for predictable latency. The balanced tree uses the opposite approach - the synthesis of the design based on the properties of the synchronized circuit. The processor has a large number of these local points and requires a large number of branches and therefore a deep distribution tree. Deep Spanning Tree has long POD latency and low clock performance. Dividing the array into fewer strips and using a grid to serve each area may be a better solution. Clock grid looks like a network with fully connected clock tracks in two dimensions and grid controllers on all four sides. Local loads in the region can

be connected directly to the grid. The network effectively prevents all pilots from working and helps to minimize latency mismatches.

A shorted gate assembly helps to equalize load imbalances and results in a more gradual delay profile in the region. In addition, because network drivers are bypassed, POD latency for all loads in the region is limited by the network link latency, which is usually small and results in lower clock drift uncertainty in the region. DSCH2 is a logic editor and simulator. DSCH2 is used to validate logic architecture before starting microelectronic design. DSCH2 provides an easy-to-use environment for designing hierarchical logic and fast modeling with lag analysis, allowing you to design and validate complex logic structures. Several low energy design techniques are described in the manual. DSCH also includes symbols, templates, and assembly support for 8051 and 18f64. DSCH also contains an interface for SPICE.

The MICROWIND2 program allows the student to design and simulate an integrated circuit at the physical description level. The package contains a library of common analog and logic ICs for display and simulation. MICROWIND2 contains all the commands of the skin editor, as well as original tools that have never been combined in one module before (2D and 3D process representation, VERILOG compiler, MOS device tutorial). You can access the circuit simulation with the click of a button. Electrical extraction of your circuit is done automatically and the analog simulator immediately generates voltage and current curves.

4. SIMULATION RESULTS

The schematic diagram was created using the DSCH2 software.

1. First, the components required for the schematic are placed by drawing them from the symbol palette, which is available in the DSCH software as a sidebar.
2. When you are done with the tour, save the .SCH file.
3. Go to the File menu and select Create Verilog File to generate a Verilog program for the circuit you have designed.
4. The diagram drawn with the DSCH software is shown in fig. 8.
5. The layout diagram is created using the MICROWIND program.
6. First go to the full menu and select the "Compile Verilog File" option.
7. A dialog box will open.

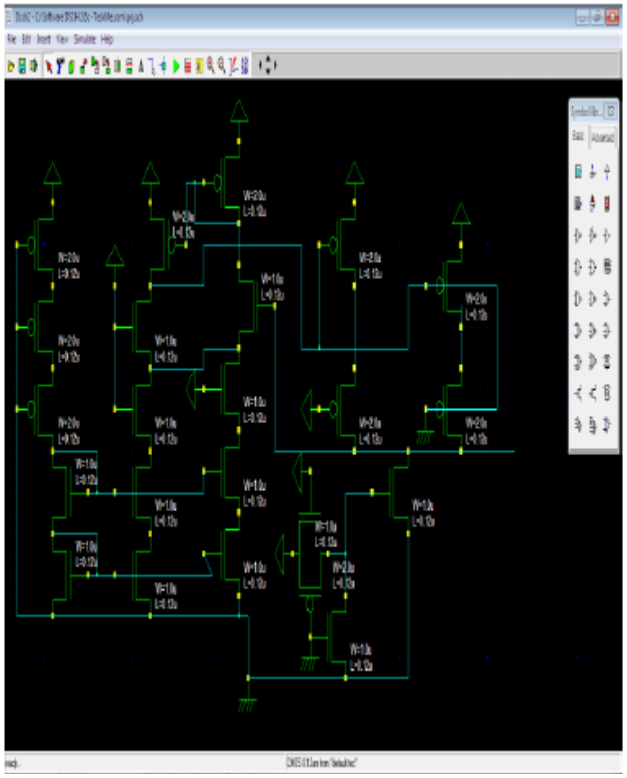


Fig 4 Schematic diagram

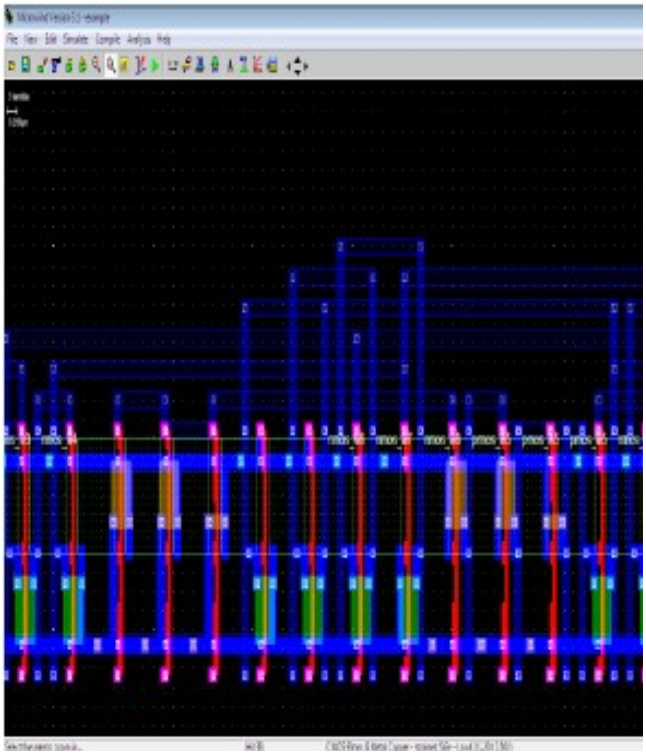


Fig. 5 Distribution scheme

5. CONCLUSION

Our laboratory has a platform for rapid prototyping of electronic systems - a waffle card. It is based on an active schema that can be configured at the system level. Electronic components that are firmly in contact with its surface are powered and connected to each other through circuits implemented on this active surface. This article will focus on ways to provide power that reduces heat generation by introducing a new multi-rail supply voltage regulator operating on 1.8 and 3.3 V rails. By adding a second supply rail, energy savings of up to 25% are achieved at increase in working area by reducing the total power available per tire due to limited space. The proposed design combines two regulators that quickly charge one using adjustable wattage, ground bias technology, and common transistors. The proposed architecture was built using 0.12µm CMOS technology and occupies a small area of 0.0075mm2 by combining two control loops into one, making it suitable for cut-scale integration. In addition, the proposed design provides a fast response time of 11 ns at 35 mA into line voltage or very low quiescent currents of 120 µA. This job also brings in the best profit, outperforming its closest competitors by three times.

REFERENCES

1. Andre.W, Valorge.O, Blaquiere.Y, Sawan.M, "Configurable Input–Output Power Pad for Wafer-Scale Microelectronic Systems," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.21, no.11, pp.2024,2033, Nov. 2013
2. Valorge.O, Andre.W, Savaria.Y, Blaquiere.Y, "Power supply analysis of a largearea integrated circuit," New Circuits and Systems Conference (NEWCAS), 2011 IEEE 9th International , vol., no., pp.398,401, 26-29 June 2011
3. 3.Hazucha.P, Karnik.T, Bloechel.B.A, Parsons.C, Finan.D, Borkar.S, "Area-efficientlinear regulator with ultra-fast load regulation," Solid-State Circuits, IEEE Journalof , vol.40, no.4, pp.933,940, April 2005
4. 4.Laflamme-Mayer.N, Blaquiere.Y, Savaria.Y, Sawan.M, "A Configurable Multi-Rail Power and I/O Pad Applied to Wafer-Scale Systems," Circuits and Systems I: Regular Papers, IEEE Transactions on , vol.61, no.11, pp.3135,3144, Nov. 2014
5. 5.A textbook on “Modern VLSI Design-IP Based Design” by Wayne Wolf - Prentice Hall Modern Semiconductor Design Series- Fourth Edition.
6. 6.Norman.R, Valorge.O, Blaquiere.Y, Lepercq.E, Basile-Bellavance.Y, El-Alaoui.Y, Prytula.R, Savaria.Y, "An active reconfigurable circuit board," Circuits and Systems and TAISA Conference, 2008. NEWCAS-TAISA 2008. 2008 Joint 6th International IEEE Northeast Workshop on, vol., no., pp.351,354, 22-25 June 2008.

ADAPTIVE CRUISE CONTROL IN AUTONOMOUS VEHICLES USING TCP/IP PROTOCOL IN RASPBERRY PI

Y. Kalavathi[1]., B.Akhila[2]., Christy mary bose[3]., M.Harshitha[4]., T.Sruthi[5]

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: vimireddy.kalavathi.@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0408, 17RG1A0413, 17RG1A0494, 17RG1A04A8), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— This article gives an idea to design an adaptive cruise control with sensors and two Raspberry Pi boards. The proposed system consists of two Raspberry Pi, one of which is the slave and the other is the master. The Raspberry Pi acts as a slave device and is responsible for detecting various parameters such as vehicle distance, rainy weather monitoring, road slope detection, damaged road detection, temperature monitoring, location, and speed detection. Both the Raspberry Pi and the slave are connected to the master over a TCP / IP link. Here the communication between the master and the slave is based on the TCP / IP protocol, i.e. H. The recognized values of the slave can be sent to the master via a TCP / IP channel using an Ethernet cable (RJ45). The sensor values must be predefined as the thresholds must be lower if these measured values are higher than the thresholds of the PWM pulses generated in the master. The PWM signal controls the speed of the DC motor. The values will be displayed later on the LCD screen..

Keywords— TCP / IP protocol, adaptive rate control, Raspberry pi.

1. INTRODUCTION

Reduce road accidents and develop systems such as adaptive cruise control. It consists of sensors to detect imminent accidents. When detection occurs, the system takes automatic control measures without driver intervention. nIn [1] CAN-based cruise control in road situations, the goal of the intelligent vehicle frame is to reduce the number of road accidents and increase the flow. The proposal contains two controls, one of which is to propel the vehicle and the other to control the speed of the vehicle. Here, the main processor is using ARM11 and the bottom controller is ARM Cortex M3. The slave device can send the collected data to the master using the CAN protocol as the communication medium. The sensor values are fixed, the threshold values must be lower. If these values are above the thresholds, the master generates signals that use these signals to control the motor speed. In [2] "Intelligent car driver assistance system". The proposed structure includes two ARM controllers, sensors and a CAN protocol. A separate ARM controller acts as a slave, which is responsible for registering sensor values. Another ARM controller acts as the master controller for the motor. Here is the CAN protocol by which the values are sent from the slave module to the master module [3]. In [4], "Adaptive cruise control", adaptive cruise control has a kind of cruise control system that can automatically control the speed of the vehicle to maintain the distance between vehicles and the speed range. “Approximately 20-25 miles per hour. An ACC-equipped vehicle is detected by the vehicle in front, any object is detected, and the system decelerates and maintains the distance set by the driver from the vehicle in front. off If the road is clear, the vehicle with the ACC system increases the speed set by the driver and fig. one.

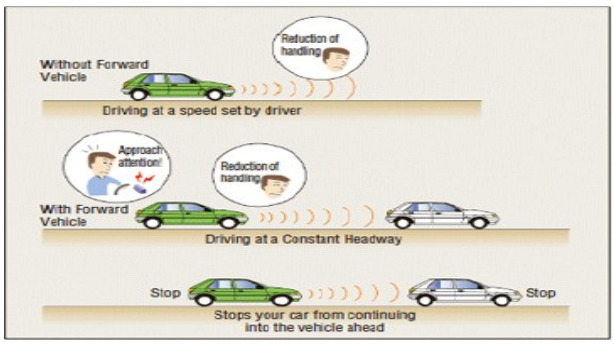


Fig 1: ACC working principle

Some things need to be noted in the ACC, namely:

Frame ACC may not work in certain natural conditions such as rain and fog. Even in environments such as dust or ice collectors. The ACC can draw on little power to avoid getting close to the vehicle in front. Use this innovation to focus more on your point of

movement, distance between vehicles and changes in flight path at altitude.

In [5] Heavy Traffic Collision Avoidance System, this article provides instructions on how to operate the ultrasonic sensor. Calculate the distance between car formulas as follows

D = 0.5 * C * (T1-T0) 1.1

Where D = distance to object

C = speed of sound

T0 = time during which the sound wave is transmitted

T1 = time to receive the sound wave

2. PROPOSED METHODOLOGY

This article is planning to create an adaptive cruise control using sensors and two Raspberry Pi boards. The proposed structure consists of two Raspberry Pi, one of which acts as a slave module and the other as a master. This slave module can be used to recognize various parameters, for example. For example, distance between vehicles using an ultrasonic sensor, monitoring rainy weather with a humidity sensor, detecting a road slope using an accelerometer, detecting a damaged road using a vibration sensor, monitoring temperature using a temperature sensor and determining a location using GPS, detecting rotational speed using a tachometer and the master is responsible for controlling the DC motor. Here, both slaves of the Raspberry pi are assigned to the master via TCP / IP. This TCP / IP protocol is used to exchange information between the packet module and the main module. The surge sensor values need to be adjusted as the thresholds need to be lower. If these measured values are above the threshold values, the master outputs PWM signals. Using the PWM signals, the master controls the speed of the DC motor, and finally the values are displayed on the LCD screen.

The proposed system consists of

a) Obstacle detection : ultrasonic sensor to detect obstacles in front of the vehicle. Four-pin sensors are trigger, echo, Vcc and ground. A trigger is an input that continuously transmits a signal in the event that an obstacle search signal is returned to the echo output. The slave collects information from the sensor to the master over TCP / IP. The master controls the DC motor using a PWM signal.

b) Monitoring of wet weather : checks humidity near the vehicle wheels with a sensor of humidity , and also indicates the weather conditions. When hot air is turned off, the tire containing more moisture can cause accidents with this sensor.

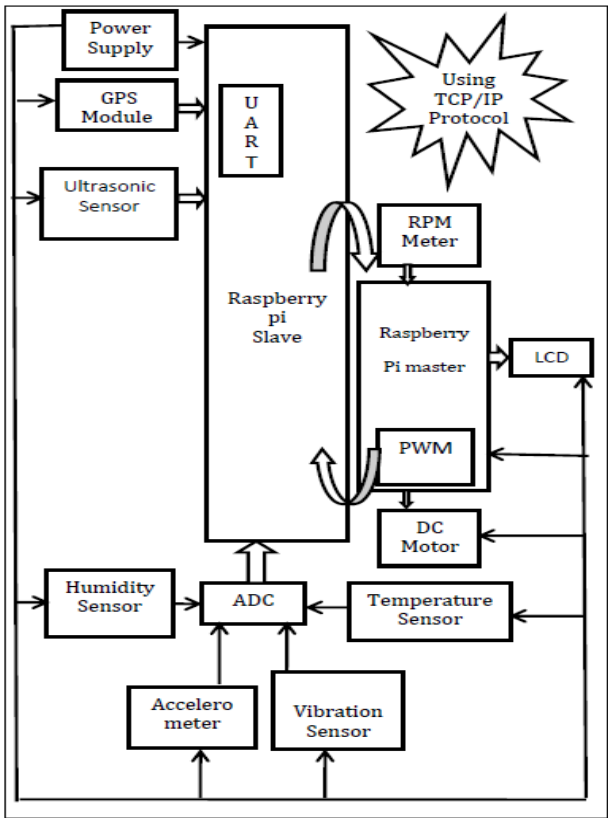


Fig. 2: Functional diagram of the proposed system.

c) Temperature control: temperature sensor to check the temperature near the vehicle wheel and similar monitoring in wet weather.

d) Slope detection in road detects potholes in the road, and recognizes the need for the road using an accelerometer. Also measure the vehicle's acceleration. A sensor with three outputs is analog and therefore must be converted to digital via an ADC. The converted data is then sent to the slave through the master using TCP / IP, and finally, the master controls the DC motor using PWM signals.

e) Damaged road detection: detects the damaged road using a vibration sensor. The

sensor works as a determination of the road slope.

f) Location search : With the Global Positioning System (GPS), the vehicle's location area is determined by longitude and latitude.

h) Speed determination: measures the pivot point of the vehicle wheel based on revolutions per minute (rpm).

3. SOFTWARE USED

Figure 3 consists of the following steps.

Step 1. Initialize all Raspberry Pi slave GPIO ports on specific sensors such as ultrasound, temperature, vibration, humidity, accelerometer, RMP, and GPS.

Step 2: Detect the values sent to the slave by each sensor

Step 3: In the Salve module, the recognized values are transmitted to the Raspberry Pi master over TCP / IP.

Step 4: the teacher makes a decision based on the thresholds

Step 5: If the detected values are between the threshold values, adjust the speed set by the driver.

Step 6: If the detected values are above or below the threshold values, set the speed according to the programmed designations.

Step 7: Finally, the values should be displayed on the LCD screen.

At this company, we use Raspbian on Linux. Raspbian is a free operating system that works in light of Debian's advances on Raspberry Pi devices.

Today Python is a plus in the use of programming languages in the world. Python has a base language in which syntax can be easily read and expressed. In addition, various languages such as Java, C, C ++ can be easily written, and large-scale and small-scale composition code can be provided. There are some features like memory management as well as problem support, multiple object-oriented programming, functional programming, and finally procedural structures. Python supports all operating systems on which a variety of code can run. IDLE is an advertising window for entering Python commands. The results are shown in Figure 4.

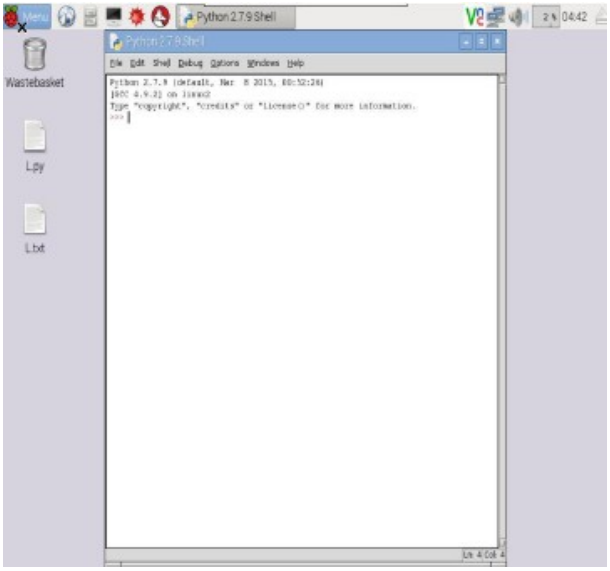


Figure 3 : Python IDLE Window

4. RESULTS OBTAINED

Figure 5 shows the interface of all sensors such as ultrasound, humidity, vibration, temperature, accelerometer and GPS module with raspberry ointment module.

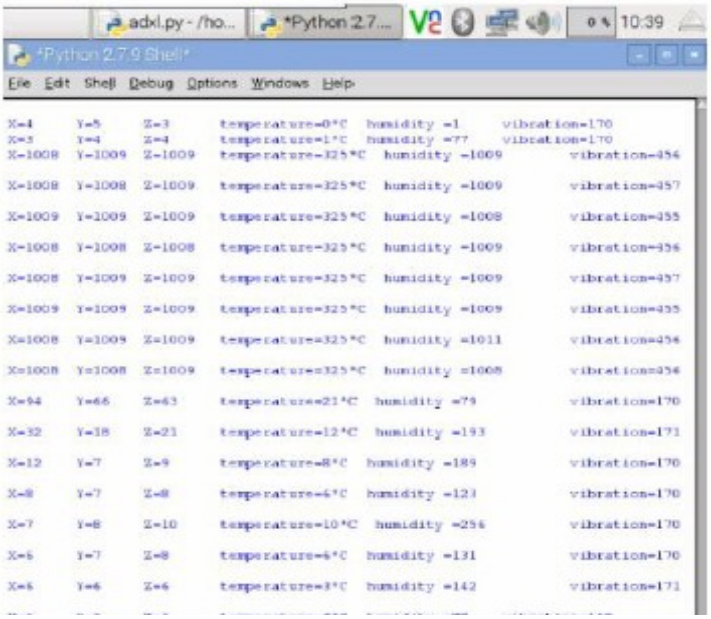


Fig. 4: Sensor values

Figure 4 shows all the sensor values after the interface. Sensors such as accelerometer, temperature, humidity and vibration in the Python IDLE window.

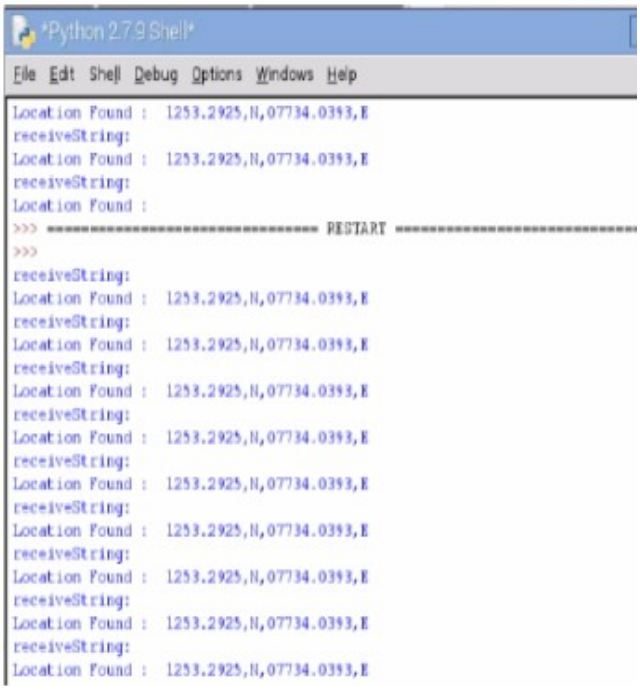


Fig. 5: GPS values

Figure 5 shows the GPS values in the Python IDLE window.

5. CONCLUSION

A driver's actions are influenced by various factors related to the vehicle, the environment and the pipeline route. Observing and sensing the driver's movements to ensure road safety is essential in the event of road accidents. Thus, it is important to do driving exercises that prevent mistakes on the road, as the driver pays a lot of attention to adjustments, laziness, drowsiness, alcohol, as well as bad weather conditions such as fog, wet road, certain turns. points.

The proposed device has been tested under various sensory conditions. The results were assessed as satisfactory. The Trip Information Index obtained from this review was analyzed in terms of the total driving and door open times for the ACC as measured by the number of times the engine was run at different speeds. In the coming days, the framework can be improved by adding additional futures, reducing the load on drivers and lowering usage costs.

REFERENCES

1. Ms. Divya K .S, Ms. K. A Drishya, Mr. Sakthiprasad .K .M , “Vehicle Speed Control System using CAN”, IJSTE - International Journal of Science Technology & Engineering | Volume 1 | Issue 10 | April 2015
2. Prof. D. S. Vidhya, Miss Delicia Perlin Rebelo, Miss Cecilia Jane D’Silva, Mr. Linford William Fernandes, “Adaptive Cruise Control”, IJIRST International Journal for Innovative Research in Science & Technology| Volume 3 | Issue 01 | June 2016
3. M. Divya and G. Bhaskar Phani Ram, “Controller Area Network Based Cruise Control in Traffic Situations”, International Journal of Current Engineering and Technology ©2015 INPRESSCO®, Vol.5, No.4 (Aug 2015)
4. Ashutosh U. Jadhav, N.M. Wagdarikar, “Intelligent vehicle system for driver assistance”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol.4, Issue 7, July 2015
5. Babu Varghese, Renju Thomas Jacob, Fajas Kamar and Rizwan Ali Saifudeen, “Collision Avoidance System in Heavy Traffic and Blind Spot Assist Using Ultrasonic Sensor”, international journal of computer science and Engineering communication-IJCSEC. Volume 2, Issue.1, February 2014

REVERSIBLE ARITHMETIC AND LOGICAL UNIT FOR IMPROVED COMPUTATIONAL ARCHITECTURE AND BETTER DESIGN OF MICROPROCESSORS

K. Manasa[1]., M.Pravalika[2]., D.Sravani[3]., R.Sandhya Rani[4]., T. S.Shirisha[5]

1Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: manasareddy.@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0441, 17RG1A0417, 17RG1A0450, 17RG1A0456), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Reversible logic is used to reduce power dissipation, which is a basic requirement in low-power digital circuits. It has wide applications in modern computing, low power CMOS design, optical information processing, DNA computing, bio-information, quantum computing, and nanotechnology. Reversible logic is gaining more and more importance as a logical design style for modern nanotechnology and quantum computers with minimal heat generation as existing irreversible designs reach their physical limits. Therefore, the use of reversible logic offers an improved computational architecture and better design of arithmetic logic devices. An important block of microprocessors is the arithmetic logic block (ALU). This article provides an overview of the reversible logic-arithmetic unit.. reversible logic gates, Reversible Arithmetic, ALU.

Keywords— reversible logic gates, Reversible Arithmetic, ALU.

1. INTRODUCTION

Reversible logic synthesis has been quite active in recent decades, mainly due to the reduction of magical power through reversible logic. According to Moore's Law, the number of transistors wills double every 18 months. Therefore, energy efficient devices are in the order of things. Heat dissipation can be minimized with production optimization techniques. Landauer's principle [10] shows that a circuit that is logically reversible is in principle also thermodynamically reversible, and investigated that for every loss of KT * log 2 Joule bit, heat is generated. Since this amount of heat is too low today, Zhirnov showed that it is very difficult to dissipate heat as the number of CMOS (Complement Metal Oxide Semiconductor) devices increases, leading to research in this area on an important topic.

A scheme in which data at the end is not lost is called reversible and therefore offers a solution to the problem discussed by Landauer. This could be a great achievement for the semiconductor world. Bennett [17] showed that heat removal from zero is possible only if the circuit consists only of reversing valves. The main application of reversible logic is quantum computing. A quantum computer is considered a quantum network (or a family of quantum networks) consisting of quantum logic gates, and any gate that performs an elementary unit operation on one, two or more quantum two-state systems are called qubits. Quantum networks must be built from components of reversible logic.

2. ASSESSMENT OF PROBLEMS AND PERFORMED WORK

Priyal Hemant Grover and Verma [1] represent the article "Design, Layout and Simulation 8-bit arithmetic and logic unit (2015)," International Journal of Electrical and Electronics Engineers. In this presented work, an 8-bit ALU is designed, implemented and modeled using electrical CAD and SPICE software. The proposed construction is an 8-bit ALU that can perform: AYB, A + B (addition), AOB and A - B (subtraction), as well as all kinds of arithmetic and logical operations. The physical design of each submodule is done using the 300nm C5 process technology. The workflow used here is the C5 process provided by MOSIS. This ALU has design flexibility and lower speed.

Shefali Mamtaj et al. [2] This paper "Optimized implementation ALU to the control unit for two-sided gate (2014)" in the Journal of Advanced Research in Comp. Software development and science. This article proposes a control unit consisting of double-sided gates. This control unit is more efficient than the

existing control unit. This article also shows an optimized implementation of the logic arithmetic unit using the proposed control unit and DKFG reversing gate. This ALU has a lower quantum cost, and the arithmetic loss and control unit are about the same as the traditional circuit.

Ajay Kumar Sharma Anshul Jain [3] represents article «Low Area field of low arithmetic and logic unit Design (2014)," International Journal of innovative research in computing and communications technologies. This

The article describes a design technique for low-power arithmetic logic devices with a small area. This item will reduce the number of gates and power. The design area is also reduced. Therefore, this ALU is of low power, small area, and complex complexity.

Chetan Kumar et al. [4] Submit the article “Toffoli's Implementation of a 16-Bit Computational Unit with a Reverse Gateway (2014)” in the International Journal of Science, Technology and Innovation Innovation (JISET). In this article, a conventional ALU is implemented using reversible AND or OR logic gates. Power dissipation in terms of data bit loss is greatly reduced if logic gates are replaced with reversing gates. The proposed 16-bit reversible ALU reduces performance loss through bit reuse. These circuits are modeled using Mentor graphics tools, and the programming language is Verilog's high-speed hardware IC hardware description language. This ALU consists of Toffoli gate only and found low power consumption during simulation.

Vijay Roi Et G., et al. [5] This article "Implementation of a low-power 8-bit ALU using quantum reversible logic structure (2014)," International Journal of Science and Research (IJSR). In this work, new programmable reverse logic gates are used in the design of a reverse arithmetic logic device. An 8-bit ALU was designed and tested using a 1-bit ALU. The proposed 8-bit ALU is also compared to the existing 8-bit ALU with reference to some important parameters such as latency and power dissipation. The main advantage of the proposed ALU is the increased number of operations with a series of selected low power inputs. This ALU can be used in low power VLSI, nanotechnology, quantum computing and optical computing. This ALU has more walking and less speed.

Avinash G. Keskar and Vishal R. Satpute [8] to submit an article in IEEE titled "Designing a new reversible arithmetic and logic unit Bit Novel (2011)». This article discusses various aspects of reversible computation and reversible logic gates. In addition, in this article, we tried to develop a reversible implementation of an 8-bit arithmetic logic unit that is optimal in terms of the number of gates used and the number of generated garbage outputs.

Using a multiplexer and control signals. ALU is one of the most important components of a processor, which can be part of a programmable reversible computing device like a quantum computer. In a multiplexer based ALU, operations are performed according to the selection string. The ALU based on the control unit was designed with 9n elementary reversible gates for four basic arithmetic logic operations on two n-bit operands. The sequence of operations is performed on the same line in accordance with the control signals instead of selecting the desired result through the multiplexer. The new design proved to be more profitable than the previous one in terms of the number of waste outlets and permanent inlets. This ALU has better efficiency and higher quantum cost.

3. PROPOSED METHODOLOGY

An irreversible arithmetic logic unit (ALU) consumes a significant amount of power due to the loss of bits during operation. Due to this bit loss, the heating problem becomes inevitable in many situations. To improve the performance of the irreversible logical arithmetic unit (ALU), we use the reversible logical arithmetic unit (ALU). Therefore, in this research paper, we investigate several reversible logic gates for designing a reversible arithmetic logic unit (ALU).

4. CONCLUSION AND FUTURE PROSPECTS

New designs of reversible arithmetic and logic units (ALUs) benefit from irreversible arithmetic and logic units (ALUs) and contribute to low power dissipation as well as use a smaller area, which is desirable for implementing a reversible center unit. The research results can be very effectively used in quantum computers and low-power designs. Future areas of this research include the applicability of Moore's Law in the coming decades to quantum computers using reversible logic. This reversible arithmetic logic unit (ALU) can be used in applications such as quantum computing, nanotechnology, optical computing, low power VLSI, etc.

REFERENCES

1. Chetan Kumar, Dr. Rekha.K .R and Dr. Natraj K .R, "Implementation of 16 bit Arithmetic and Logical Unit using Toffoli Reversible Logic Gate" International Journal of Innovative Science, Engineering and Technology (IJISET), Vol. 01, Issue 06, August 2014.
2. Vijay G.Roy, P.R.Indurkar and D.M.Khatri, "Low Power 8 bit Quantum ALU Implementation using Reversible Logic Structure", International Journal of Science and Research (IJSR), Vol. 03, Issue 07, july 2014.
3. Akanksha Dixit and Vinod Kapse, "Arithmetic and Logical Unit Design using Reversible Control Unit",International Journal of Engineering and Innovative Technology (IJEIT), Vol. 01, Issue 06, June 2012.
4. Priyal Grover and Hemant Verma, "Design, Layout and Simulation of 8 bit Arithmetic and Logical Unit" International Journal of Electrical and Electronics Engineers (IEEE),Vol. 07, Issue 02, July- December 2015.
5. Shefali Mamtaj, Biswajit Das, Anurima Rahama "An Optimized Realization of ALU for 12 Operation by using a Control Unit of Reversible Gates", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 04, Issue 01, January 2014.
6. Ajay Kumar Sharma and Anshul Jain, "Design of Low Power Low Area Arithmetic and Logical Unit" International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 02, Issue 12, December 2014.
7. Zhijin Guan, Wenjuan Li, Weiping Ding, Yueqin Hang and Lihui Ni, "An Arithmetic and Logical Unit Design based on Reversible Logic Gates", International Journal of Electrical and Electronics Engineers (IEEE), 2011.
8. Avinash G. Keskar and Vishal R. Satpute, "Design of 8 bit Novel Reversible Arithmetic and Logical Unit" International Journal of Electrical and Electronics Engineers (IEEE),2011.
9. Y.Syamala and A. V. N. Tilak, "Reversible Arithmetic and Logical Unit" International Journal of Electrical and Electronics Engineers (IEEE), 2011.
10. R.Landauer, "Irreversibility and Heat Generation in the Computational Process", IBM Journal of Research and Development, Vol. 05, 1961.

MINIATURIZATION OF RECTANGULAR SLOT MICROSTRIP PATCH ANTENNA FOR GSM BAND

Dr. Ashwani kumar yadav[1]., M.Tejasree[2]., M.Srilakshmi[3]., G.Aruna[4]., M.Kavya [5]

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: ashwani kumar.@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0443, 17RG1A0442, 17RG1A0428, 17RG1A0423), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

***Abstract*— As an important design prospect, the demand for reducing the size of low frequency antennas is the main development of communication technology with integration technology. For this kind of purpose is the design of it, with the reduction of rectangular microstrip - patch antenna to focus. At the structure is a micro-band - the patch antenna with a resonant frequency of 3.11 GHz without the use of slots used. With the use of slots works the design of a microstrip antenna with a resonant frequency of 0.932 GHz. In this article is a frequency shift of 3.11 GHz to 0.932 GHz observed. The 89% miniaturization is the main contribution of this paper, which very encouraging..**

***Keywords*— Rectangular Microstrip Patch antenna (RMPA), Return Loss (RL), Miniaturization, Defected Ground structure (DGS).**

1. INTRODUCTION

With the advantage of low cost, low profile, low weight, simple production, small size and integration of flat and non-planar surfaces, and VLSI design is the application of microstrip antennas for wireless applications for commercial use of communication takes to. The idea of the patch micro-antenna was followed in 1953. In recent years, small antennas using low frequency antennas have aroused great interest among researchers [1]. The antenna size decrease, are many techniques or Miniaturization process is used, such as for example the use of a slot on a patch, a defective basic structure (DGS), dielectric substrate with a high frequency. RMPA usually has a conductive patch which is made of PEC (see Figure 1) and on a printed base substrate is [2] [3]. For miniaturization are rectangular microstrips - antenna slots used. The present work is concerned with themselves with the design and analysis of a rectangular microstrip antenna for GSM communications and - applications. At first, is the antenna for a resonant frequency of 3.11 GHz designed, and while using slots is the resonant frequency of 0.932 GHz reduced. So, is a size reduction of 89% achieved.

2. DESIGN, FORMULATION AND SIMULATION PROCEDURE

A. Desired parametric analysis [4] :

a) Calculation of the width (W)

$$W = \frac{1}{2fr\sqrt{\mu\varepsilon}}\sqrt{\frac{2}{\varepsilon r + 1}} = \frac{c}{2fr}\sqrt{\frac{2}{\varepsilon r + 1}}$$

b) Effective dielectric constant is calculated from:

$$\varepsilon eff = \frac{\varepsilon r + 1}{2} + \frac{\varepsilon r - 1}{2}\left(\frac{1}{\sqrt{1 + \frac{12h}{w}}}\right)$$

c) Calculation of Length Extension

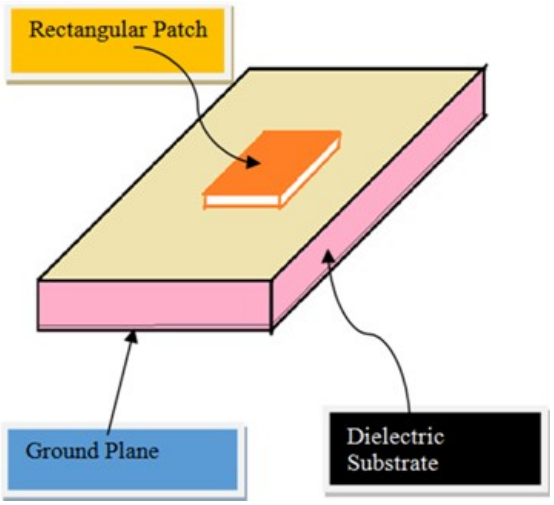


Figure 1: A basic rectangular microstrip patch antenna

$$\frac{\Delta L}{h} = 0.412\frac{(\varepsilon eff + 0.3)\left(\frac{w}{h} + 0.264\right)}{(\varepsilon eff - 0.258)\left(\frac{w}{h} + 0.8\right)}$$

Where,

c = free space velocity of light,

= Dielectric constant of substrate

h = height of dielectric substrate
= Effective length
= Resonating frequency
L= Length of patch
W= Width of patch
= Effective dielectric constant

3. PROPOSED ANTENNA SPECIFICATION

Computer Simulation Technology (CST-MSW) 2010 software is the software to design and simulate the desired antenna. CST MSW assists in the fast and accurate analysis of high frequency devices such as antennas, couplers and filters. Apart from this, MSW CST is one of the special tools for 3D simulation of high frequency devices or antennas. CST Microwave Studio is the ultimate software for design simulation, since this software for 1D, 2D and 3D platforms to simulate a full wave simulation is desirable and other specifications. [4]

- Length of ground= 30mm
- Width of ground= 30mm
- Length of dielectric substrate= 30mm
- Width of dielectric substrate= 30mm
- Length of rectangular patch= 22.779mm
- Width of rectangular patch= 29.53
- Dielectric constant of substrate= 4.3
- Height of dielectric substrate= 1.6mm
- Free space velocity of light= 2.99*
- Resonating frequency= 3.118GHz

4. RESULT ANALYSIS

A microstrip patch antenna without slits and with slits can be found in items 2 and 3 shown. As in Figure 2 below, the discrete point is assumed to be (-5, -5).

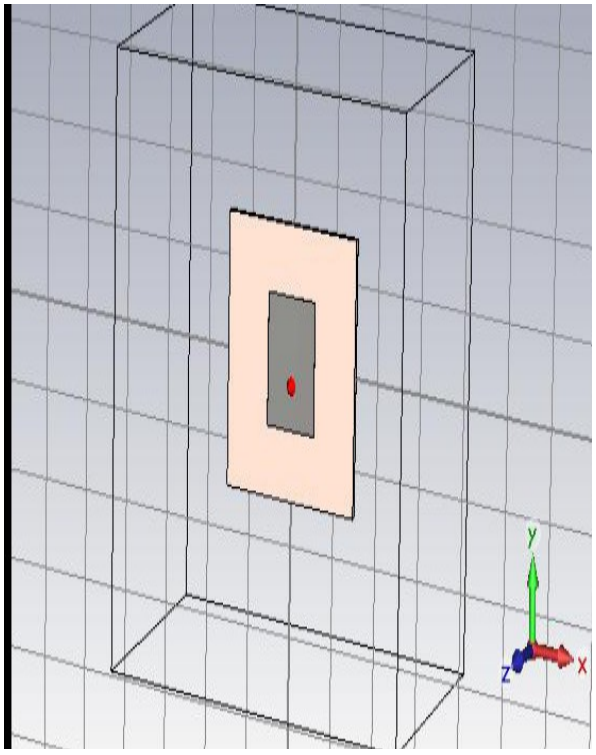


Figure 2: A rectangular microstrip - patch antenna without slots

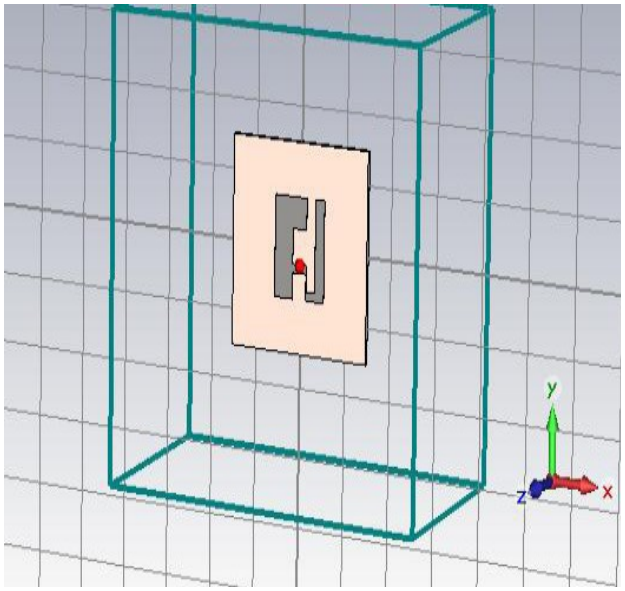


Figure 3: A rectangular microstrip patch antenna with slits

The return loss of the slotted and slotted rectangular microstrip patch antenna is shown in Figure 4 and Figure 5.

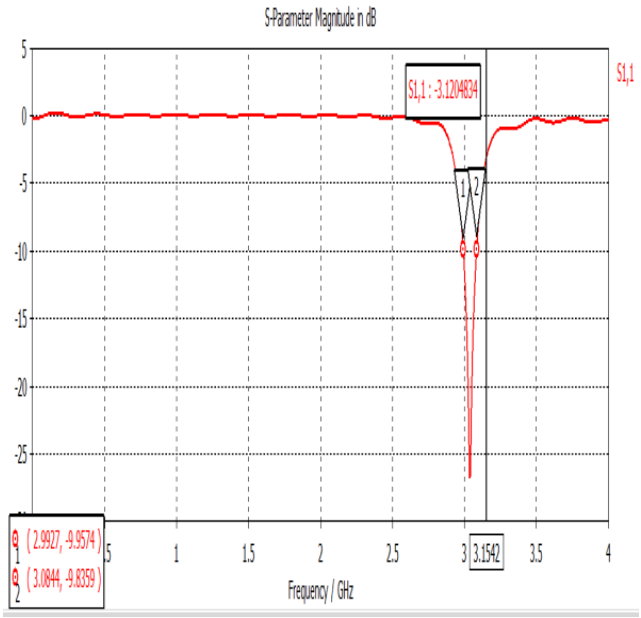


Figure 4: Return loss without slits

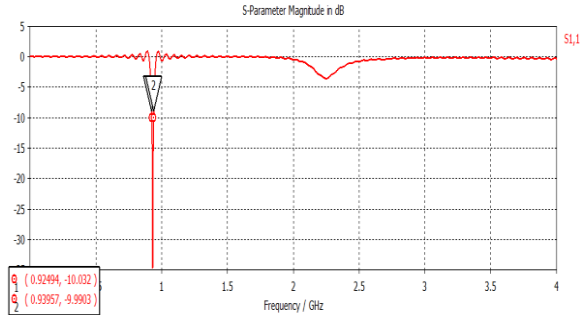


Figure 5: Return loss with slits

With the help of three slots is carried out, the size reduction from 3.11 GHz to 0.932 GHz of frequency, which for GSM modules and applications used is. There is a T-shaped slit on the product patch , slit 1. The length of the upper T-shaped slit is 6mm, and the width of the T-shaped slit is 7.5mm. Slot 1 and slot 2 are the combination of the T-shaped slot (see Figure 5.3.2). The length of the lower T-shaped slot is 3.89mm , and the width is 27mm. The final slot 3 is directly under the T-shaped slot 9.8 mm long and 9.5 mm wide prepared for the end result and the final frequency of 0.932 GHz to achieve that of the applications GSM used is the measurement of the length and width.

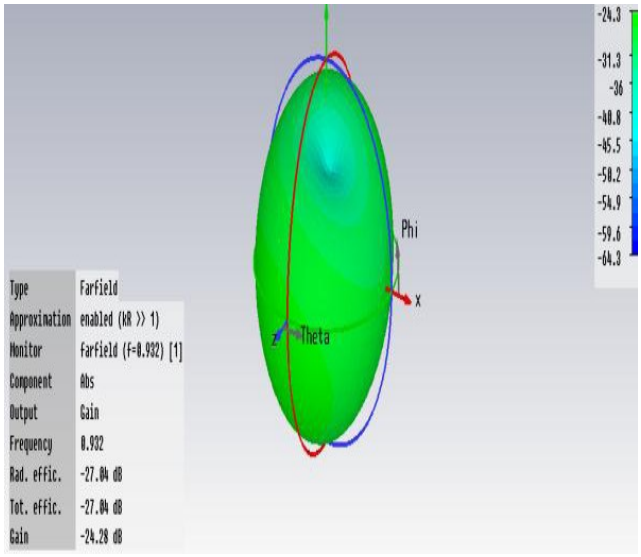


Figure 6: Gain at 0.932 GHz

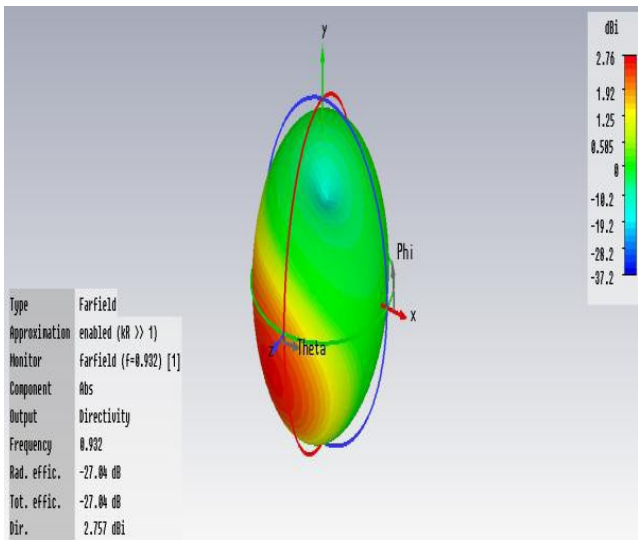


Figure 7: Directivity at 0.932 GHz

The gain of a 0.932 GHz rectangular microstrip patch antenna is shown in Figure 7. The directivity of a rectangular microstrip - patch antenna at 0.932 GHz is in Figure 8 shown.

5. CONCLUSION

As above already explained, at the end of the paper, a size reduction in rectangular microstrip - patch antennas. With the help of slits is in this work the design of a rectangular microstrip antenna - Patch carried out. Finally, a small and efficient microstrip antenna - rectangular patch with an operating frequency of 0.932 GHz. A size reduction of about 89% and a resonant frequency shift from 3.11 GHz to 0.932 GHz with a return loss

of -34.71 dB fascinates the antenna for GSM wireless applications.

REFERENCES

1. H.D. Chen, "compact circularly polarized microstrip antenna with slotted ground plate ", electron let 34, 2002, pp.616-617.
2. K.L. wong and T.W. chiou, "Design of compact microstrip antennas with slotted ground plane", In:proceeding of the IEEE antenna and propagation society international symposium, Vol.2, Boston, MA, 2001, pp.732-735.
3. A.K. Skivernilk, J.R. Mosig and Zurcher O. staub, "PCS Antenna Design: The challenges of Miniatururization", IEEE Antenna Propagation Magazine, 43(4), pp. 12-27, August 2011M, 1989.
4. Ping Jack Soh, Guy A. E Vandenbosch, Soo Liam Ooi, "Design of a Broadband All-Textile Slotted PIFA by CST", IEEE Transactions on Antennas and Propagation, Vol.60, Issue: 1, January 2012, pp. 379-384.

DESIGN OF ASYNCHRONOUS PARALLEL SELF-TIMED ADDER USING MICROWIND

N Uma Maheshwari[1]., A.Ashritha., C.Sai Poojitha[3]., G.Deepthi Goud[4] ., G.Sahithi[5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: umaece05@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0402, 17RG1A0409, 17RG1A0418, 17RG1A0426), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Adders are the basic building blocks of various VLSI circuits such as microprocessors, ALUs, etc. The performance of the adder circuit has a large impact on the overall capacity of the system. In this article, we introduce the design and performance of the parallel synchronized automatic adder. It is based on a recursive formulation for performing multibit binary sums. The operation is in parallel for the bits that do not require transport chain propagation. A convenient implementation is provided with a termination detection unit. The implementation is regular and has no practically high distribution limits. The proposed work was mainly aimed at minimizing the number of transistors and at estimating various parameters, namely the area, power and delay for PASTA. We also designed 4-bit PASTA as an example of the proposed approach. The simulations were carried out with the software MICROWIND 3.1 and the DSCH tool in 45 nm CMOS technology in order to check the practicability and superiority of the proposed approach compared to existing asynchronous adders.

Keywords— Binary adders, Parallel, Adders, Asynchronous circuits, CMOS design.

1. INTRODUCTION

The sum is the most common and widely used arithmetic operation in microprocessors, digital signal processors, especially digital computers. In addition, it serves as a building block for the synthesis of all other arithmetic operations. Therefore, the performance of a circuit is mainly determined by the speed of the adder circuit. Circuits can be classified as synchronous or asynchronous. Synchronous circuits are based on clock pulses, while an asynchronous circuit or a self-timed circuit is not controlled by a clock or a global clock circuit, but often uses signals that indicate the completion of operations. The basic component of combinational digital adders is a single bit adder. The simplest single bit adder is a half adder (HA). Full adders (FAs) are single bit adders with carry input and output. Full adders essentially consist of two half adders in terms of area, connection and time complexity.

2. RELATED WORKS

1] Jens Sparso and S. Furber, 2001 [1] introduced us to the basics of asynchronous circuit design against the background of the synchronous design of digital circuits. In addition, his work provides the basis for clarifying the need for asynchronous circuits as well as their performance parameters and their implementation.

2] Ashivani Dubey and Jagdish Nagar, 2013 [2] This article suggests the comparison between the series adder and the parallel adder. The author compared the serial adder and the parallel adder to determine the parameters of operating speed and power consumption. The series adder consumes little power, but is slow compared to the parallel adder. Parallel adder uses more power than serial adder, but because parallel adder adds all the bits at the same time, they give a quick response.

3] N. Weste and D. Harris, 2005 [3] This book discusses the basic theory behind CMOS VLSI designs. This includes a brief overview of CMOS logic, CMOS processing technology, circuit characterization and performance estimation, combinational and sequential circuit design, circuit simulation and various test tools and their verification.

3. PROPOSED SYSTEM

3.1 PASTA DESIGN

The architecture and theory behind PASTA are presented in this section. The selection input for two input multiplexers corresponds to the handshake signal Req and is a single transition from 0 to 1, which is indicated by SEL.

3.2 IMPLEMENTATION OF THE PASTA

In this section, PASTA is implemented using CMOS technology. The general block diagram of the parallel synchronized automatic adder contains the following circuit modules: -

- Half adder
- Multiplexers
- Completion detection circuit

A) Half adder using logic gates

For the addition side, the EX-OR gate, which uses the NOT, AND and OR gates, requires 22 transistors. For the carry side, the carry output is obtained by applying an AND to both inputs A and B. This means that we need 6T, a total of 28T, to implement a half adder using CMOS transistors.

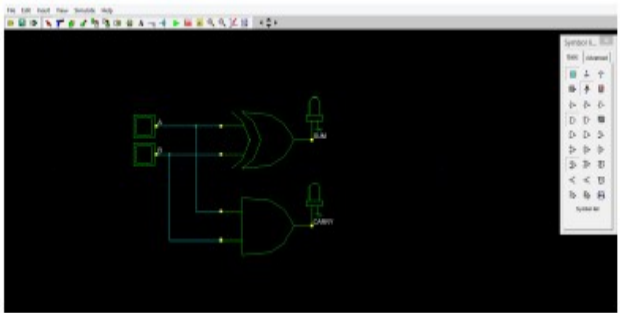


Fig. 1: - Basic logic diagram of the half adder

B) Half adder using NAND gates

The basic NAND gate requires 4T for its MOS transistor implementation. that is, two pMOS transistors in a pull-down network and two nMOS transistors in a pull-down network. Therefore, if we implement a half adder with only NAND gates, we need 20T for the tracking circuit.

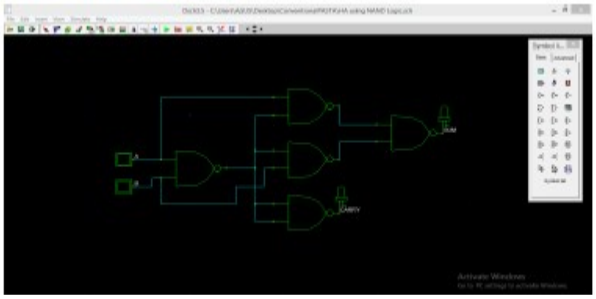


Fig. 2: - Half adder with NAND gates

C) Half adder as suggested in document [11]

Therefore, the half adder proposed in Article [11] uses 16T (10T for the sum module and 6T for the carry module).

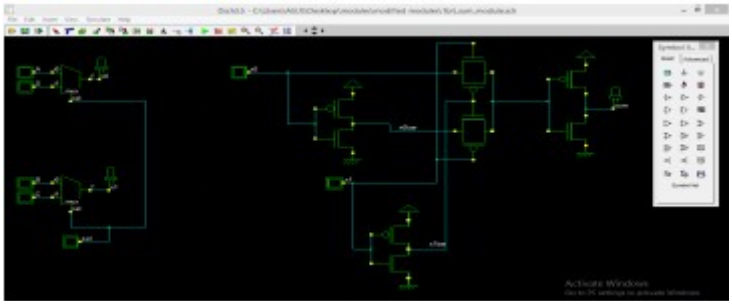


Figure 3: -1-bit add module

D) Proposed design of the half adder

Figure 7 explains the EX-OR scheme proposed with 6 transistors. This diagram uses a new concept of X-OR gate design using a transmit gate with two inverting circuits. This optimized EX-OR using the pMOS and nMOS transistor is used for the SUM side in a half adder and on the carry side with the new Y gate is replaced by NAND & NOT gate. Therefore, the proposed circuit only needs 12T for its implementation using CMOS technology.

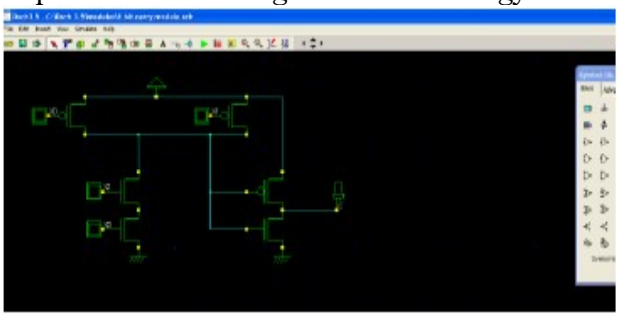


Fig. 4: - Arrangement of the proposed half adder

3.2.2 Multiplexer

The multiplexer or MUX is a digital switch also known as a data selector. It is a combination circuit with more than one input line, one output line and more than one select line. In PASTE 2: 1, MUX is used. Figure 9 shows the general scheme of 2: 1 MUX.

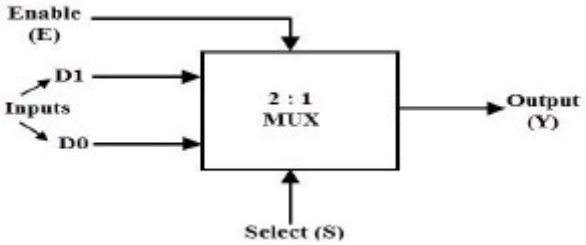


Fig. 5: - Block diagram of the 2: 1 multiplexer

A) 2: 1 MUX using basic logic gates.

The following 2: 1 MUX logic circuit requires 2 AND gates, 1 OR gate, and a NOT gate. When

the circuit of Fig. 10 is implemented using pMOS and nMOS, the circuit requires 6T for every two AND gates, 6T for the OR gate and 2T for the NOT gate. This means that 20T must be implemented for the circuit shown below.

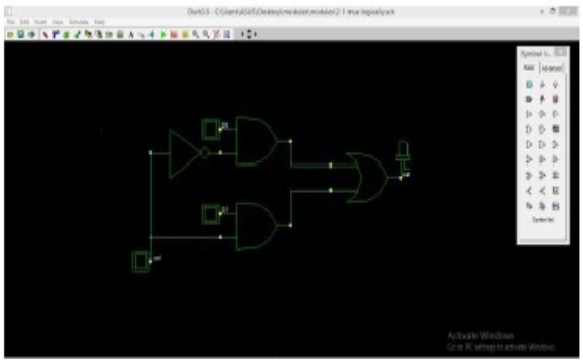


Fig. 6: - MUX 2: 1 using basic logic gates

B) 2-1 MUX with NAND gates

The circuit in Fig. 11 requires four NAND gates, which means that if pMOS and nMOS are used, the above circuit requires 16T (4T for each NAND gate).

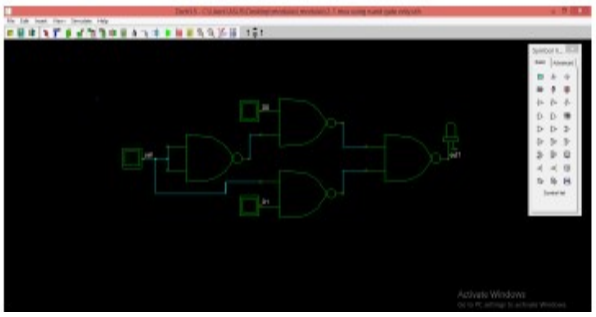


Fig. 7: - MUX 2: 1 with NAND gates

C) 2: 1 MUX using as suggested in document

The CMOS implementation proposed on paper requires 4T in the pull-up network, 4T in the pull-down network, and 2T for the inverter. The circuit requires a total of 10 T, which is less compared to the previous circuits. The circuit is as shown in Figure 12.

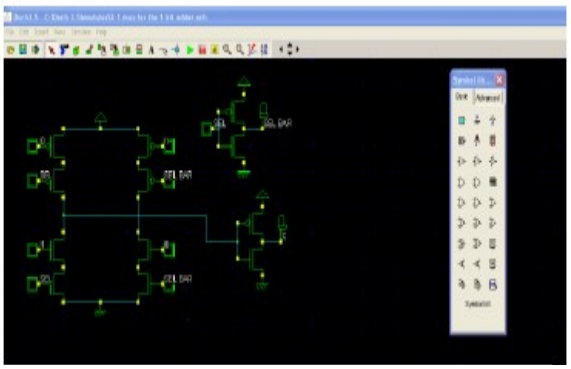


Fig. 8: - MUX 2: 1 proposed in document

D) MUX 2: 1 suggested

The schematic diagram of the proposed 2: 1 MUX is shown in FIG. This circuit is designed with the transmission auxiliary grid and the MOS transistors. The MUX works based on the SEL input. The proposed circuit uses 6T for a 2: 1 MUX layout.

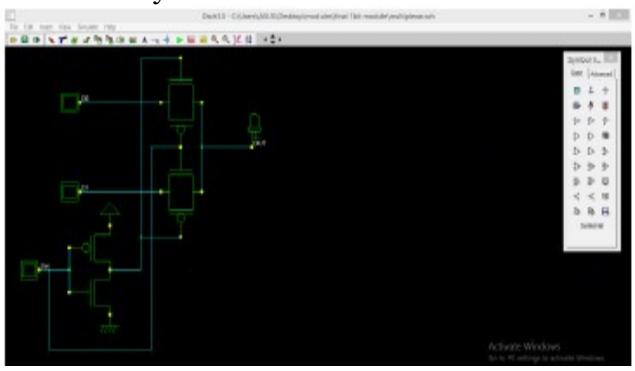


Fig. 9: - MUX 2: 1 suggested

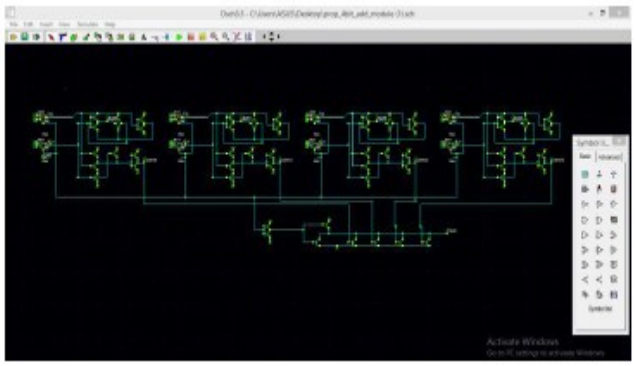


Fig. 10: 4-bit PASTA diagram

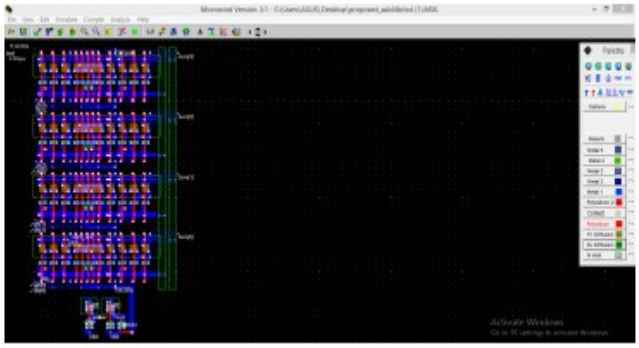


Fig. 1\1: - 4-bit PASTA layout

4. RESULTS AND DISCUSSION

Table 4 shows the analysis of the performance parameters of the proposed circuits. We rated the parameters based on the number of transistors required, propagation delay, area, maximum power and frequency, etc. The superiority of the proposed approach can be determined by comparing the previous and the proposed circuit in terms of performance, delay and delay range. The automatic 4-bit adder proposed in [12] is simulated in the 130 nm bulk CMOS process technology from Faraday using the Synopsys and Cadence tools on a Linux platform, which has a delay of 2.06 ns , an output of 19.09 uW and an estimated area of 775 µm2. While the proposed 4-bit PASTA is simulated in the Microwind 3.1 tool, the

Power indicating a 0.046 ns delay, 1.416 µW power, and a calculated area of 48.85 µm 2, as shown in Table 4 below.

Table 2: - Analysis of the parameters of the proposed circuits

Circuit Parameters	Proposed Half Adder	Proposed 2-to-1Mux	Completion detection circuit	Proposed 4 bit PASTA
No. of transistor Required	12T	6T	5T	101T
Propagation Delay	0.214ns	0.008ns	0.017ns	0.046ns
Area	6.25um2	5.1875um2	1.74um2	48.85um2
Power	0.126uW	0.069uW	2.044uW	1.416uW
Maximum Frequency	4.67*10[9] Hz	125*10[9] Hz	58.82*10[9] Hz	21.739*10[9] Hz

5. CONCLUSION

In this article we implement the modified PASTA. First, the theoretical basis of a single-track pipeline adder is established. The architecture design and CMOS implementations for Parallel Self-Timed Adder are then presented. The new design using a transmission gate and a CMOS transistor is proposed and implemented using 45 nm CMOS technology. The proposed design achieves the reduction in the number of transistors compared to the previous CMOS implementation of PASTA. This makes it possible to obtain a very simple n-bit adder representing a zone. The power consumption is thus much more efficient than the previous timed automatic adder. We also developed a parallel timed 4-bit automatic adder and analyzed it for various performance parameters. . In addition, the circuit works in parallel for independent transport chains and thus achieves a logarithmic average time output with random input values. The termination detection unit for the proposed adder is also practical and efficient. The results of the simulation are used to check the advantages of the modified timed automatic adder.

REFERENCES

1. Akansha Maheshwari, Surbhit Luthra," Low Power Full Adder Circuit Implementation using Transmission Gate", International Journal of Advanced Research in Computer and Communication Engineering Volume. 4, Issue 7 pp.183-185, July 2015.
2. Swaranjeet Singh," Comparative Analysis of CMOS Transmission Gate Based Adders", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 , pp2544-2548, August 2013.
3. N. Weste and D. Harris, "CMOS VLSI Design: A Circuits and Systems Perspective Reading", MA, USA: Addison-Wesley, 2005.
4. D. Geer, "Is it time for clockless chips? [Asynchronous processor chips]," IEEE Comput., Volume. 38, no. 3, pp. 18–19, Mar. 2005.
5. Masashi Imai and Takashi Nanya," Performance Comparison between Self-timed Circuits and Synchronous Circuits Based on the Technology Roadmap of Semiconductors", IEEE/IFIP DSN-2008 2nd Workshop on Dependable and Secure Nanocomputing, pp.1-6, June 2008.
6. N. R. Poole," Self-timed logic circuits", Electronics & Communication Engineering Journal, pp. 261-270, December 1994.
7. Mark A. Franklin and Tienyo Pan," Performance Comparison of Asynchronous Adders",pp.117-125,1994 IEEE.
8. Sparso and S. Furber, "Principles of Asynchronous Circuit Design", Boston, MA, USA: Kluwer Academic, 2001.
9. Ashivani Dubey and Jagdish Nagar," Comparison between Serial Adder and Parallel Adder", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, September 2013.
10. Mohammed Ziaur Rahman, Lindsay Kleeman and Mohammad Ashfak Habib," Recursive Approach to the Design of a Parallel Self-Timed Adder", IEEE Transactions on Very Large Scale Integration (VLSI) System, pp.1-5, 1063-8210, 2014 IEEE.

EFFICIENT ROUTING PROTOCOL FOR VEHICULAR AD-HOC NETWORK (VANET) USING MOBILITY MODELS

Manju padidela[1]., P.Shireesha[2]., G.Haripriya[3]., G.Sivapriya[4]., G.Harshitha[5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: cheers2manju@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0447, 17RG1A0425, 17RG1A0430, 17RG1A0422), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— VANET has become an important research area in recent years. It enables intelligent vehicle-to-vehicle communication (IVC) and improves the safety and efficiency of road traffic. Network simulation is the most common way to evaluate the performance of a large and complex system. You have the freedom to rule yourself or control your own affairs, and you can optimize and repair the cellular network easier and faster. In this document, the AODV routing protocol was simulated using different mobility models such as the random trip model and random path model. The aim of this research is to offer more options by comparing the various parameters of quality of service such as delay, power, power, jitter and packet delivery rate. The analysis was carried out on the basis of various no. of nodes as a result of a radical ad hoc protocol change.

Keywords— VANET, Routing Protocol, Mobility Model, Delay, Energy, Throughput, Packet delivery Ratio, jitter.

1. INTRODUCTION

An ad hoc wireless network is a collection and self-organization of wireless nodes on a network without the help of any infrastructure. All nodes are movable. These networks can be divided into three categories depending on the application.

- Mobile ad hoc network (MANET)
- Wireless mesh network (WMNS)
- Wireless sensor network (WSN)

It is an autonomous cellular network. This can be trained without the need for legacy networking or centralized management and can be configured at random. These have been the most popular among MANET researchers since the early 1990s. Many protocols were introduced for communication with the development of wireless modem and router technology for large area switching. MANET uses multi-hop technology. But only for a few miles of connectivity using a single hop. developed by a network. Mobile nodes are related to the type of VPN network gateway that was used for this type of VANET network. This is made possible by the intelligent transport system and therefore enables efficient communication. This is why VANET is also known as vehicle-to-vehicle or vehicle-to-vehicle communication

Figure 1.1: - Structure of VANET

The main application of VANET is ITS, with the help of which collisions and vehicle services in the vicinity can be prevented. VANET can also operate internationally, so VANET has many uses such as online music playback, GPS services, checking email information and downloading. VANET are new sub-categories in two different types:

- Wireless infrastructure network.
- Network without wireless infrastructure, also known as an ad hoc network

The communication carried out by the mobile nodes follows the path of the base station so

that the wireless infrastructure network contains the base station and the access point.

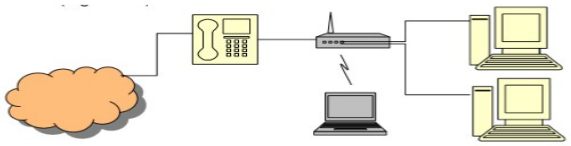


Figure 1.2: - Wireless infrastructure

The figure shows the wireless infrastructure network, which does not require cabling to maintain the connection between VANETs of this network type. A fixed base station or router is required to establish connectivity between the VANET nodes. The VANET node detects it and transmits it to the fixed router using a routing protocol. The data was then transmitted to the other base stations using a routing protocol, and then the data was transmitted to the other base station using a wired network.

On the other hand, when a router is needed to carry out the communication between the nodes of the vehicle and when a base station or a router is not needed. This type of network can directly maintain connectivity from vehicle nodes.

2. RELATED WORKS

VANET modeling, which is contested by experience feedback, uses two mobility models, including feedback for the Manhattan mobility model and the random shift model using SUMO and the OMNeT ++ mobility generator, with the simulation result, packet delivery rate and throughput during the Delay and decrease in jitter. . Mobility in vehicles For a realistic and efficient motorway VANET simulation, the author has integrated the real topology and the extension of the real data of the motorway performance measurement system. This adjustment mechanism is used to adjust a parameter of the log normal model and the urban highway model in this article. The author simulates the parameter where the delay, throughput and jitter increase and the packet delivery rate decreases.

3. PROPOSSED ROUTING PROTOCOL

AODV is a reactive on-demand protocol as well as DSR (Destination Sequence Number). AODV is used for dynamic wireless networks and is a reactive routing protocol that allows nodes to leave and enter the network frequently. It is therefore an on-demand routing protocol, which means that it is forwarded when the source node requests it. Immediate broadcast path of the source node when it is sucked up by the source node. The source node then sends a route request message (RREQ) to its neighbor when the source node requests a route to a destination. It confirms a routing with reply messages (RREP). If one of its neighbors routes to the destination, if not the node, the neighbor resends the RREQ and continues until the RREQ returns the request. The AODV has a local nutrition plan to maintain the route for as long as it is effective.

4.SYSTEM DESIGN

The random motional mobility pattern changes direction and / or speed, including a time interval between nodes, by staying in one place for a period of time and once. This time node chooses a random target in the simulation area and a speed that is evenly distributed between the minimum and maximum speed. The node evenly and randomly selects its new direction ϕ (t) from (0.2π) and the speed S (t) from (0, Smax) in the time interval t, the node moves with the speed vector [V (t) cos ϕ (t), V (t) sin ϕ (t)] When the node reaches the limit of the simulation area, it jumps at an angle of ϕ (t) or π-ϕ (t).

The random travel pattern has less memory and creates a playable movement pattern.

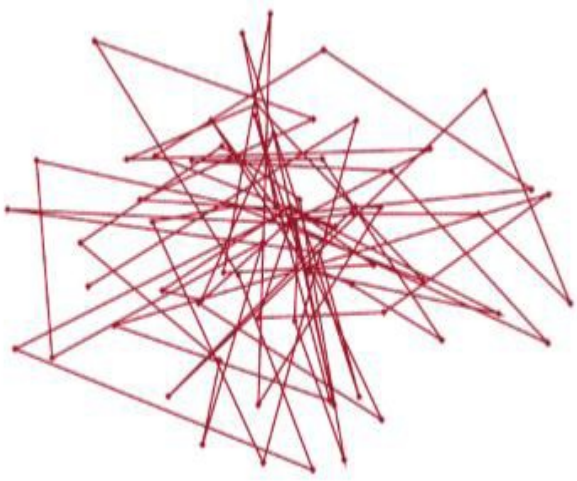
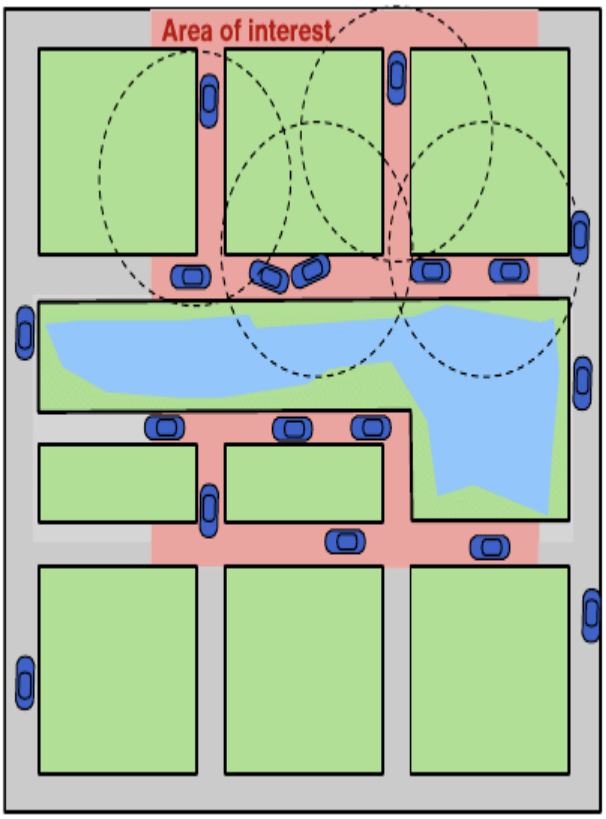


Figure.1: - Displacement diagram for the random displacement model

The even distribution of the nodes finally reaches a steady state in the course of the simulation time and forms the transformation of the random path model. The cell phones are concentrated in the center and not on the borders of the region. Here the mobile nodes are almost zero. The random path model has turned this news on its head. The node has chosen a fixed direction randomly and comparably and moves side by side in the same direction until it reaches the limits. He randomly chooses a different direction of travel after reaching the limits and stopping to take a break. Therefore this model is more stable than RTMM.

The Manhattan Grid (MG) mobility model using a grid road topology. This mobility model has been proposed mainly for travel in urban areas where the roads are organized. Mobile nodes move horizontally or vertically on a city map. The MG model uses a probabilistic approach to the selection of node movements as a vehicle decides at each intersection to continue moving in the same direction or to turn. The break probability and the maximum break time can also be set in order to model different situations such as traffic lights or jumps in traffic.



5. RESULT & DISCUSSION

In practical systems, a mobile user generally travels with a view to a destination, which is why the location and speed of the mobile phone is likely to correlate with its current location and speed in the future. The memoryless nature of random walk models makes it impossible to represent such behavior. Another mobility model that is widely used in cellular network analysis is the fluid flow model, which is suitable for vehicle traffic on highways, but not for pedestrian movements with frequent stops and walks. Models that, like the two extreme cases, include random walking and constant, velocity fluid flow models. In the GM model, the future location of a rover is predicted based on the probability density function of the rover's location, which is reported by the GM model as a function of its location and its speed at the time of the last location update. . This model captures the speed correlation of a moving node over time and represents random movements without sudden stops or sharp

turns. At set time intervals, the movement is done by updating the speed and direction of each node. With each iteration, the new parameter values are calculated as a function of the current speed and direction or a random variable. In the urban vehicle mobility model, the road is a critical factor, forcing nodes to constrain their movements to well-defined trajectories regardless of their ultimate destination. Two different models of urban vehicle mobility are as follows

Stop Sign Model (SSM): -

The stop sign model mimics the mobility of vehicles in the presence of stop signs at every intersection. Each vehicle waits for a set period of time when it reaches an intersection before driving to its destination. Each vehicle maintains a certain distance from the vehicle in front.

Traffic Sign Model (TSM): -

In this model, the vehicle may or may not stop at a traffic light. When a vehicle is waiting at an intersection, all successive vehicles arriving at that intersection will wait for it to move. Vehicles queuing at an intersection move together after the selected waiting time has elapsed

6. CONCLUSION

This document contains an examination of VANET and various mobility models with the specified routing protocol. Section II describes the related work of various researchers and scientists. This review will add to future work. We compared the various parameters of the Random Path Model (RPM), the Random Trip Model (RTP), the Manhattan Model (MH), the Markov Model (Mk) and the Urban Vehicular Model (UMM) using the AODV routing protocol.

M M	Jitter	Energy	Through-put	Delay	PDR
RTM	High	High	Varies according to cluster size	Less	High
RPM	Less	High	High	Less	High
MH	Less	Less	High	Less	Less
MK	High	High	High	High	Less
UMM	High	Less	Low	High	Less

REFERENCES

1. Bhushan Dhok, "Performance Matrix Optimization of Routing Protocol using Swarm Intelligent for Vahicular Ad-Hoc Network (VANET)".
2. Harald Meyer, "VANET Mobility Challenges by Feedback Loops."
3. Institute Of Electronics and Electrical Engineers (IEEE), 2011.
4. Nabeel Akhtar, "Vehicle Mobility Model For Realistic And Efficient Highway VANET Simulation." Institute Of Electronics and Electrical Engineers (IEEE),Vol.64, No. 2015.
5. Nilambike S," An Efficient Environmental model Considering Factor For V2I application services." ." Institute Of Electronics and Electrical Engineers(IEEE), 2015.
6. Yang He, "A Stable Routing Protocol For Highway Mobility Over Vehicular Ad-Hoc Network." Institute Of Electronics and Electrical Engineers (IEEE), 2015.
7. Huixian Wang, " VANET Modelling and Design Under Mobility Conditions." Institute Of Electronics and Electrical Engineers(IEEE), vol.63 no.3,March 2013.

SMART SHOE FOR FOOT PRESSURE MONITORING IN DIABETIC PATIENTS AND ELDERLY PEOPLE

Narmada kari[1]., Y.Poojitha[2]., G.Pravalika[3]., D.Sadhana[4]., B.Keerthana[5].,

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: mamatha@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0460, 17RG1A0419, 17RG1A0414, 17RG1A0407), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Diabetics cause neurovascular complications that lead to the development of areas of high pressure in the feet. Diabetic neuropathy causes severe nerve damage that can ultimately lead to ulcers. This article is about early detection of neuropathies in the foot at home. Flexi force sensors measure the pressure in different areas of our foot and are displayed on the wearable device. Vibration motors can be used to stimulate vibrations at different frequencies at desired locations, thereby improving blood flow. Therefore, an inexpensive foot pressure and motion analysis and blood flow stimulation system is being developed that a patient can use anywhere to monitor the pressure distribution of the foot..

Keywords— neurovascular, neuropathy, ulceration

1. INTRODUCTION

Diabetics are a leading cause of illness and death worldwide. Diabetics lead to the development of areas of high pressure on the human limbs. In 2012 a survey on "The Economic Cost of Diabetes in America". It found that 9.3% of the population was affected by diabetes. It also found that 25.9% of people over 65 (11.8 million elderly people) had diabetes. In 2010, approximately 69,071 death certificates indicated that diabetes was the underlying cause of death. Diabetics cause neurovascular complications that lead to the development of areas of high pressure in the feet. Diabetic neuropathy causes severe nerve damage that can ultimately lead to ulcers. According to a study by a biomedical university in the United States, sending imperceptible vibrations through the feet of diabetics and stroke sufferers dramatically improves damaged nerves and stimulates blood flow.

2. RELATED WORKS

Benoit Mariani, Mayt'e Castro Jim'enez, François JG Vingerhoets and Kamiar Aminian, IEEE Fellow (2012) “Wearable sensors on shoes for assessing gait and turning in patients with Parkinson's disease”. This article introduces an innovative technology based on wearable shoe sensors and a processing algorithm that provides outcome measures that characterize the motor symptoms of Parkinson's disease during TUG tests and while walking. Our results in ten patients with Parkinson's disease and ten elderly patients of the same age show an accuracy ± accuracy of 2.8 ± 2.4 cm / s and 1.3 ± 3.0 cm for the stride pace and the estimate of the stride length. Compared to optical motion detection with the advantage that it can be used comfortably at home or in the clinic without the subject feeling uncomfortable. In addition, the use of new spatiotemporal parameters, including spin, oscillation width, path length and their variability between cycles, was validated and showed interesting trends for differentiating between patients in the ON and OFF states as well as in control persons.

3. EXISTING SYSTEM

- Diabetic neuropathy is a serious medical disorder and can be prevented by detecting abnormal pressure patterns under the foot early on. Although foot pressure distribution measurement kits are available in India and elsewhere, they are not yet readily available to a large segment of the population. They are too expensive to own and too big to be portable. Foot pressure gauges are also not readily available in less developed countries, where there are many communities with high diabetes prevalence.

4. PROPOSED SYSTEM

This project not only enables early detection, but also offers treatment and prevention of diabetic neuropathy. The sensor and actuators can be installed in the shoe unit, and the monitoring unit is a simple handheld device that is portable and less expensive. Therefore,

our project will be cheaper and available in less developed countries. Thanks to the large external memory, the system can continuously save the data of the smart shoes over several weeks.

Description of the equipment

- The system consists of two components
- shoe unit
- Handheld unit

The shoe unit has a 3-axis MEMS accelerometer to monitor foot movement. The pressure distribution of the foot is measured with a set of Flexi Force pressure sensors located on the sole of the shoe. To improve blood circulation, the smart shoes have a set of miniature vibration motors. The shoe unit measures the outputs of the pressure sensor and transmits the information to the portable control unit via an IEEE 802.15.4 wireless transceiver.

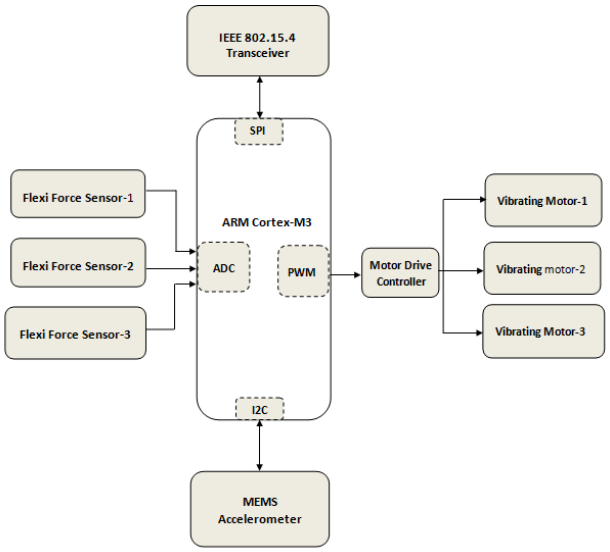


FIG 1. Block diagram of the shoe unit Transmitter

The portable device is equipped with a 65K color TFT touchscreen that receives data wirelessly. When the accelerometer detects an abnormality, the buzzer is used to alert the patient. A 2 GB memory card is used to store the collected data.

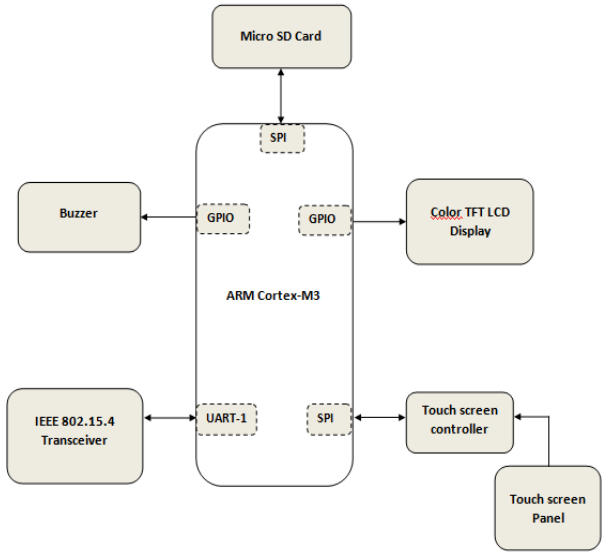


FIG 2. Block diagram of the portable devices receiver

5. DESCRIPTION OF THE MODULES

The work system consists of three modules such as The device monitors the movement of the user's foot using a 3-axis MEMS accelerometer and actively looks for situations that lead to foot injuries. As soon as the system detects an abnormality in the pressure distribution of the user's foot or in the movement of the foot, it alerts the portable touchscreen device. The portable touchscreen device communicates wirelessly with the connected device and collects the data in real time and stores it on the memory card for later analysis by a physicist. In this system, the pressure distribution of the foot is measured by a set of Flexi Force pressure sensors located on the insole of the shoe. These sensors are based on force measuring resistors, the resistance of which changes inversely with the force exerted. The shoe unit measures the outputs of the pressure sensor and transmits the information to the portable control unit via an IEEE 802.15.4 wireless transceiver. The monitor is equipped with a 65K color TFT touchscreen that receives data wirelessly and displays foot pressure information in a color bar graph. This data is also saved on the memory card. The shoe unit and the portable display unit use LPC1313, a 32-bit ARM Cortex-M3 microcontroller from NxP Semiconductors. In addition to application

software and device driver firmware, the microcontroller also runs software such as graphics library, FAT-32 file system, and IEEE 802.15.4 protocol stacks for wireless networks. The portable touchscreen unit communicates wirelessly with the foot unit, collects data in real time and stores it on the memory card for later analysis by a doctor. The shoe unit measures the output of the pressure sensor and transmits the information to the portable monitoring unit using an IEEE 802.15.4 wireless transceiver. The monitor is equipped with a 65K color touchscreen TFT that receives the data wirelessly and also displays the foot pressure information when you save this data to the memory card.

6. RESULT & DISCUSSION

The data logger option offers options for START_RECORD and VIEW_RESULT. The START_RECORD shows three scales A, B, C for the three flexible load cells. Depending on the pressure, the display is shown on the scale. The VIEW_RESULT option supplies the maximum measured value as well as the average value of the system

FIG 3. Options provided in the data logger

The vibration motor option allows the patient to deliver vibrations to the muscles in their feet. Again it shows three scales for the three vibration motors. By adjusting the scale, the frequency of the vibration motors can be manipulated by the user.

FIG 4.Pressure area at sensors A, B, C.

7. CONCLUSIONS

This system has been proposed to provide a short term and inexpensive means to patients with diabetic disorders. It is designed to control the high pressure areas of your feet by delivering vibrations at different frequencies through the muscles of your feet depending on the needs of the user. This device can be used from anywhere, anytime. Future improvements can be made by minimizing the size of the components used in the shoe to make it more comfortable for the wearer who wears it. The shoe unit can also be connected to the mobile phone.

REFERENCES

1. Jeffrey Larson, Kuo-Yun Liang, and Karl H. Johansson, Fellow, IEEE,"A Distributed Framework for Coordinated Heavy-Duty Vehicle Platooning", IEEE Transactions on Intelligent Transportation Systems, Vol. 16, No. 1, February 2015.
2. J. Larson, K.-Y. Liang, and K. H. Johansson, "A distributed framework for coordinated heavy-duty vehicle platooning," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 1, pp. 419–429, Feb. 2015.
3. K.-Y. Liang, J. Mårtensson, and K. H. Johansson, "Fuel-saving potentials of platooning evaluated through sparse heavy-duty vehicle position data," in Proc. IEEE Intell. Veh. Symp., Dearborn, MI, USA, Jun. 2014, pp. 1061–1068.
4. S. van de Hoef, K. H. Johansson, and D. V. Dimarogonas, "Fuel-optimal centralized coordination of truck-

platooning based on shortest paths," in Proc. Amer. Control Conf., Chicago, IL, USA, Jul. 2015, pp. 1–6.

5. Kuo-Yun Liang, Jonas Mårtensson, Member, IEEE, and Karl H. Johansson, Fellow, IEEE, "Heavy-Duty Vehicle Platoon Formation for Fuel Efficiency" IEEE Transactions on Intelligent Transportation Systems, 2015.
6. Ge Guo, Senior Member, IEEE, and ShixiWen, "Communication Scheduling and Control of a Platoon of Vehicles in VANETs", IEEE Transactions on Intelligent Transportation Systems, 2015.
7. Mario di Bernardo, Fellow, IEEE, Paolo Falcone, Member, IEEE, Alessandro Salvi, and Stefania Santini, Member, IEEE "Design, Analysis, and Experimental Validation of a Distributed Protocol for Platooning in the Presence of Time-Varying Heterogeneous Delays", IEEE Transactions on Control Systems Technology, 2015.

SMART IOT HEALTH CARE AND MONITORING OF PHYSIOLOGICAL PARAMETERS USING RASPBERRY PI

M. Mahesh[1]., K.Jayanthi[2]., K.Jyoshna[3]., B.Pooja[4]., S.Meghana[5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: mahesh@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0485, 17RG1A0487, 17RG1A0473, 17RG1A04A1), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Today, in the health monitoring system, it is necessary to constantly monitor the patient's physiological parameters. This system includes a monitoring system that allows the physiological parameters of the patient's body to be monitored every 10 seconds. A sensor node was connected to the patient's body to collect all signals from the wireless sensors and send them to the BSN care node. The sensors connected to the patient's body form a wireless body sensor network (WBSN) and can record the heart rate and the temperature of the environment. This system is primarily intended to record abnormal conditions in the human body and abnormal physiological parameters. The main advantage of this system over previous systems is to reduce power consumption to extend network life, speed up and expand communication coverage to improve patient quality of life..

Keywords— IOT, BSN, LPU, PDA, EKG.

1. INTRODUCTION

Today one-day children suffer from at least one death and are health conscious and put on weight. And in the hospital there are difficulties in treating these patients. The Body Sensor Network provides patients with excellent portability for detecting patient abnormalities and is used to avoid critical situations and provide timely treatment. Therefore, the IoT concept used and the sensor are connected to the human body via a well-managed wireless network. To measure heart rate, temperature etc. can be monitored by sensors. Therefore, the sensors and the software system can work remotely through the integration of all components. In this system we use a sensor to record the biological parameters and process them with Raspberry Pi. All hardware components are integrated into the software system to display the data to the user and the user can control the system.

2. PROPOSED SYSTEM

In a modern and secure IoT-based healthcare system, the Internet of Things offers the flexibility and fast operating speed to achieve the expected results. Here hardware elements such as Raspberry Pi 3, heart rate sensor, temperature sensor, etc. are used. and more sensors can also be used to detect various biological functions. In this hardware, the elements are integrated into the software system that controls the hardware and reporting. The heart rate sensor is used Easy Pulse 1.1 and the general temperature sensor is used to sense temperature. With this system we can detect abnormal conditions in the human body in real time. Raspberry pi3 is a device connected to sensors, the sensors are connected to human bodies, and this raspberry pi3 is connected to software systems through wireless connection. When all the elements are connected, the sensor detects the data from the human body and then sends it to the server. After that these data are compared with the data already stored in the system default values. As a result, the normal and abnormal condition check is carried out. And if there are any abnormalities, immediately send a message to the doctor in order to avoid critical situations. In this system, the administrator is there to control the system. He can control new patient and doctor entries. When you get the sensor data and database storage is shown on one side of a separate user interface that periodically loads and retrieves data from the system database. The time interval varies between 5 and 10 seconds. In the event of anomalies, the message is sent to the doctor's mobile phone within a minute. In this system we should have to centrally connect the system and the hardware device as well as the server. For this we need two servers, one for the implementation of the system and one for the database in which the data is stored.

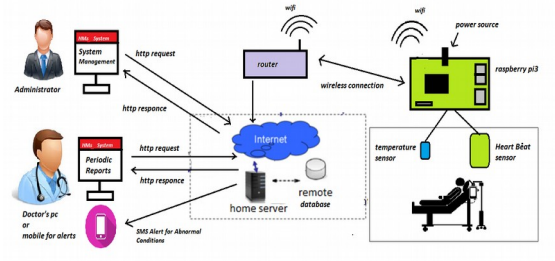


Fig. 1 System architecture

Digital format to have an advantage in terms of operating speed, and digital processing is much more efficient than analog signal. For connectivity, we use the Kitt app connecting devices and a software system that works as an intermediary when sending data to Raspberry Pi comes to Kitt and then transfers it through the system database. This also has the advantage of shortening the time intervals between the situation and your notification of the doctor, which means that the doctor will know the situation immediately if it occurs. In this system we use the BSN Care server to implement the system and we also use a separate database server to store the data. MySQL is a relational database that stores data in record format. Separate tables are created to store the data from the sensors. The sensors re connected to the local processing unit (LPU) to process the data in digital format.

3. MATERIAL MODULE

The material we use is important to our project. The main tasks are to retrieve the physical parameters of the heart rate monitor and the temperature sensor and convert them into digital ones. It is also known as a Local Processing Unit (LPU). The DHT11 is an inexpensive digital temperature sensor. Based on a powerful 8-bit microcontroller, it offers fast response and high precision. The sensor can only get new data once every 1 second . Easy Pulse is used to measure heart rate and the DIY heart rate monitor as you just stick your finger in to measure the cardiovascular waveform. The latest version of Easy Puls (V1.1). It uses an infrared light source, around the fingers on one side and the photo detector on the other side to light to the change of the transmitted light to be measured in tissue due to the change in blood volume. Analog wave and a digital impulse at the output and in sync with the beat

Organizational chart of the proposed system

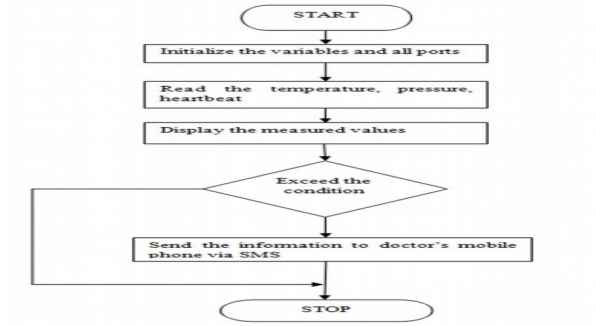
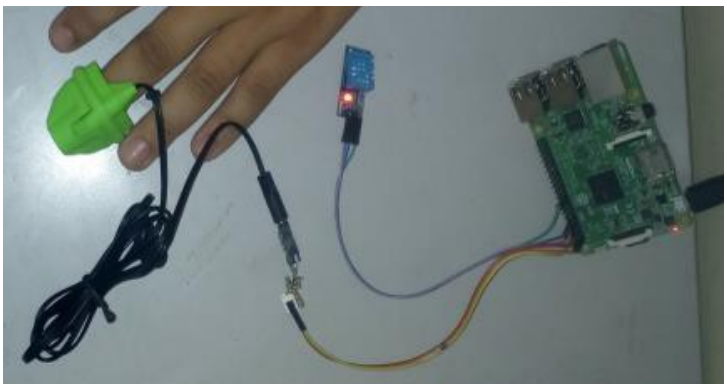


Fig 3: Organizational chart of the proposed system

4. RESULT ANALYSIS

1. Sensors that recognize data and send it to the PuTTY server



Fi 4: Sensors connected to the body

2. The data is sent to the PuTTY server

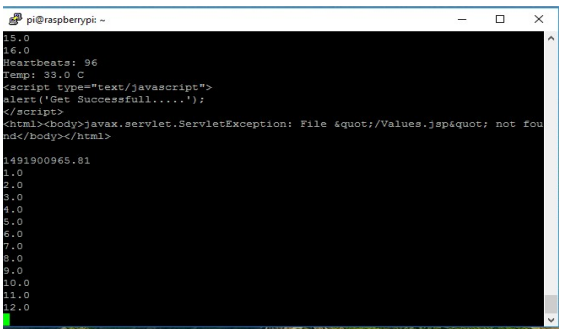


Fig 5: Screenshot of the PuTTY server

The message is sent to the mobile as an alert

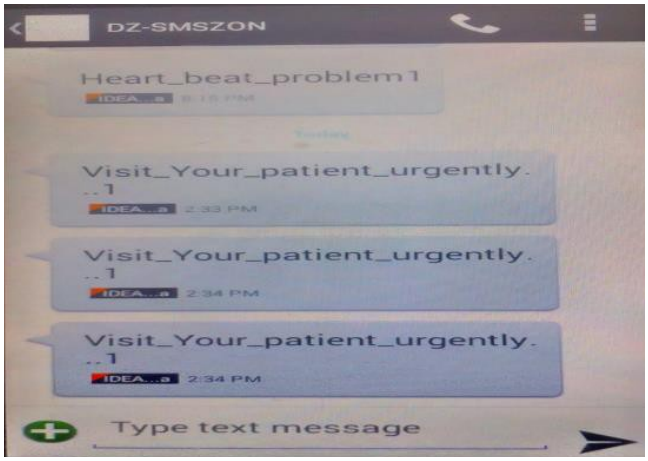


Fig 6: News alert on the mobile phone

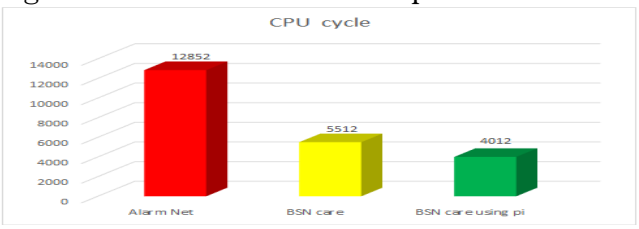


Fig 7: Benchmark performance based on CPU cycles

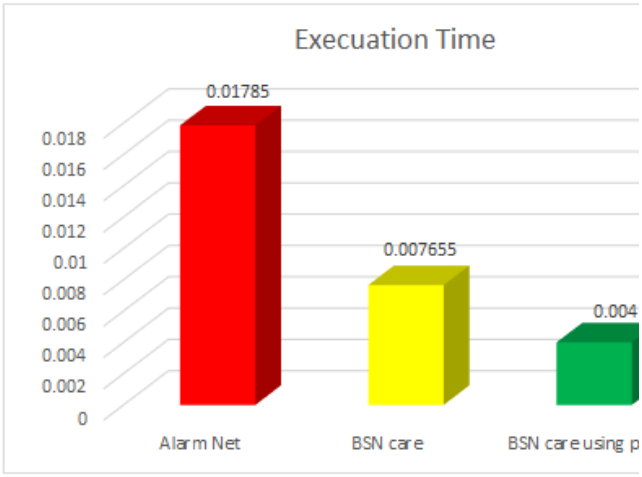


Fig 8: Benchmark performance based on runtime

5. CONCLUSIONS

The result of the project has shown that it works with real-time monitoring. If there are any abnormalities, the alert will be sent to the registered number. We can therefore avoid critical situations and deal with them in good time.

REFERENCES

1. Body sensor network – a wireless sensor platform for pervasive healthcare monitoring [benny p.l. lo, surapa thiemjarus, rachel king and guang-zhong yang] 2015.
2. A Unique Health Care Monitoring System Using Sensors and Zig Bee Technology [Ekta Madhyan ahesh Kadam, Department of Electronics & Telecommunications, Mumbai University, India] 2013.
3. Predictive Monitoring of Mobile Patients by Combining Clinical Observations With Data From Wearable Sensors Lei Clifton, David A. Clifton, Marco A. F. Pimentel, Peter J. Watkinson, and Lionel Tarassenko.
4. Discovering Multidimensional Motifs in Physiological Signals for Personalized Healthcare. [Arvind Bal Subramanian, Jun Wang, and Ramakrishnan Prabhakaran] 2014.
5. Coexistence of zigbee-based WBAN and WiFi for Health Telemonitoring Systems [Yena Kim, Student Member, seungseob Lee, Student Member, and sukyoung Lee, Member,] 2013.
6. Effective Ways to Use Internet of Things in the Field of Medical and Smart Health Care. [Kaleem Ullah, Munam Ali Shah, Sijing Zhang, Department of Computer Science, University of Bedfordshire, Luton, UK] 2015.
7. Automated Patient Handling Activity Recognition for At-Risk Caregivers Using an Unobtrusive Wearable Sensor. [Feng Lin, Xiaowei Xu, Aosen Wang, Lora Cavuoto, and Wenyao Xu] 2015.

IMPLEMENTATION OF CUDA FRAMEWORK IN EMBEDDED SYSTEM FOR BETTER PERFORMANCE OF GPU

K Surekha[1]., G.hima bindu[2]., M.Ashwini[3]., M.Sushma[4]., Pallak singh[5].,

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: surekhakorudu413@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0481, 17RG1A0491, 17RG1A0492, 17RG1A0498), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— CUDA is a programming model developed and introduced by NVIDIA Company in 2006. This programming works in a heterogeneous environment where we have two different types of CPU and GPU processors. By using CUDA programming, the programmer can leverage a GPU processor to execute code that reduces execution time. However, there are some disadvantages to using a GPU processor in the system such as: B. the increase in system acquisition costs, the increase in power consumption, the need for more space for new GPU hardware and the use of the GPU processor in the system is relatively small. To overcome these drawbacks in the system, we will use one of the visualization techniques to allow the application to use the remote GPU to run the code. There are many display techniques that the programmer can use the remote GPU such as VGPU, GVirtuS, GridCuda, Shadowfax, GViM, vCUDA, rCUDA, and DS-CUDA. In this article we will implement rCUDA on one of the embedded system platforms (Jetson Tk1) to fix these problems in the system. rCUDA is a platform designed and developed by the development team at the Polytechnic University of Valencia, Spain. The resonances of the implementation of the platform form rCUDA in the support system for other platforms because it has a higher fidelity, shows better performance compared to other display technologies and also shares the processor GPU between clients.

Keywords— CUDA, rCUDA , Embedded System and Jetson Tk1.

1. INTRODUCTION

The GPU (Graphics Processing Unit) is a processor that was originally designed for graphics operations, especially when the graphics application becomes more complicated and places more stress on the CPU processor. The GPU processor has become increasingly popular as the demand for graphics applications has increased. It can process data in parallel, which increases performance, and it can also process 2D and 3D data. The success of the GPU determined that the software developer used the GPU for a general calculation called GPU. Designed for graphical operations to perform general purpose calculations. GPU is still used for applications that require high performance processors such as chemical physics, image analysis of fluid dynamics, and many other areas. However, there are some drawbacks to using a GPU processor in the system such as: B. increased power consumption, increased acquisition cost, it also requires more space to adapt to new hardware, and the system does not require GPU processing in all operations, leaving the GPU processor idle most of the time.

2. LITERATURE REVIEW

As mentioned above, adding the GPU processor to the system increases power consumption by about 30% [1]. The reasons behind the incense in power consumption are because the system uses two processors instead of one. The second disadvantage is the increase in initial cost as new hardware is added to the system, which also requires more space for customization. Adding the GPU processor to the system doesn't mean apps are using it all the time. Time it is only used to run a piece of application code that requires a lot of repetition, which means the GPU processor, is idle most of the time.

3. PROPOSED SYSTEM

CUDA (Compute Unified Device Architecture) is a model developed, programming and introduced by NVIDIA 2006. This platform programming runs on a heterogeneous platform has two different types of processors CPU and processors, and the flat - shape one of the programming modules allows the programmer to use the Use the power of GPU processors for general calculations. It supports various programming languages such as C, C ++, Fortran and Python, which allows the programmer to easily write code without learning a new language. However, the CUDA

programming model only supports the NVIDIA hardware.

rCUDA (Remote CUDA) is middleware that allows the device to use another device's remote GPU to run GPU code. This platform, developed by the Parallel Architectures Group at the Polytechnic University of Valencia (Spain), allows applications to simultaneously access GPUs installed in other nodes in the cluster. If several applications have to access the GPU in rCUDA , the rCUDA middleware is responsible for the common use of the GPU between the applications. The source code of the applications does not require any code change to use the remote GPU. It only causes additional costs in the execution time, which are generally less than 4% [7].

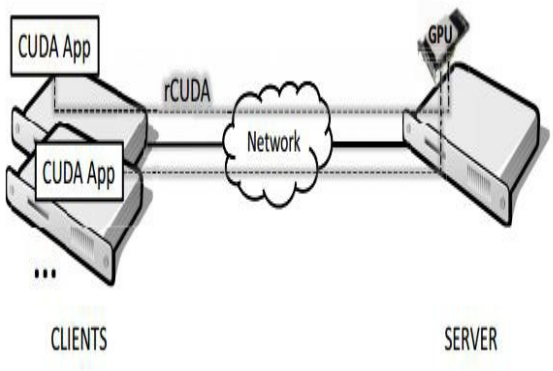


Fig. -1: Simple rCUDA scenario [1]

Jetson TK1 (also called Tegra K1) is an integrated board designed and developed by NIVIDA . This is one of two solutions released by NVIDIA to support integrated GPU systems.

Jetson TK1 has 192 CUDA GPU cores (Kepler GPU), 4 ARM Cortex-A-15 processors and 2 ISP cores. It also supports CUDA programming which allows the programmer to use the GPU processor to run code. Moreover, the Jetson TK1 Board in comparison to one with a GPU processor -equipped PC low cost and low power consumption to , what it a good choice for researchers and makes students involved in the work GPU programming. In this article we will use the implementation platform form rCUDA on the Jetson TK1 card to operate its GPU code for remote devices.

Fig. 2 Jetson TK1 dashboard

4. FRAMEWORK ARCHITECTURE OF THE RCUDA

The distributed client-server architecture of the rCUDA framework consists of two software modules, as shown in Figure (3):

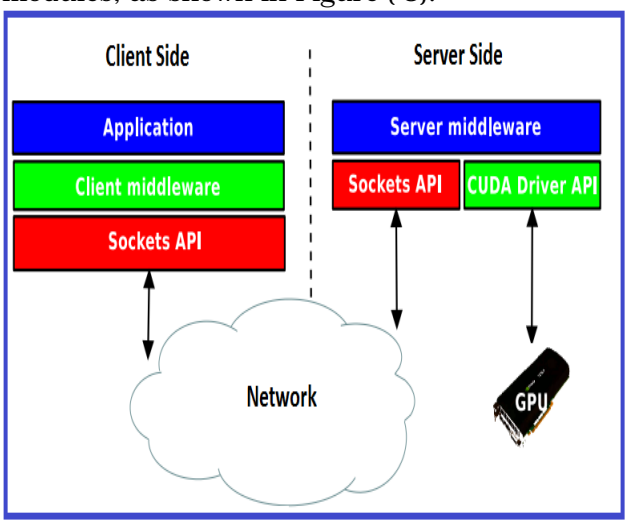


Fig. 3 rCUDA architecture [1]

1. Client middleware: Consists of a series of containers that are responsible for replacing the runtime library on the client computer with rCUDA libraries . The client middleware is also responsible for routing CUDA API calls generated by applications. At runtime, the client middleware is responsible for forwarding the API call from the client computer and waits for the server result.

2. Server Middleware - Installed on the computer on which the GPUs reside. Who is responsible for receiving, interpreting and executing the API call sent by client computers? RCUDA platform that can

support different clients at the same time. To manage more than one client at the same time , the server middleware multiplexes access to the GPU processor between clients and ensures efficient multiplexing of rCUDA, which is integrated into the SLURM scheduler, an open source job scheduler , to achieve more efficient performance . The communication between the client and the server takes place over the network. To establish communication between the server and the client we can use one of two protocols like TCP or INFINIBAND. TCP protocol for the Ethernet connection. However, the INFINIBAND protocol is used for high-speed connections.

5. RESULTS

Server side:

Afterdownloading files rCUDA, unzip first the p ackage rCUDA to any decompression software. Then copy the rCUDA folder to the computer's server. To rCUDA first on the server to perform are preparing the environment must with the export command. The export command adds the variable to a shell's environment variables. These variables are passed to subordinate processes that we can use to run programs. In this scenario, the LD_LIBRARY_PATH variable points to the location of the CUDA libraries, which can usually be found in "/ usr / local / cuda / lib64". If the cuDNN libraries are to be used , they should also be added to the LD_LIBRARY_PATH variable . After adding the path of the CUDA libraries, the number of GPUs in the system must be specified in rCUDA . This is done via the export command RCUDA_DEVICE_COUNT = 1.

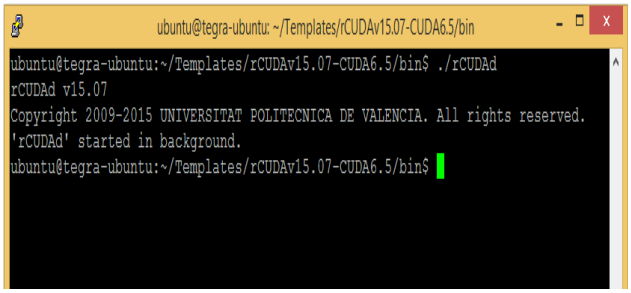


Fig-4 Server rCUDA in is performed .

At this point the server is waiting for the incoming call from the client. To do this, the client and the server must be in the same network in order to be able to communicate. For debugging purposes, we can rCUDA in a different way to run, in which the communication and the call between the server and the client are displayed.

2. Client side:

As mentioned above, the rCUDA client consists of wrappers that replace the CUDA runtime libraries.

To run the code on a remote GPU, the first CUDA compiler must be installed on the client computer. The CUDA compiler generates the binary code file. After the binary file from the compiler has generated, the applications using the rCUDA- library run properly, you must configure the following variables:

- Export LD_LIBRARY_PATH: Points to the storage location of the rCUDA libraries .
- RCUDA_DEVICE_COUNT: Indicates the number of GPUs available on the remote server
- Export RCUDA_DEVICE_0 = 192.168.xx: Contains the IP address of the server in the network.

If rCUDA is working properly, the normal result of the application is displayed.

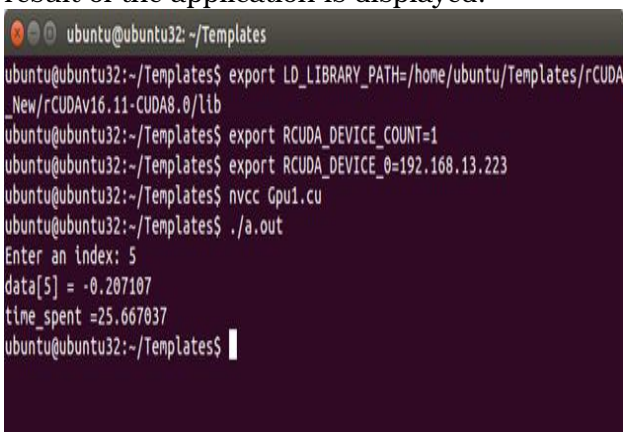


Fig-5: The output of the code

3. CONCLUSION AND FUTURE WORK

The rCUDA framework was implemented on the Jetson TK1 card , an integrated card with CPU and GPU processors. After the implementation of the rCUDA framework , we can access the GPU from the remote PC. The remote application can use

the Jetson TK1 GPU to run the code. In future work we will measure the current system overhead when we use the rCUDA framework to run the applications.

REFERENCES

1. F. Silla, J. Prades, S. Iserte and C. Reaño, "Remote GPU Virtualization: Is It Useful?," 2016 2nd IEEE International Workshop on High-Performance Interconnection Networks in the Exascale and Big-data Era (HiPINEB), Barcelona, 2016.
2. M. S. Vinaya, N. Vydyanathan and M. Gajjar, "An evaluation of CUDA-enabled virtualization solutions," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, 2012.
3. C. Reaño, F. Pérez and F. Silla, "On the Design of a Demo for Exhibiting rCUDA," 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Shenzhen, 2015.
4. J. Duato, A. J. Peña, F. Silla, R. Mayo and E. S. Quintana-Ortí, "rCUDA: Reducing the number of GPU-based Computing & Simulation, Caen, 2010.
5. C. Reaño and F. Silla, "A Performance Comparison of CUDA Remote GPU Virtualization Frameworks," 2015 IEEE.

MULTIBANDING OF L-BAND RESONANT MICRO STRIP PATCH ANTENNA USING HFSS

Dr. Archek Praveen Kumar[1]., A.Rahalya[2]., Gauri tiwari[3]., K.Sukeerthi[4]., M.Nikitha[5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (:archekpraveenkumar@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0461, 17RG1A0478, 17RG1A0488, 17RG1A0490), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— A 1.81 GHz L-Band resonance micro strip antenna has been designed. The coaxial cable antenna parameter S11 is greater than -20.3684 dB at the desired frequency. Then the same antenna is converted into a multi-band antenna using two branch lines. Now the antenna resonates in the L-band at 1.65 GHz and 1.8375 GH with return losses of -19.377 and -23.8268 dB, respectively. The gain of the two antennas is 4.2 and 5 dB, respectively. The results simulated in Ansoft HFSS confirm that the antenna can be used in the L-band. The VSWRs of the antennas are 1.9 and 1.5, respectively..

Keywords L-band, S-parameters, return loss, gain, polar diagram.

1. INTRODUCTION

Most portable wireless communication devices require more than one frequency band to be covered in order to support more wireless applications. For example, a mobile telephone antenna may be required to provide wireless access services for WLAN (2.45 GHz) and PCS (2.2 GHz) to provide. If the antenna is to cover the WiMAX band (3.3 - 3.7 GHz) , a tri-band antenna is required. However, the microstrip antenna has a narrow bandwidth and operates on a single frequency. Therefore, these antennas have to be modified so that a multi-band antenna with sufficient bandwidth is obtained.

Recently, multiband patch antennas have been developed and analyzed to cover various wireless communication services such as GSM, DCS, CDMA and PCS [2, 3 4]. Thus a single antenna covers these bands must it be a trade multiband. The solution to the problem is to use techniques such as probe compensation (L-shaped probe, capacitive "cylinder" on the probe), parasitic patches, direct coupled patches, groove-loaded patches, and grooves (U-groove, V-shaped) and grooves -Patch, U-shaped groove), stacked patches, scatter band patch and the use of electromagnetic band structures (EBG) [4-10] Most of these methods require complex feeding techniques and complex structures such as overlaying and parasite structures.

To avoid the expected disadvantages, a simple antenna with branch lines on both resonance sides of the patch is offered. First, Ansoft HFSS designs and simulates a rectangular patch antenna with a simple coaxial feed. Then two leads are removed from the patch. This article compares the simulated antenna results. In addition, the production of the derivative lines is very easy to carry out, since no special tools for printing are required for the production steps.

2. PROPOSED ANTENNA SYSTEM

In the proposed antenna, a rectangular spot is designed on the FR4 substrate. This patch is then removed with single and double bypass lines. However, the dimensions of the antenna fed by a coaxial cable are calculated from its design equations.

Design equations: The dimensions of the rectangular patch antenna are calculated using the following design equations [2].

$$W = \frac{c}{2fr}\sqrt{\frac{2}{\epsilon r+1}} \qquad \text{--- (1)}$$

For the given operating frequency and dielectric constant, the width of the patch antenna can be calculated by equation 1. Furthermore, the effective dielectric constant is calculated by equation 2 [2].

$$\epsilon reff = \frac{\epsilon r+1}{2} + \frac{\epsilon r-1}{2}\left[1+12\frac{h}{W}\right]^{-.5} \text{--- (2)}$$

Due to the edge effect, the effective length of the patch is increased. This is calculated by equation 3.

$$\Delta L = 0.412h \frac{(\epsilon reff+0.3)\left(\frac{W}{h}+0.264\right)}{(\epsilon reff-0.258)\left(\frac{W}{h}+0.8\right)} \quad \text{--- (3)}$$

Now the net length of the patch is calculated according to the formula

$$Leff = L + 2\Delta L \quad \text{--- (4)}$$

Table 1 shows the various dimensions that were calculated and taken for the single band antenna design.

Table 1: Calculated dimensions of the patch antenna

Parameter	Single band antenna(in mm)	Patch with spur line
Length of patch (L)	38	38
Width of patch(W)	28	28
Resonate frequency(F_r)	1.89 GHz	28
Length & Width of slots	NA	11.5 & 1 mm
Length & Width of spur line in mm	--	21.5 & 2 mm

Antenna design: - The designed patch shapes are shown in Fig. 1. First, a coaxially fed rectangular patch antenna is designed on a 1.6 mm high FR4 substrate. Two slits are then cut on one side of the patch, followed by the single and double branch lines.

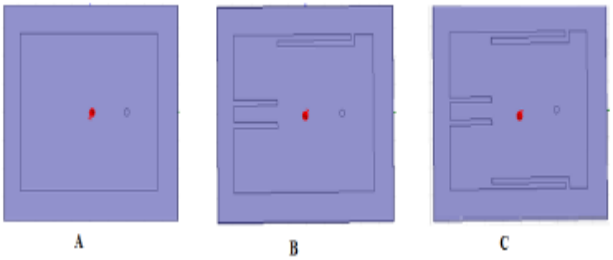


Figure 1: A) Rectangular antenna array B) Patch with a single derived line C) Patch with double derived lines.

To explain the role of spur lines in multiband antennas, the surface current density of the antennas is drawn. Since the current flows in several ways with the impression of the derivation lines, several resonance bands are formed . Figure 2 shows the comparison of the electric field and the antenna field.

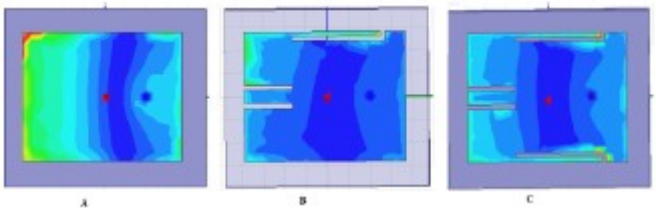


Figure 2: - Electric fields of A) Rectangular antenna field B) Patch with a single derived line C) Patch with double derived lines.

3. SIMULATED RESULTS

In the simulated results, the antennas are designed in HFSS, which solves the antenna network equations based on the method of the moment. Various parameters such as return loss, standing wave ratio and antenna polar graphs are compared. 3 shows the comparison of the antenna parameter S11 with green lines showing the antenna without a branch line, blue with a single line and red with two branch lines.

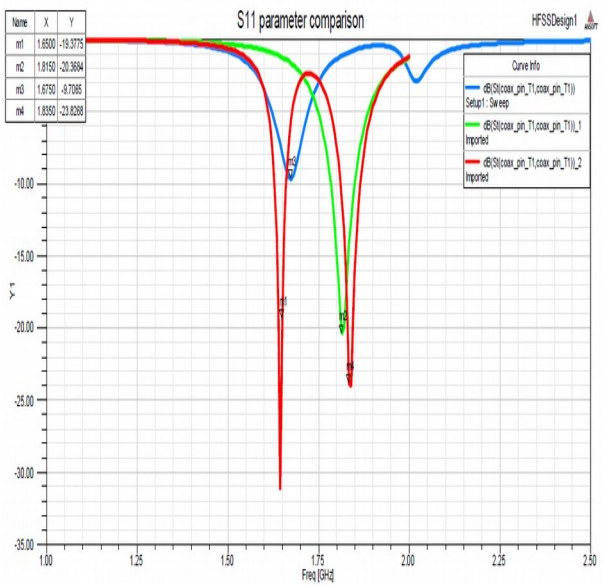


Figure 3: - Comparison of the S11 parameters of the antenna.

Another parameter that shows the matching of the antenna impedance is the polar diagram. Figure 4 shows the comparison of the polar diagrams of the three simulated antennas.

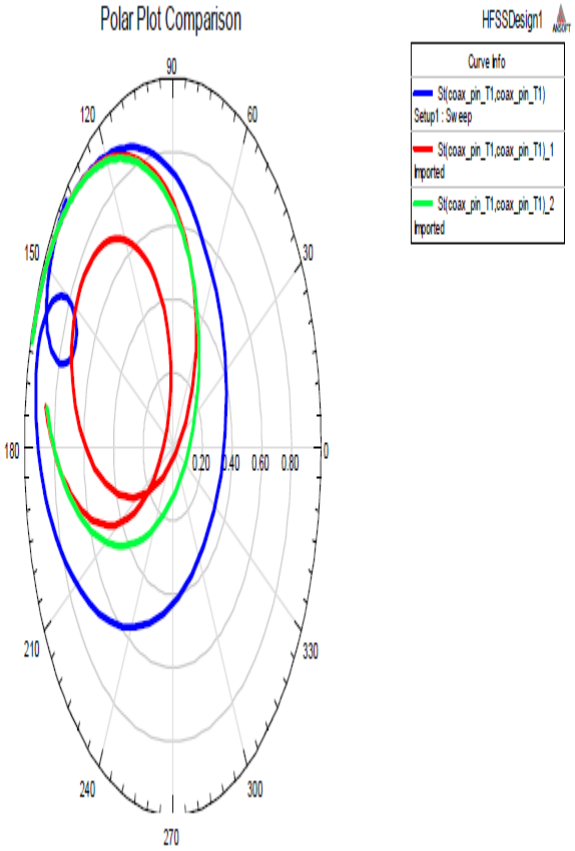


Figure 4: - Comparison of the designed antenna pole patterns.

In addition to the investigation of the radiation behavior, radiation patterns are compared by antennas. The antennas emit half in the microstrip due to the presence of a perfect electric field with an earthen structure under the substrate. The same is shown in Figure 5.

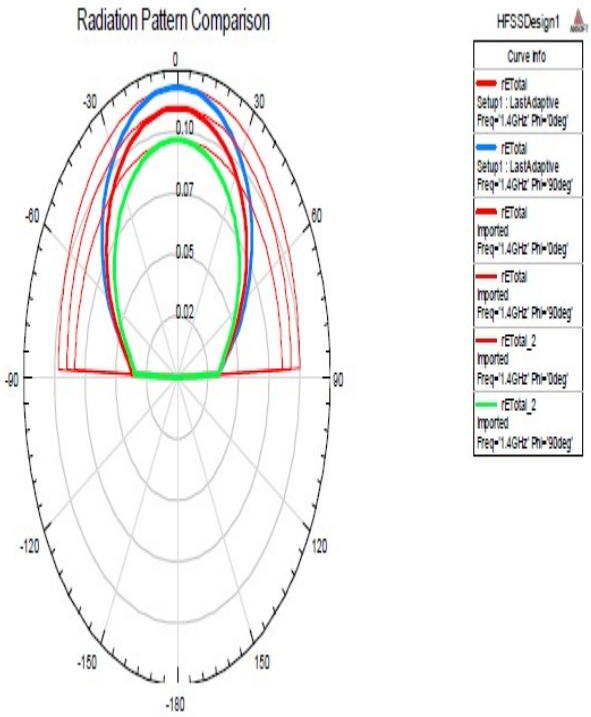


Figure 5: Radiation pattern of the designed antennas.

At the end of the article, all parameters of the designed antennas are compared in the form of Table II.

Table II: Comparison of the antenna parameters.

Antenna Parameter	Without spur lines	With One spur line	Two Spur lines
S11 parameter	-20.3684 @ 1.81GHz	-9.7065 @1.67 GHz	-19.377 @ 1.65 GHz and -23.8268 @ 1.8350 GHz
VSWR	1.9	3.26	1.5 & 1.3
Gain (in dB)	4.2	5.2	4.9

As shown in the graph and table, the VSWRs of the antennas are within the prescribed limits. In addition, the gain is sufficient to cope with L-band applications , however techniques are available to improve the antenna gain.

4. CONCLUSION

1. In this article, the multiband antenna is proposed by changing the shapes of the patch. The shape can be changed using grooves and a contour line. It can be seen that the antenna return loss at

the L-band frequency is less than 10 dB. Also, the VSWR is less than 2 and the gain is around 5 dB. Therefore, the antenna can be used in the L-band.

2. 5. REFERENCES
3. Md. Saad-Bin-Alam and Sanjida Moury, —Multiple-Band Antenna oupled Rectifier Circuit for Ambient RF Energy Harvesting for WSN‖, 3rd International conference on Informatics, Electronics & vision 2014.
4. F. Khodaei, J. Nourinia, and C. Ghobadi (2008), „A Practical Miniaturized U-slot Patch Antenna with Enhanced Bandwidth", Progress in Electromag. Research B, Vol. 3, pp. 47–62.
5. Kundukulam, S.O., Paulson, M., Aanandan, C.K., 2001. Slot-loaded compact microstrip antenna for dual frequency operation. Microwaveand Optical Technology Letters 31 (5).
6. Kwak, W., S. O. Park, and J. S. Kim, \A folded planar inverted-F antenna for GSM/DCS/bluetooth Triple-band application," IEEE Antennas and Wireless Propagation Letters, Vol. 5, 18{21, 2006.
7. Wong, K. L., Compact and Broadband Microstrip Antennas, 1st Edition, John Wiley & Sons, Inc., 2002.
8. Sai Hoi Wong, Wing Chi Mok, Kwai Man Luk, and Kai Fong Lee (2013), „Single-Layer Single-Patch Dual-Band and Triple-Band patch antennas", IEEE Transactions on Antennas and Propagation, Vol. 61, No. 8, pp. 4341–4344.

Most portable wireless communication devices require more than one frequency band to be covered in order to support more wireless applications. For example, a mobile telephone antenna may be required to provide wireless access services for WLAN (2.45 GHz) and PCS (2.2 GHz) to provide. If the antenna is to cover the WiMAX band (3.3 - 3.7 GHz) , a tri-band antenna is required. However, the microstrip antenna has a narrow bandwidth and operates on a single frequency. Therefore, these antennas have to be modified so that a multi-band antenna with sufficient bandwidth is obtained.

Recently, multiband patch antennas have been developed and analyzed to cover various wireless communication services such as GSM, DCS, CDMA and PCS [2, 3 4]. Thus a single antenna covers these bands must it be a trade multiband. The solution to the problem is to use techniques such as probe compensation (L-shaped probe, capacitive "cylinder" on the probe), parasitic patches, direct coupled patches, groove-loaded patches, and grooves (U-groove, V-shaped) and grooves -Patch, U-shaped groove), stacked patches, scatter band patch and the use of electromagnetic band structures (EBG) [4-10] Most of these methods require complex feeding techniques and complex structures such as overlaying and parasite structures.

To avoid the expected disadvantages, a simple antenna with branch lines on both resonance sides of the patch is offered. First, Ansoft HFSS designs and simulates a rectangular patch antenna with a simple coaxial feed. Then two leads are removed from the patch. This article compares the simulated antenna results. In addition, the production of the derivative lines is very easy to carry out, since no special tools for printing are required for the production steps.

2. PROPOSED ANTENNA SYSTEM

In the proposed antenna, a rectangular spot is designed on the FR4 substrate. This patch is then removed with single and double bypass lines. However, the dimensions of the antenna fed by a coaxial cable are calculated from its design equations.

Design equations: The dimensions of the rectangular patch antenna are calculated using the following design equations [2].

$$W = \frac{c}{2fr}\sqrt{\frac{2}{\epsilon r+1}} \qquad \text{--- (1)}$$

For the given operating frequency and dielectric constant, the width of the patch antenna can be calculated by equation 1.

Furthermore, the effective dielectric constant is calculated by equation 2 [2].

$$\epsilon reff = \frac{\epsilon r+1}{2} + \frac{\epsilon r-1}{2}\left[1+12\frac{h}{W}\right]^{-.5} \quad \text{--- (}$$

Due to the edge effect, the effective length of the patch is increased. This is calculated by equation 3.

$$\Delta L = 0.412h\frac{(\epsilon reff+0.3)\left(\frac{W}{h}+0.264\right)}{(\epsilon reff-0.258)\left(\frac{W}{h}+0.8\right)} \quad \text{--- (3)}$$

Now the net length of the patch is calculated according to the formula

$$Leff = L + 2\Delta L \quad \text{--- (4)}$$

Table 1 shows the various dimensions that were calculated and taken for the single band antenna design.

Table 1: Calculated dimensions of the patch antenna

Parameter	Single band antenna(in mm)	Patch with spur line
Length of patch (L)	38	38
Width of patch(W)	28	28
Resonate frequency(F_r)	1.89 GHz	28
Length & Width of slots	NA	11.5 & 1 mm
Length & Width of spur line in mm	--	21.5 & 2 mm

Antenna design: - The designed patch shapes are shown in Fig. 1. First, a coaxially fed rectangular patch antenna is designed on a 1.6 mm high FR4 substrate. Two slits are then cut on one side of the patch, followed by the single and double branch lines.

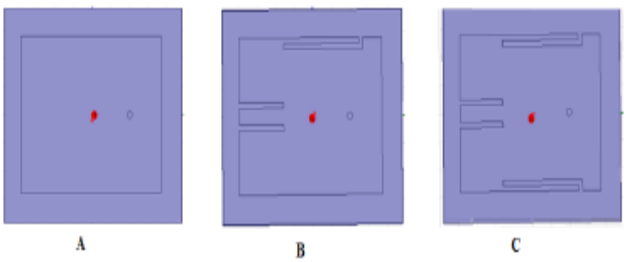


Figure 1: A) Rectangular antenna array B) Patch with a single derived line C) Patch with double derived lines.

To explain the role of spur lines in multiband antennas, the surface current density of the antennas is drawn. Since the current flows in several ways with the impression of the derivation lines, several resonance bands are formed . Figure 2 shows the comparison of the electric field and the antenna field.

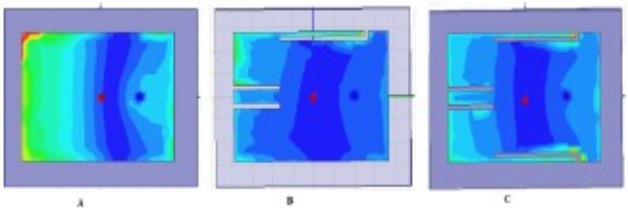


Figure 2: - Electric fields of A) Rectangular antenna field B) Patch with a single derived line C) Patch with double derived lines.

3. SIMULATED RESULTS

In the simulated results, the antennas are designed in HFSS, which solves the antenna network equations based on the method of the moment. Various parameters such as return loss, standing wave ratio and antenna polar graphs are compared. 3 shows the comparison of the antenna parameter S11 with green lines showing the antenna without a branch line, blue with a single line and red with two branch lines.

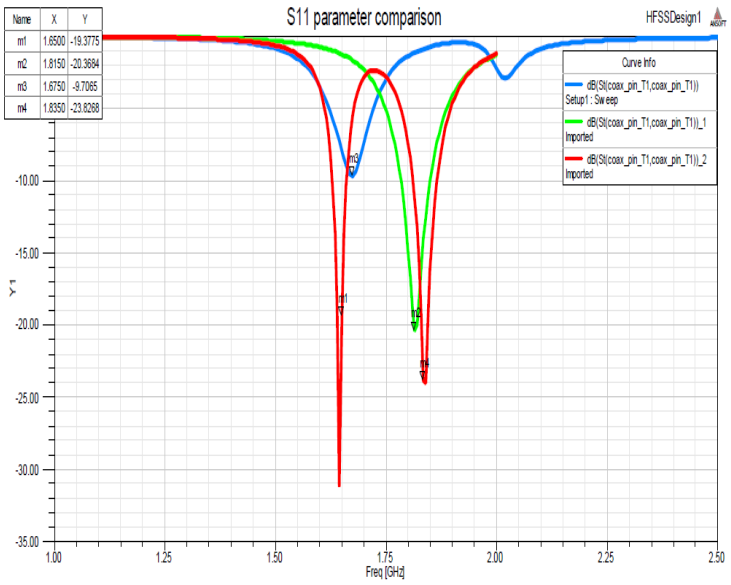


Figure 3: - Comparison of the S11 parameters of the antenna.

Another parameter that shows the matching of the antenna impedance is the polar diagram. Figure 4 shows the comparison of the polar diagrams of the three simulated antennas.

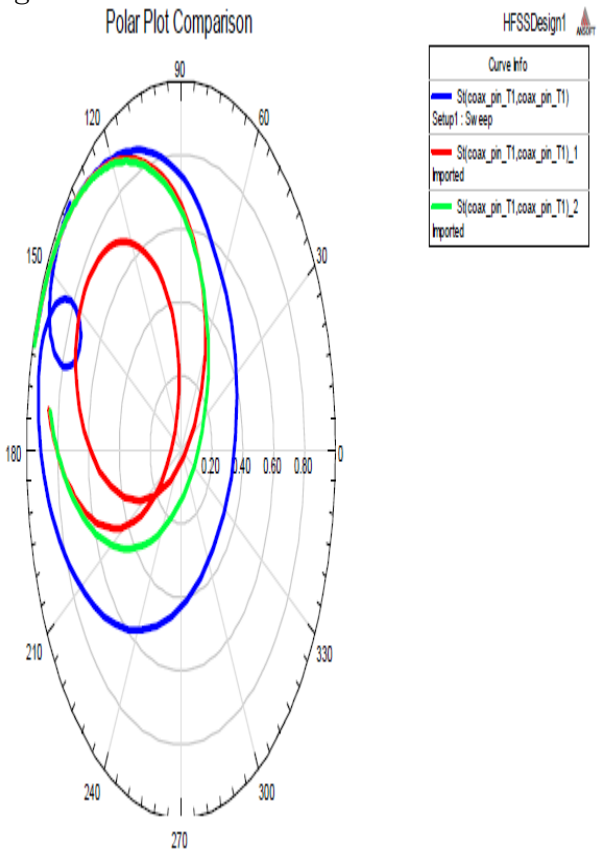


Figure 4: - Comparison of the designed antenna pole patterns.

In addition to the investigation of the radiation behavior, radiation patterns are compared by antennas. The antennas emit half in the microstrip due to the presence of a perfect electric field with an earthen structure under the substrate. The same is shown in Figure 5.

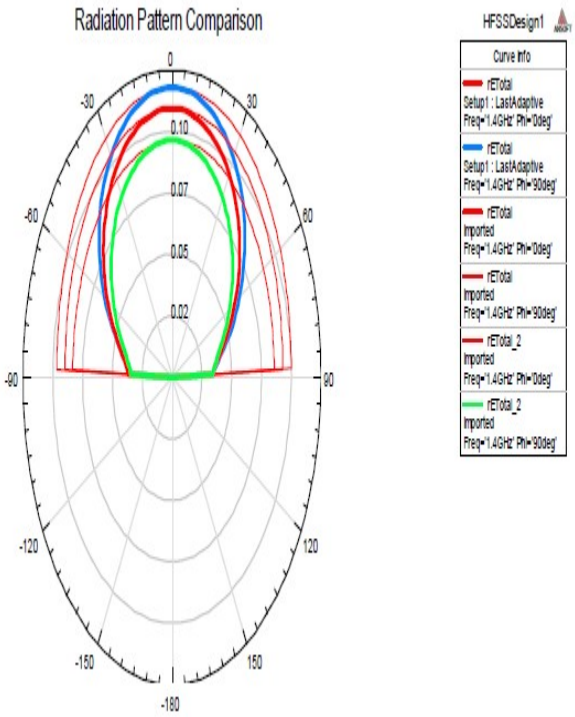


Figure 5: Radiation pattern of the designed antennas.

At the end of the article, all parameters of the designed antennas are compared in the form of Table II.

Table II: Comparison of the antenna parameters.

Antenna Parameter	Without spur lines	With One spur line	Two Spur lines
S11 parameter	-20.3684 @ 1.81GHz	-9.7065 @1.67 GHz	-19.377 @ 1.65 GHz and -23.8268 @ 1.8350 GHz
VSWR	1.9	3.26	1.5 & 1.3
Gain (in dB)	4.2	5.2	4.9

As shown in the graph and table, the VSWRs of the antennas are within the prescribed limits. In addition, the gain is sufficient to cope with L-band applications , however techniques are available to improve the antenna gain.

4. CONCLUSION

1. In this article, the multiband antenna is proposed by changing the shapes of the patch. The shape can be changed using grooves and a contour line. It can be seen that the antenna return loss at

the L-band frequency is less than 10 dB. Also, the VSWR is less than 2 and the gain is around 5 dB. Therefore, the antenna can be used in the L-band.

2. 5. REFERENCES
3. Md. Saad-Bin-Alam and Sanjida Moury, —Multiple-Band Antenna oupled Rectifier Circuit for Ambient RF Energy Harvesting for WSN‖, 3rd International conference on Informatics, Electronics & vision 2014.
4. F. Khodaei, J. Nourinia, and C. Ghobadi (2008), „A Practical Miniaturized U-slot Patch Antenna with Enhanced Bandwidth", Progress in Electromag. Research B, Vol. 3, pp. 47–62.
5. Kundukulam, S.O., Paulson, M., Aanandan, C.K., 2001. Slot-loaded compact microstrip antenna for dual frequency operation. Microwaveand Optical Technology Letters 31 (5).
6. Kwak, W., S. O. Park, and J. S. Kim, \A folded planar inverted-F antenna for GSM/DCS/bluetooth Triple-band application," IEEE Antennas and Wireless Propagation Letters, Vol. 5, 18{21, 2006.
7. Wong, K. L., Compact and Broadband Microstrip Antennas, 1st Edition, John Wiley & Sons, Inc., 2002.
8. Sai Hoi Wong, Wing Chi Mok, Kwai Man Luk, and Kai Fong Lee (2013), „Single-Layer Single-Patch Dual-Band and Triple-Band patch antennas", IEEE Transactions on Antennas and Propagation, Vol. 61, No. 8, pp. 4341–4344.

Most portable wireless communication devices require more than one frequency band to be covered in order to support more wireless applications. For example, a mobile telephone antenna may be required to provide wireless access services for WLAN (2.45 GHz) and PCS (2.2 GHz) to provide. If the antenna is to cover the WiMAX band (3.3 - 3.7 GHz) , a tri-band antenna is required. However, the microstrip antenna has a narrow bandwidth and operates on a single frequency. Therefore, these antennas have to be modified so that a multi-band antenna with sufficient bandwidth is obtained.

Recently, multiband patch antennas have been developed and analyzed to cover various wireless communication services such as GSM, DCS, CDMA and PCS [2, 3 4]. Thus a single antenna covers these bands must it be a trade multiband. The solution to the problem is to use techniques such as probe compensation (L-shaped probe, capacitive "cylinder" on the probe), parasitic patches, direct coupled patches, groove-loaded patches, and grooves (U-groove, V-shaped) and grooves -Patch, U-shaped groove), stacked patches, scatter band patch and the use of electromagnetic band structures (EBG) [4-10] Most of these methods require complex feeding techniques and complex structures such as overlaying and parasite structures.

To avoid the expected disadvantages, a simple antenna with branch lines on both resonance sides of the patch is offered. First, Ansoft HFSS designs and simulates a rectangular patch antenna with a simple coaxial feed. Then two leads are removed from the patch. This article compares the simulated antenna results. In addition, the production of the derivative lines is very easy to carry out, since no special tools for printing are required for the production steps.

2. PROPOSED ANTENNA SYSTEM

In the proposed antenna, a rectangular spot is designed on the FR4 substrate. This patch is then removed with single and double bypass lines. However, the dimensions of the antenna fed by a coaxial cable are calculated from its design equations.

Design equations: The dimensions of the rectangular patch antenna are calculated using the following design equations [2].

$$W = \frac{c}{2fr}\sqrt{\frac{2}{\epsilon r+1}} \qquad \text{--- (1)}$$

For the given operating frequency and dielectric constant, the width of the patch antenna can be calculated by equation 1.

Furthermore, the effective dielectric constant is calculated by equation 2 [2].

$$\epsilon reff = \frac{\epsilon r+1}{2} + \frac{\epsilon r-1}{2}\left[1+12\frac{h}{W}\right]^{-.5} \quad \text{--- (2)}$$

Due to the edge effect, the effective length of the patch is increased. This is calculated by equation 3.

$$\Delta L = 0.412h\frac{(\epsilon reff+0.3)\left(\frac{W}{h}+0.264\right)}{(\epsilon reff-0.258)\left(\frac{W}{h}+0.8\right)} \quad \text{--- (3)}$$

Now the net length of the patch is calculated according to the formula

$$Leff = L + 2\Delta L \quad \text{--- (4)}$$

Table 1 shows the various dimensions that were calculated and taken for the single band antenna design.

Table 1: Calculated dimensions of the patch antenna

Parameter	Single band antenna(in mm)	Patch with spur line
Length of patch (L)	38	38
Width of patch(W)	28	28
Resonate frequency(F_r)	1.89 GHz	28
Length & Width of slots	NA	11.5 & 1 mm
Length & Width of spur line in mm	--	21.5 & 2 mm

Antenna design: - The designed patch shapes are shown in Fig. 1. First, a coaxially fed rectangular patch antenna is designed on a 1.6 mm high FR4 substrate. Two slits are then cut on one side of the patch, followed by the single and double branch lines.

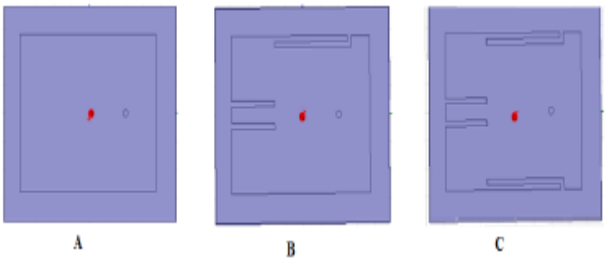


Figure 1: A) Rectangular antenna array B) Patch with a single derived line C) Patch with double derived lines.

To explain the role of spur lines in multiband antennas, the surface current density of the antennas is drawn. Since the current flows in several ways with the impression of the derivation lines, several resonance bands are formed . Figure 2 shows the comparison of the electric field and the antenna field.

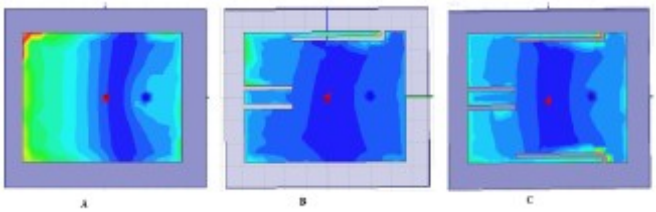


Figure 2: - Electric fields of A) Rectangular antenna field B) Patch with a single derived line C) Patch with double derived lines.

3. SIMULATED RESULTS

In the simulated results, the antennas are designed in HFSS, which solves the antenna network equations based on the method of the moment. Various parameters such as return loss, standing wave ratio and antenna polar graphs are compared. 3 shows the comparison of the antenna parameter S11 with green lines showing the antenna without a branch line, blue with a single line and red with two branch lines.

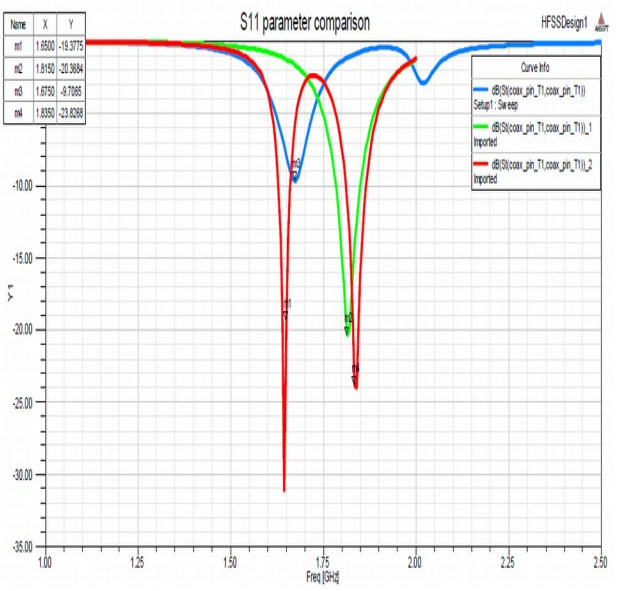


Figure 3: - Comparison of the S11 parameters of the antenna.

Another parameter that shows the matching of the antenna impedance is the polar diagram. Figure 4 shows the comparison of the polar diagrams of the three simulated antennas.

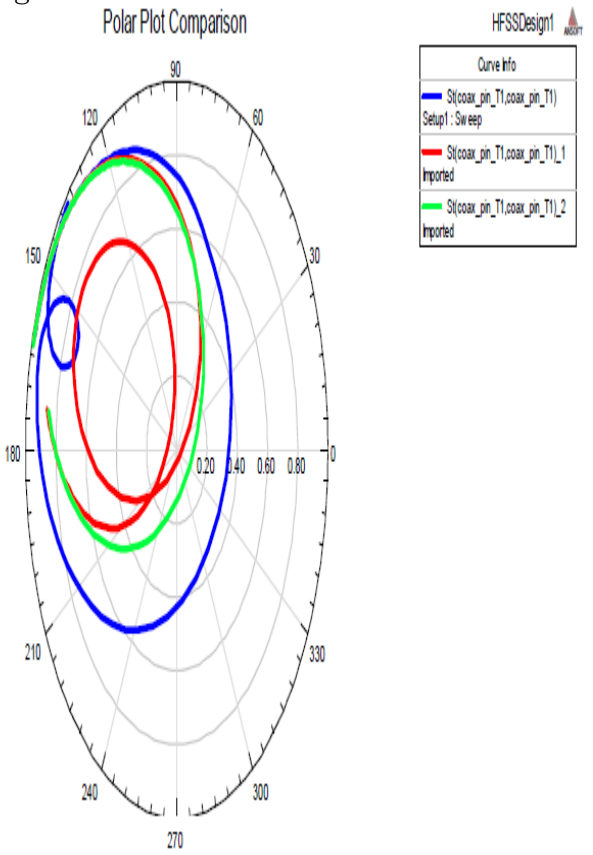


Figure 4: - Comparison of the designed antenna pole patterns.

In addition to the investigation of the radiation behavior, radiation patterns are compared by antennas. The antennas emit half in the microstrip due to the presence of a perfect electric field with an earthen structure under the substrate. The same is shown in Figure 5.

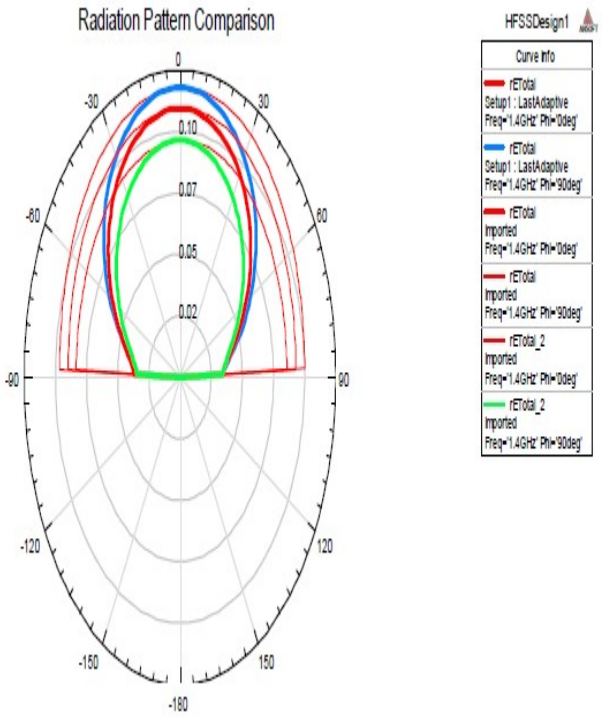


Figure 5: Radiation pattern of the designed antennas.

At the end of the article, all parameters of the designed antennas are compared in the form of Table II.

Table II: Comparison of the antenna parameters.

Antenna Parameter	Without spur lines	With One spur line	Two Spur lines
S11 parameter	-20.3684 @ 1.81GHz	-9.7065 @1.67 GHz	-19.377 @ 1.65 GHz and -23.8268 @ 1.8350 GHz
VSWR	1.9	3.26	1.5 & 1.3
Gain (in dB)	4.2	5.2	4.9

As shown in the graph and table, the VSWRs of the antennas are within the prescribed limits. In addition, the gain is sufficient to cope with L-band applications , however techniques are available to improve the antenna gain.

4. CONCLUSION

1. In this article, the multiband antenna is proposed by changing the shapes of the patch. The shape can be changed using grooves and a contour line. It can be seen that the antenna return loss at

the L-band frequency is less than 10 dB. Also, the VSWR is less than 2 and the gain is around 5 dB. Therefore, the antenna can be used in the L-band.

2. 5. REFERENCES

3. Md. Saad-Bin-Alam and Sanjida Moury, —Multiple-Band Antenna oupled Rectifier Circuit for Ambient RF Energy Harvesting for WSN‖, 3rd International conference on Informatics, Electronics & vision 2014.
4. F. Khodaei, J. Nourinia, and C. Ghobadi (2008), „A Practical Miniaturized U-slot Patch Antenna with Enhanced Bandwidth“, Progress in Electromag. Research B, Vol. 3, pp. 47–62.
5. Kundukulam, S.O., Paulson, M., Aanandan, C.K., 2001. Slot-loaded compact microstrip antenna for dual frequency operation. Microwaveand Optical Technology Letters 31 (5).
6. Kwak, W., S. O. Park, and J. S. Kim, \A folded planar inverted-F antenna for GSM/DCS/bluetooth Triple-band application," IEEE Antennas and Wireless Propagation Letters, Vol. 5, 18{21, 2006.
7. Wong, K. L., Compact and Broadband Microstrip Antennas, 1st Edition, John Wiley & Sons, Inc., 2002.
8. Sai Hoi Wong, Wing Chi Mok, Kwai Man Luk, and Kai Fong Lee (2013), „Single-Layer Single-Patch Dual-Band and Triple-Band patch antennas“, IEEE Transactions on Antennas and Propagation, Vol. 61, No. 8, pp. 4341–4344.

MULTI SENSOR DATA ACQUISITION IN HEALTH DIAGNOSIS BASED ON SELF-LEARNING SYSTEM AND THING SPEAK SERVER

Dr. I. Selvamani[1]., A.Prathusha[2]., V.Varshini[3].., B.Anitha[4]., S.Shravani[5].,

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: i.selvamani@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0463, 17RG1A04B5, 17RG1A0469, 17RG1A04A3), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Predicting heart disease is a critical issue for humans today. In the first case, heart disease cannot be identified until it occurs. This article describes the work of the self-learning system for monitoring cardiac activity using ANFIS. Here, heart disease can be understood after reaching an abnormal state or at any stage of fall detection. This article develops a method for classifying the degree of heart disease in patients with ANFIS. The neural network predicts the target level and the fuzzy logic compares the target level with the current inputs and optimizes it. The IoT plays an important role here. The predicted and optimized heart disease data is sent to the server for continuous information and every 10 seconds. In this way, the early stages of heart disease can be identified and recovered, and current problems and future directions can also be identified.

Keywords— EKG, pulse oximeter, Arduino UNO, Thing Speak server.

1. INTRODUCTION

Heart disease occurs mainly due to blockage of the blood vessels. It includes coronary artery disease, myocardial infarction, and tachycardia. It can be due to high blood pressure, obesity, smoking, and poor diet. High blood pressure causes 13% of deaths from CVD, tobacco in 9%, robustness in 5% and diabetes in 6%. Coronary artery disease can be prevented if it is predicted earlier. The human-machine interaction system is an investigation of the relationship between people and information transmitted by computers. The future of the human-machine interaction system lies in how these systems can intelligently take into account the context of the user as areas of application, social organization and work. Researchers have made steady progress in recognizing people's daily activities, but little attention has been paid to recognizing common activities and movements in a given activity.

1.1 EXISTING APPROACH

In the existing system, the health system was used to monitor the physiological signal and current position of a patient using the machine learning function. The medical box was used for the automatic detection of ECG signals and patient position. The EKG acquisition module detects the signal and transmits it to the health center. The position of the patient can be recognized by an external precision GPS. Through the health center, doctors can help with the detailed health status of a patient when the patient reaches or falls into the abnormal stage. This notification to save her is sent to the health officer. The health chart continuously records the condition of the EKG signal. Once the abnormal stage is reached, an emergency notification will be sent to the affected doctors and family members. It has some drawbacks such as remote patient monitoring, disease prediction is not possible, high cost. 2.

3. PROPOSED SYSTEM

Proposed system Neuro-fuzzy and Arduino-based health diagnoses are used as a gateway for communication with the various sensors such as ECG sensor, temperature sensor and pulse oximeter sensor. The microcontroller collects the data from the sensor and sends it to the network via WLAN. In this way, doctors can monitor health parameters in real time. First, the ANFIS algorithm is converted into embedded C code and uploaded to the microcontroller. In general, ANFIS consists of two parts: a) Training b) Testing. In the training part, the target level is defined by transferring input data to the data record of the LVM file. During the test, the clinical input data from the patient's body is compared to the target values. The doctor can access the data at any time. The remote monitoring system is that the data is securely transmitted to the destination end and only the authorized user should be allowed access to the data. The user / doctor can access the data by logging

into the HTML website. At the time of the member's situation, in order to prevent the patient from suffering from any abnormal situation, a Twitter alert will be sent to the doctor through the ThingSpeak (Internet of Things) server connected to the controller. Mobile application software (ThingsView) is also provided to continuously check a patient's health via a mobile phone.

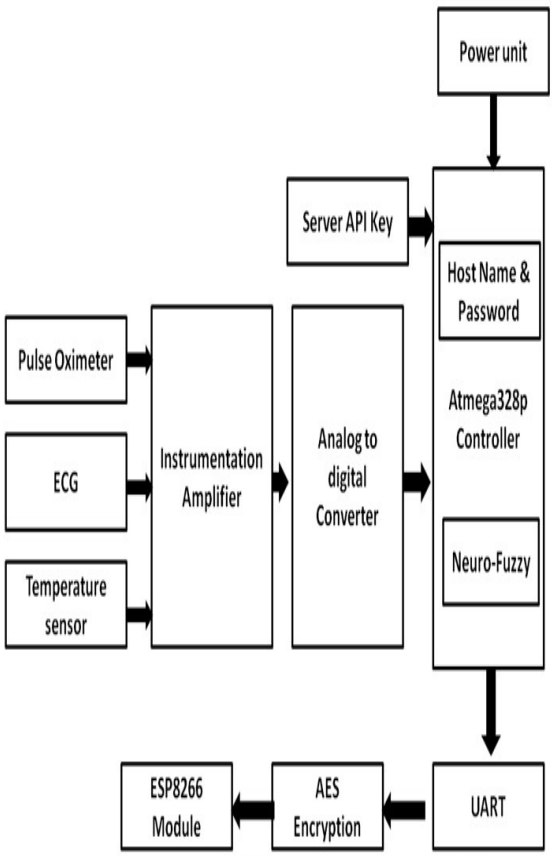


Fig. -1: Function diagram

4. DESCRIPTION OF THE BLOCK DIAGRAM

1. INPUTS

Pulse oximeter

The pulse oximeter shows the strength of the blood and measures the oxygen content of the blood. It has an infrared emitter and a photodetector that shows the oxygen flow as 0 and 1. The "1" is assumed to be 1023 due to the use of a 10-bit ADC.

EKG

In this case, a three-electrode EKG is used. One electrode is on the left arm and one electrode is on the right arm and the other is used as a reference electrode. The electrodes on the left and right arms determine the heart rate.

Temperature sensor

It records the patient's body temperature.

2. Instrument amplifiers

The sensor values are given at the input of the KI. It consists of two parts: a) amplifier b) filter. The filter removes the unusable signals , the amplifier amplifies the filtered sensor values.

3 ADC

The amplified analog signal is converted into a digital signal by the ADC. The output is represented by zeros and ones that are fed to the microcontroller.

4 ESP8266

It's a WiFi module. It has a more robust operating system that it is installed on (OS). Putty software is used to check the network connection of the ESP8266.

5 Thing Speak Server

It is a free server that is used for publishing data and continuously monitoring health values. For this purpose, each person has a separate username and password to log in.

5. METHDOLOGY USED AND RESULT

It refers to the adaptive inference system Neuro Fuzzy. The neural network has the ability to learn, such as supervised and unsupervised learning. This article describes backward propagation in supervised learning. Back propagation primarily uses multilayer perceptrons, including input, hidden, and output layers. This algorithm uses a calculated output error to change the weight values in the opposite direction.

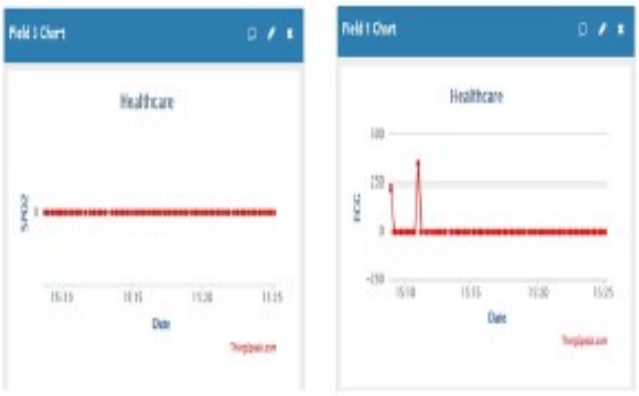


Fig 2: pulse oximeter, ECG sensor

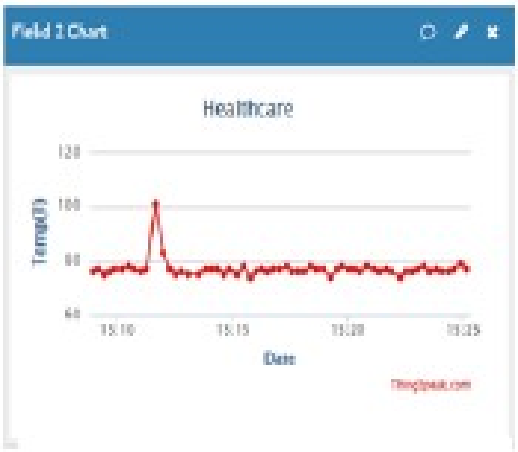


Fig 3: Temperature Sensor

4.3 Snapshot

Fig 4: Hardware Prototypr

6. CONCLUSION

Heart disease plays an important role in human life today due to changes in lifestyle. This self- earning system design for diagnosing health parameters using ANFIS will predict heart diseases before they seriously affect humans. This device has been properly designed and tested.

REFERENCES

1. An Inductorless Self-Controlled Rectifier for Piezoelectric Energy Harvesting by Shaohua Lu and FaridBoussaid from University of Western Australia 2015.
2. G. Virone, A. Wood, may 2011, “Advanced wireless network for health monitoring system”.
3. “Innovative approach for wireless health monitoring system using client-server architecture” Ms. Poonam Agrawal ,Prof. S. P. Hingway,jun 2013.
4. Damjanovic, Dragan (1998). "Ferroelectric, dielectric and piezoelectric Properties of ferroelectric thin films and ceramics" .
5. J. Lauardini, Heat Transfer in Cold Climates (Van Nostrand, New York).
6. T.R. Goodman, The heat balance integral and its application in problems involving a change. J. Sol. Energy Eng. Trans.

SEAMLESS INTEGRATION OF MULTIPLE ANTENNAS IN MOBILE COMMUNICATION SYSTEMS USING MIMO-LTE SYSTEM FOR HIGH SPEED COMMUNICATION

S. Swetha[1]., B.Sanjana[2]., A.Vaishnavi[3]., D.Tejaswini[4]., R.Navya[5].,

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: swethasara83@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0470, 17RG1A0467, 17RG1A0477, 17RG1A0499), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The suggestion of this article is to appreciate the 3GPP LTE, representative of the 4G radio system. LTE is a newer high-speed wireless communication technology that promises higher data speeds, higher bandwidth, security and more productive use of the wireless spectrum. An intuitive way to improve overall performance on both the sender and receiver side is to use diversity. The diversity-based beam forming approach uses multi-transceiver RF systems, which may increase the strength of the received signal and enable higher data rates. The core of this proposal is an LTE-MIMO system. MIMO (Multiple Antenna System) technology is used in the LTE standard for performance parameters, including higher radio access data rates, improved system capacity, significant increase in spectral efficiency, support of sockets for multiple antennas and seamless integration into existing mobile communication systems. This proposal promises a good quality signal with high data rates..

Keywords— 3GPP, LTE, MIMO, UMTS, HSDPA.

1. INTRODUCTION

The growth of data-intensive mobile applications and services has led to the expansion of the next generation of high-speed wireless standards to provide the data speeds and network capacities required for the global delivery of multimedia applications. In 1997 the goals declared by the ITU IMT-2000 (International Telecommunications Union International Mobile Telecommunication) were implemented. Various wireless standards such as UMTS, HSDPA, HSUPA, HSPA + (MIMO) have been developed. The HSPA + standard can achieve speeds of 84 Mbit / s and the use of an even higher modulation scheme (64QAM).

2. MULTIPLE ANTENNA SYSTEM

The multiple antenna system uses multiple TxN antennas / multiple RxN antennas . With this system, it is possible to establish high-speed wireless communication that offers extended data rates and a low error rate. Several antenna systems are SISO, SIMO, MISO and MIMO [10-11, 17].

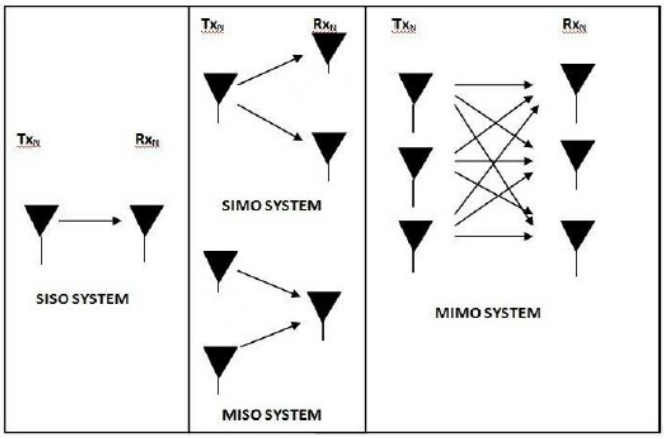


Fig. 1: Several antenna systems (SISO, SIMO, MISO, MIMO).

2.1 SISO (conventional radio system)

Conventional radio transmission systems use a single antenna for transmitting and one antenna for receiving [1]. In the MIMO diction, the system is referred to as the SISO system (single input, single output) (Fig. 1). Channel capacity is the maximum transmission capacity that can be achieved on a given channel by any combination of any coding, transmission, or decoding scheme. The capacity of channel C of this system is given by:

$$C_{SISO} = B * \log_2(1 + S/N) bit/\sec \quad (1)$$

C is the capacity, B (in Hz) the channel bandwidth, S (in watts) the power of the output signal and N (in watts) the power of the output noise. Implementing SISO is relatively easy and inexpensive. It is used for broadcasting television, radio, and personal wireless technologies such as Wi-Fi and Bluetooth.

2.2 SIMO

In the term MIMO, a system in which the number of receiving antennas is greater than the TxN antenna system [2] is referred to as SIMO (single output with several inputs), also referred to as receiving diversity (Fig. 1). The simplest case is the Tx1 Rx2 antenna. Multiple receiving antennas can help us get a stronger signal through diversity. The capacity of the SIMO channel is given by:

$$C_{SIMO} = B * \log_2(1 + {}^{nS}/_{N}) bit / \sec \quad (2)$$

When C is called capacity, B is called bandwidth, S / N is called signal-to-noise ratio, n is the number of antennas used on the receiver side. The implementation is very easy. The signal-to-noise ratio can be improved by using a suitable focus on the receiver.

With the switched diversity or select diversity technique, the receiver selects the best antenna to receive a stronger signal, or it can combine the signals from all antennas to produce the SNR known as the combination ratio technique (SNC) maximize. . CRM is generally good multi-antenna system technology when the signals in a fading channel are of the same strength.

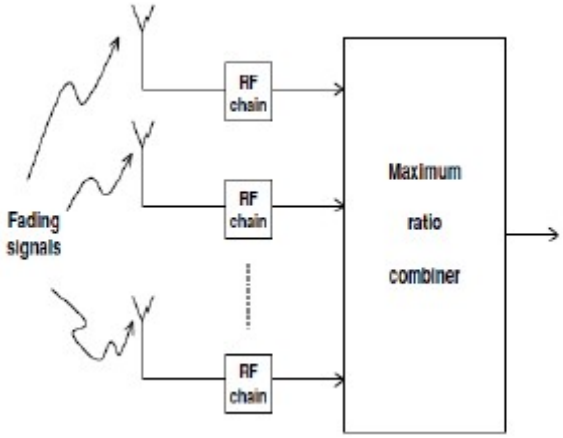


Fig. 2: MRC technology

2.3 MISO

A system in which the number of TxN antennas is greater than the number of RxN antennas is called a MISO system (Single Input Multiple Output), which is also called transmission diversity (Fig. 1). The simplest scenario uses the Tx2-Rx1 antenna (MISO, 2x1).

The redundancy coding is shifted from the mobile UE to the base station, so that this method is advantageous, simpler and cheaper to implement. Alamouti STC (Space-Time Coding), a technique used in the transmitter with two antennas. STCs are used to generate a redundant signal. It allows the message to be sent by sending antennas at different consecutive times, i. H. The replica of the signal sent at different times by different antennas. This type of delayed transmission is called delayed diversity.

$$C_{MISO} = B * \log_2(1 + {}^{nS}/_{N}) bit / \sec \quad (3)$$

Where n = number of transmitting antennas in MISO systems, C = system capacity, B = system bandwidth and S / N = signal-to-noise ratio.

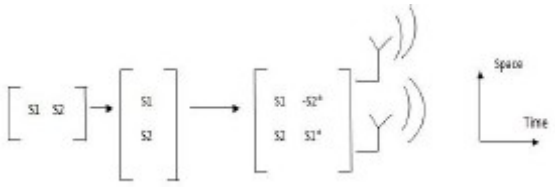


Fig-3: Alamouti Coding

3. GAIN MULTIPLEXION IN SPACE

When using spatial multiplexing, up to a minimum of {TxN, RxN} symbols can generally be transmitted per time slot, with

- TxN: transmitting antenna number
- RxN: Number of receiving antennas

Yes, you can send RxN symbols and receive a diversity win of TxN-RxN + 1 Note that for TxN = RxN , the diversity win will be. On the other hand, the maximum spatial diversity while only one symbol is transmitted per time slot is TxN * RxN. Therefore, the advantage of a MIMO channel can be used in two ways, thereby increasing the variety and number of symbols transmitted by the system. If the transmitting antenna is more than one, there is a theoretical trade-off between the number of transmitter symbols and the diversity of the system (Fig. 4). The capacity of a MIMO channel increases with increasing SNR.

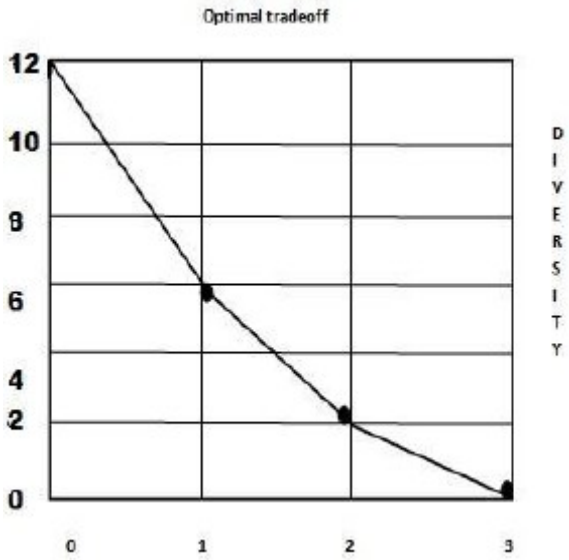


Fig. 3: Optimal balance between spatial multiplex gain (display of throughput) and diversity [4]

4. LONG TERM DEVELOPMENT (LTE)

LTE fulfills the goal of global mobile broadband communication. The goals include improved radio access data rates, improved system capacity and spectral efficiency, reduced operating costs, flexible bandwidth, low latency and support for multiple antennas.

Table 1: Summarizes the maximum data rates for various wireless technologies.

Technology	Theoretical peak data rate (at low mobility)
GSM	9.6 Kbps
IS-95	14.4 Kbps
GPRS	171.2 Kbps
EDGE	473 Kbps
CDMA-2000(1xRTT)	307 Kbps
WCDMA(UMTS)	1.92 Mbps
HSDPA(Rel 5)	14 Mbps
CDMA-2000(1x-EV-DO)	3.1 Mbps
HSPA+(Rel 6)	84 Mbps
WiMAX(802.16e)	26 Mbps
LTE(Rel 8)	300 Mbps
WiMAX(802.16m)	303 Mbps
LTE-Advanced(Rel10)	1 Gbps

4.1 LTE (versions 8 and 9) and LTE-Advanced (version 10)

The LTE standard (3GPP version 8) was published in December 2008. Version 9 arrived in December 2009 [3]. It included features such as support for media streaming / multicast services, location and delivery services for base stations that support multiple standards. LTE-Advanced (released December 2010) is a transformation of the original LTE standard. It includes technologies such as carrier aggregation, enhanced downlink MIMO, uplink MIMO and relays [3]. Table 1 summarizes the maximum data rates for various wireless technologies.

4.2 LTE-MIMO

The integration of many techniques of multi-antenna systems makes it possible to achieve high standards for maximum data rates such as LTE and its advanced standards. MIMO algorithms use two main techniques for multiple antennas, namely transmission diversity, such as SFBC and spatial multiplexing with or without delay diversity coding. In different antennas, the relationship between the TxN and RxN resource elements is expressed by a system of linear equations on each subcarrier. In this system, the multiplication of the vector of the resource elements in the transmitting antennas by the matrix of the MIMO channels will result in the vector of resource elements received in the receiving antennas transmitted.

5. RESULTS OF SURVEY

It was investigated that the capacity and data rates by the use of multiple antenna systems, such as SIMO, MISO, MIMO despite the SISO system be increased can.

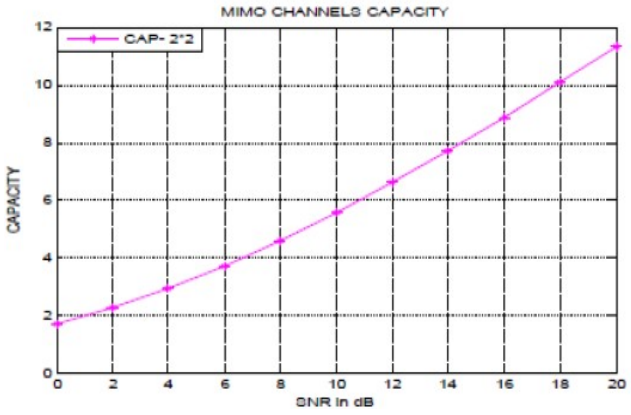


Figure 4 The capacity of the MIMO channel

Figure 4 shows the capacity of the MIMO channel with two transmit antennas and two receive antennas, assuming a Rayleigh fading model. We see that with an SNR of 20 dB, a

capacitance on the order of 11 bits / s / Hz can be achieved.

6. CONCLUSION

This document shows that the increase in data rates and system performance can be achieved by properly designing the MIMO system. The capacity increases linearly when the MIMO system is used at a high SNR, i.e. H. As the TxN and / or RxN of the MIMO system increases, its capacity increases. We introduced Shannon's capacity formula. Various multi-antenna systems are being studied in detail.

REFERENCES

1. Kritika Sengar ,Nishu Rani, Ankita Singhal, Dolly Sharma, Seema Verma, Tanya Singh. Study and Capacity Evaluation of SISO, MISO and MIMO RF Wireless Communication Systems, 1 International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 9 - Mar 2014.
2. S.D. Bhad, A.S. Hiwale, A.A. Ghatol, Bhad. Performance Analysis Of Space Time Trellis Code with receive Antenna selection. In: IEEE fourth International Conference on Wireless Comm. and Sensor Networks, WCSN 2008, pp. 148–152 (December 2008). DOI: 10.1109/WCSN.2008.4772700
3. Sandeep Bhad and A.S. Hiwale. Performance Analysis of MIMO- Space-Time Trellis Code System over Fading Channels. Springer Berlin Heidelberg on Advances in Computing, Communication and Control, 2011.
4. Yamini Devlal, Mrs. Meenakshi Awasthi. Capacity Analysis of MIMO Technology, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 1 January 2015, Page No. 9819-9824.
5. Arif Khan, Rein Vesilo. A Tutorial on SISO and MIMO Channel Capacities, publication/265811248

SEIZURE DETECTION FROM EEG SIGNAL USING DISCRETE WAVELET TRANSFORM IN VERILOG SIMULATOR

Chekuri Mahesh [1]., S.Priyanka[2]., K.Pravalika[3]., S.Sharanya[4]., N.Sadhvika[5]
1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: chekuri20@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A04A2, 17RG1A0486, 17RG1A04A0, 17RG1A0495), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The abnormal electrical activity of a group of brain cells is called a seizure. The electroencephalogram (EEG) is most commonly used to detect seizures. This article presents the study and analysis of statistical features for the detection of seizures from the EEG signal. The discrete waves transform (DWT) is used for the decomposition of sub-bands and the characteristics of the sub - bands selected to be extracted. Variance, standard deviation, maximum amplitude and skewness are the various properties analyzed. There is a significant difference between the characteristic values obtained from the patient's EEG database and the normal individual. Hence, it is possible to detect seizures. The system is checked by Verilog in the ISim simulator.

Keywords— Electroencephalography (EEG), Discrete Wavelet Transform (DWT), Feature Extraction, Seizure, Skewness, Variance, Standard Deviation

1. INTRODUCTION

The brain is one of the most important human organs that serve as the center of the nervous system controlling the coordination of human muscles and nerves. The abnormal electrical activity in a group of brain cells is called a seizure. This seizure can cause a temporary change in how the brain works, leading to a condition known as epilepsy. Around 1% of the world's population suffers from epilepsy [1]. In 50% of people, seizures can be cleared with the use of anti-epileptic drugs. Accurate detection of seizures at the precise point in time is therefore essential. The electroencephalogram (EEG), which measures the electrical activity of the brain, is very important in diagnosing seizures. Long-term EEG recording is required when epileptic seizures are infrequently detected. Detecting seizure activity is therefore a very demanding process that requires detailed analysis of all EEG data. Recognizing seizures that occur in everyday life is important to the safety and well-being of people with seizures and those around them. However, clinical systems require too many resources for outpatients. One of the many challenges of automated seizure detection is to distinguish between seizure activity and non-seizure activity. In order to accomplish this task, the identification of EEG features and their extraction play a key role [2].

2. LITERATURE SURVEY

In 1997, Hao Qu and Jean Gotman proposed the first seizure warning system. It is a patient-specific system and recognizes seizures similar to the pattern [3. Carlos Guerrero- Mosquera and
Angel Navia Vázquez introduced a new approach to feature extraction for the detection of EEG signals. In this work feature extraction was performed using time-frequency distributions (TFD). Three characteristics included in the study are based on the energy, frequency and length of the main track [4]. Adam Page et al. introduced a low power, multi-channel electroencephalography extractor (EEG) and classifier for personalized seizure detection. In this work the properties include the area under the wave, the normalized drop, the line length, the mean amplitude of the peak and the mean amplitude of the valley [2]. Mohamed Bedeeuzzaman.V et al. present a method for automatic detection of attacks by using higher order moments. In this higher order, the statistical properties are calculated from each frame of a predetermined length [5].

3. METHODOLOGY USED

The EEG database of ordinary people and those in crisis is used. Before pre-processing the feature extraction database. The properties are from the selected subband extracted. The system can be simulated in the Verilog ISim simulator. The method used can be summarized in the following figure.

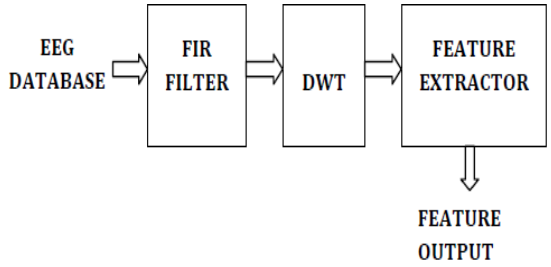


Fig -1: System Block Diagram

3.1 EEG database

The EEG database is provided as input for the system. A publicly accessible database on the Internet [6] [7] was used for this study . Five EEG databases are used by normal people and five by data subjects. The sampling frequency of the data used is 256 Hz. Figure 2 shows an example of an EEG database that is made available to the system.

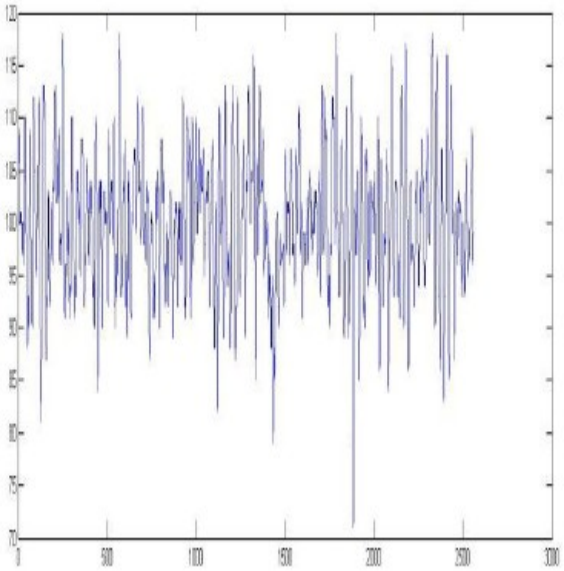


Figure -2: Example of an EEG database entry

3.2 FIR filter (Finite Impulse Response)

The FIR filter is used to remove noise present in the EEG database. Examples of noise present in the EEG are the electrocardiogram (EKG), the electrooculogram (EOG) and the disturbance of the power line. Next, Fig. 3 shows the structure of the FIR filter composed of multiplier adder and delay elements.

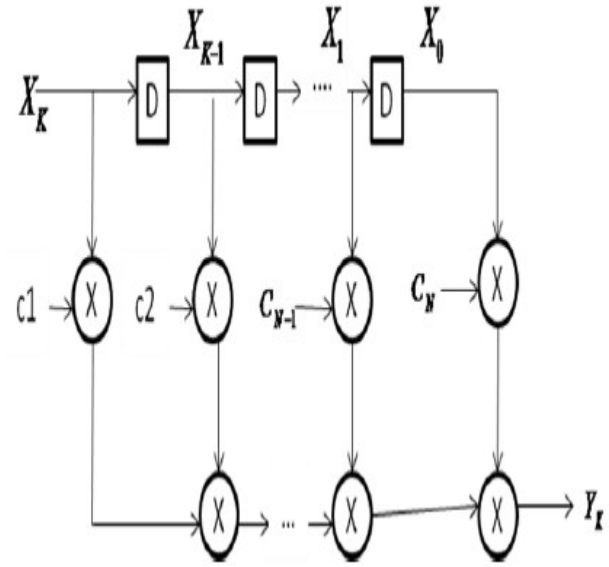


Fig. -3: Structure of the FIR filter

The output is given by the equation

$$Y_K = X_K C_1 + X_{K-1} C_2 + \ldots\ldots X_1 C_N$$

A 64th order FIR filter is used for this study. The filter was developed with the FDA tool in MATLAB and the multiplier with the Baugh Wooley multiplier. The Baugh Wooley multiplier can be effectively used for multiplication signs. Figure 4 shows the structure of the FIR filter in MATLAB with the FDA tool.

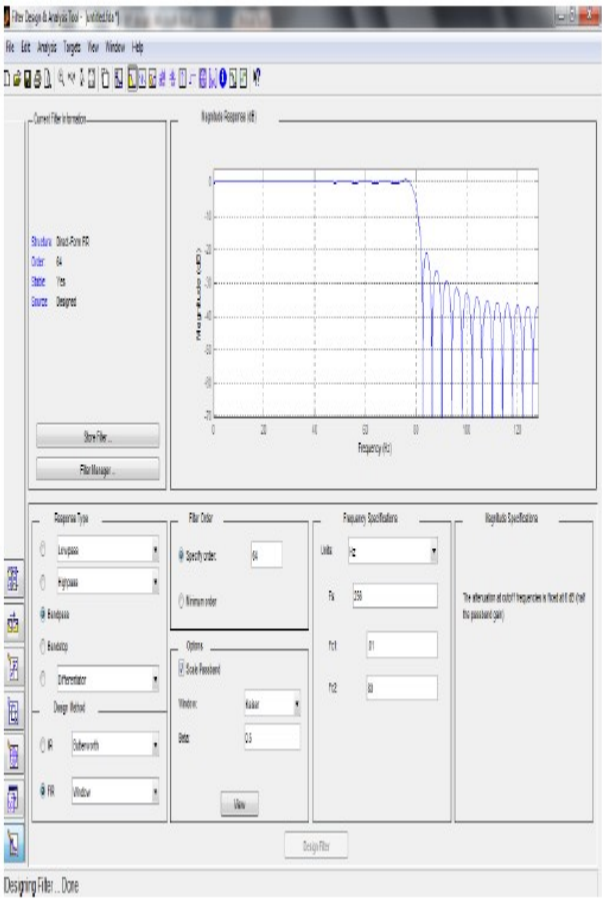


Fig. -4: FIR filter design with the MATLAB FDA tool

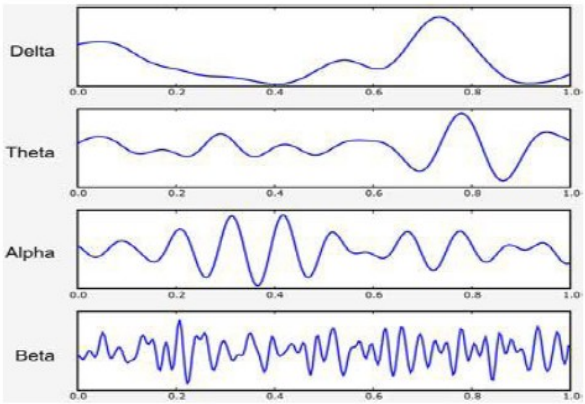
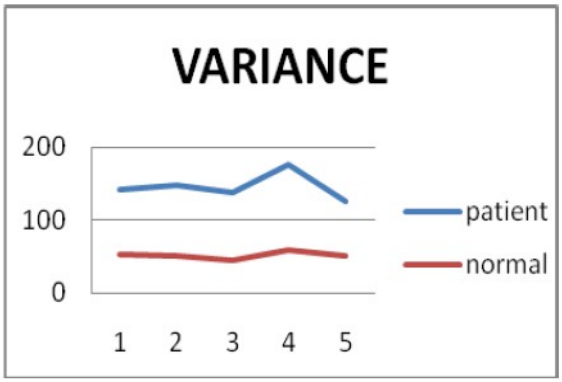


Fig. -5: Brain waves [8]

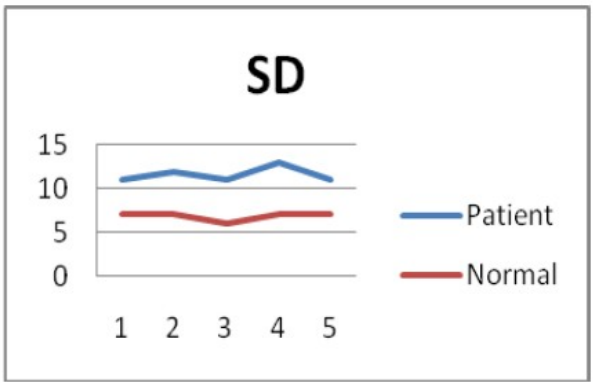
Since the EEG signal is non-stationary in nature , the Fourier transform (FT) and the short-term Fourier transform (STFT) are unsuitable for subband decomposition , DWT consists of a bank structure of low-pass and high-pass filters and filters 2-way sub-sampler. The approximate and detailed coefficients are the subsampled outputs of the low pass and high pass filters, respectively. Since the sampling frequency of the signal used is 256 Hz, the detailed fourth level coefficient d4 is in the range of 8 to 16 Hz. This sub - band is used for feature extraction. Fig. 7 shows the example of a detailed fourth-stage coefficient obtained from an EEG signal.

4. RESULT DISCUSSION

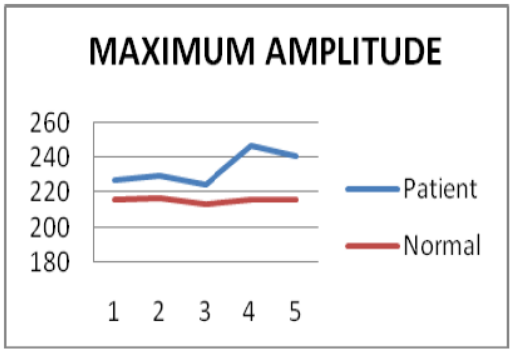
By analyzing the values of the characteristics obtained, it can be determined that there is a significant difference between the values of the normal individual and those affected by seizures. Each of the characteristic values obtained in normal and normal patients is compared and the results obtained are shown in the graphs below.



Graph -1: Analysis of Variance



Graph -2: Standard deviation analysis



Graphic -3: Maximum amplitude analysis

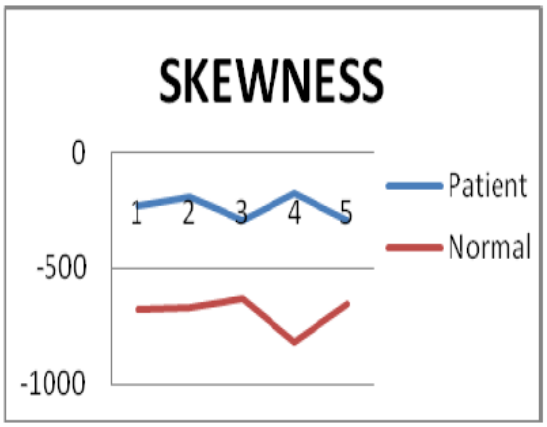


Figure 4: Asymmetry analysis

The result of the system simulation is shown in Fig. 8.

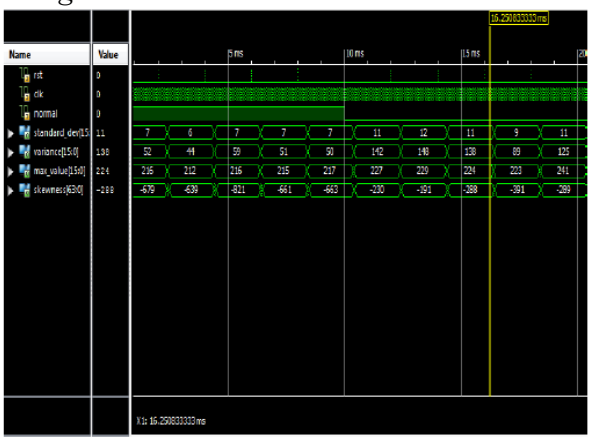


Fig-6: Result of the system simulation

If the normal signal = 1, the base of normal item data is fed to the system, and the properties of the sub - band selected are extracted. If normal = 0 then the seizure affected person's EEG database is provided and the characteristics are preserved. It is displayed in the simulation result.

5. CONCLUSIONS

The characteristics analyzed vary the standard deviation, the maximum amplitude and the asymmetry of the people who are normal and affected by the seizures of the EEG signal. Before feature extraction, the FIR filter is used to remove noise from the signal and DWT is used to get the required subband. When analyzing the characteristic values obtained, it is found that there is a significant difference between the values of normal and patient. The values obtained from the EEG database of normal and patient show a clear separation. The value of the variance, the standard deviation and the maximum amplitude in the patient's EEG signal are higher than in the normal case. The value of the variance indicates that the values in the patient's EEG signal are statistically more distributed. By comparing the standard deviation values, it can be seen that the data values vary more widely in the patient's EEG signal. The asymmetry that measures the imbalance or asymmetry is greater in the patient's EEG signal than in a normal signal. Because of this different type of characteristic values for two classes, it can be used for efficient seizure detection.

REFERENCES

1. Carlos Guerrero-Mosquera and Angel Navia Vazquez, “New approach in features extraction for EEG signal detection”, 31st Annual International Conference of the IEEE EMBS Minneapolis, Minnesota, USA, September, 2009.
2. D. Alexandros T.Tzallas, Markos G.Tsipouras and Dimitrios I. Fotiadis, “Epileptic Seizure Detection in EEGs Using Time–Frequency Analysis”, IEEE transactions on information technology in biomedicine, vol. 13, no. 5, September, 2009.
3. Adam Page, Chris Sagedy, Emily Smith, Nasrin Attaran, Tim Oates and Tinoosh Mohsenin, “A Flexible Multichannel EEG Feature Extractor and Classifier for Seizure Detection”, IEEE Transactions On Circuits And Systems II: Express Briefs, Vol. 62, no. 2 , February, 2015.
4. Mohamed Bedeeuzzaman.V, Omar Farooq, Yusuf Uzzaman Khan, “Automatic Seizure Detection Using Higher Order Moments”, International Conference on Recent Trends in Information, Telecommunication and Computing, 2010.
5. Hao Qu and Jean Gotman, “A Patient-Specific Algorithm for the Detection of Seizure Onset in Long-Term EEG

Monitoring: Possible Use as a Warning Device", vol. 44, no. 2, February, 1997.

ML CHATBOT CONVERSATION SYSTEM FOR HUMAN INTERACTION AND SENTIMENT ANALYSIS IN CHAT WEB APPLICATION

Dr. Archek praveen kumar[1]., V.Uma devi[2]., M.Devarshini[3]., G.Kavya[4]., M.Kavya [5].,

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: archekpraveen@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***This research aims to simplify the forms of communication and research in today's world that we all face due to the large amount of data on the server and website. Everyone has a question that they cannot get an answer to by crawling and scratching the website, or even after trying google search or using any other search engine. And after spending a lot of time on the internet, we always get a list of solutions, but the chances of getting the correct answer are very slim, all because we never get a solution from the owner we are looking for. Although many websites have a chat system for communication, this is not enough to function properly as a real person often needs to respond to your request. After seeing these types of issues we created a system for all inquiries in order to get the perfect answer from the right owner.***

Keywords: NANI, CHATBOT, conversation system, machine learning, programming, Levenshtein distance, sentiment analysis, most occurrences.

1. INTRODUCTION

In today's world, people are very advanced in adjusting things in their life because they appreciate knowing other ways that are wasting their time. Everyone wanted to spend less time doing things. A simplified and well-planned ML chat system called NANI has been developed that can interact with the user to get the perfect solution to their questions and even after a conversation if the user is not satisfied with the given solution, then the system has all the functions. to redirect the user to a specific dealer profile. A person can then have a conversation with the ML base chat system through the trader's profile to answer questions about the particular area the trader is working on. All institutions, stores, banks, IT companies, schools, various government agencies and companies that offer verified services can have a NANI account which can serve as a merchant profile for all other users who want to receive information over a conversation.

2. DIFFICULTIES IN THE PREVIOUS WORK

The traditional way of searching right now is to run the query through the search engine and get a list of unpredictable solutions. Another website decides on a solution.

1. It's hard to find the right answer.
2. You need to search and read data from different websites and after spending a lot of time we may not have been able to find a solution.
3. Method that takes time.
4. Sometimes boring when you can't seem to find the solution.

3. PROPOSED SYSTEM

NANI is a web application that can be used to process the conversation with the user in order to solve his problems. It is a machine learning based chat application that learns more with more time in conversation . To automate the consultation process, all you have to do is visit the app and chat with NANI. You will be guided through the app until you get its solutions. That's all the system has. It's a simplified version of everything you need to know. Simple but very effective.

NANI can be accessed via any browser. It is a Python-based conversational app with a RESTful API written in the JavaScript Framework that gives the user access to complete work application solutions.

The application does the following:

- Administrator and profile login form with various options for training further data in the Python ML script.
- Subscribe / log in to all verified dealers.
- Separate profile for the verified user.
- Form in which the merchant can create data for him with various databases for his respective users.
- Link to redirect the user to the dealer profile.
- Communication with an event-based two-way system to increase the speed of interaction.

3.1 Base Application

NANI is a highly interactive application that runs on cloud services such as AWS. This MongoDB database is mainly used to work with the NODEJ application and Python script running in the background to support the machine learning conversational method which is entirely written in Python.

Figure 1 Explain the basic process of implementing the technologies used:

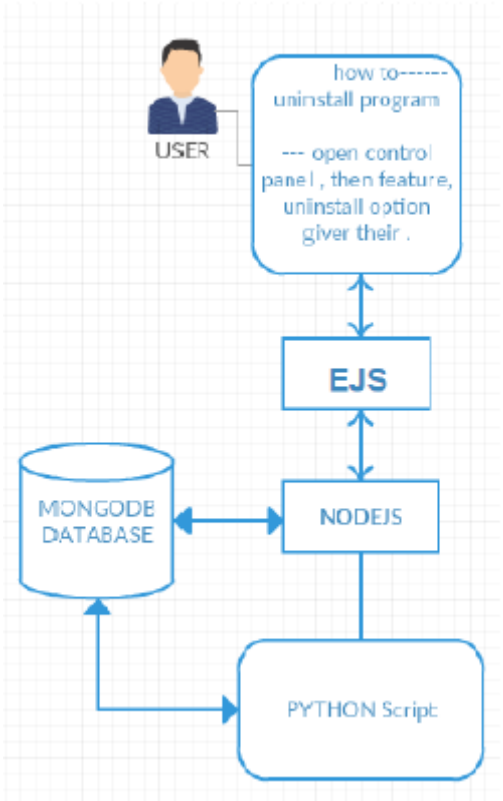


Fig. 1: Process

3.2 applied technology

ECMAScript frameworks: NODEJs, Socket.io, Express, EJS, PASSPORTJs, Python, scripting language, child process, understanding of natural language

3.3 Treatment system

User: This is the person who interacts with the chat interface to have a conversation with NANI. These users do not need to sign in or register to interact. Only the verified dealer can log in to create his profile data for the specified user.

The dealer can be:

1. School / College / University
2. State government agencies, PMO office
3. DOCTORS
4. DEFENSE
5. Teacher
6.Brand shop, etc.

EJS: It's a built-in ECMAScript just like the HTML with additional dynamic code writing to have a great way of implementing the web page switching function.

NODEJs - This is the most interesting project done with V8 Chrome engine to enable asynchronous programming in Javascript to be a pure server-side program with an event unit with no I / O blocking system and with the standard repository called What zu create NPM becomes a powerful system.

PYTHON SCRIPT: It is a strong language that is preferred when working with scientific calculations. Her library and module make this language so valuable that she is forced to include it in this project so that we can get the best result.

MongoDB - A full NOSQL database that handles large files with less disk space and a solid response time because it uses the JSON data format type to store data.

Other technologies included

1. Socket.io: To have instant dialogs with the system in real time without using AJAX, not all of us need to refresh the page.
2. EXPRESSJs: A routing module for NODEJs that is used to route to another site.
3. Child-Process - To start the thread, we use this module to start the Python script and

process the data sent and retrieved by the output of the script.

4. PASSPORTJS: Used to authenticate the user.

3.4 Work Process

In EJS-Script there is a chat interface form in which every NANI user can chat with her. When the user enters data in the input field and presses the Enter key, the onclick () function is started. In this function we use the socket.emit function, which sends data to socket.on in the nodejs file. The data is transferred via http without additional functions. Socket.emit is used to send data over http and socket.on is used to receive data over http. Although this conversation starts with. io is a snapshot of the socket.io module.

When it connects to the data received, it starts its function with the data previously received and then starts the child process where we run the Python script on this data and wait for that process to return. After we get new data from this process, we send this data over a socket in the nodejs file to socket.on in the EJS file. Then we print this data to the ejs file and that's it!

Since we know how to work in a Python file, we use the sys module to import the arguments from the node file that send data to this Python file. The NODEJs send data in the form of a list to Python to evaluate the required data. With PYMONGO we configure the Mongo database with a collection called statements. All files stored in MongoDB are JSON files and the BSON format. We need to configure the input adapter and output adapter to print the answer with the logical adapter for sentiment analysis, best match, Levenshtein and Synset removal , and then compare your answer by comparison in ML and filter the best answer with the greatest possibility. And send this data to the node file.

Natural language processing consists of two system processes, one is natural language understanding and the other is natural language generation. Our work is based solely on language comprehension, the NLP process which includes the analyzer, tokenization and the POS.

4. RESULT

NANI is a very useful web application for everyone, of all ages, everyone can chat and answer all their questions perfectly. Features like verified dealer or official government or private chat system that can be self-trained, which improves NANI's productivity and ultimately leads to better results for your inquiries. He can help you in emergency situations, he can act as a tour guide, help with booking tickets, he can consult government procedures, help with financial advice, medical advice, legal proceedings and most importantly more. The increase in the number of people joining this platform results in a better system.

5. CONCLUSIONS

We have succeeded in using this conversation portal system perfectly. This portal is very useful as we all have to change the way we search the internet and communicate with someone via email to ask the usual question every time.

The NANI bot is an easy way to get information from an ML chat dialog system. NODEJS gave this plan and is very responsive to users.

REFERENCES

1. R.S. Russell, “Language Use, Personality and True Conversational Interfaces.” Project Report, AI and CS, University of Edinburgh, Edinburgh, (2002)
2. http://www.sersc.org/journals/ IJUNESST/vol8_no2/36.pdf
3. https://pypi.python.org/pypi Bran, “Chabot‟s in customer communication”, Springer, Berlin (2003)

ONLINE EXAM SYSTEM WITH BUILT-IN SPEECH RECOGNITION INDEPENDENT SPEAKER IDENTIFICATION

Dr I. Selvamani [1]., M.Tejasree[2]., M.Srilakshmi[3]., G.Aruna[4]., M.Kavya [5]

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: i.selvamani@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0443, 17RG1A0442, 17RG1A0428, 17RG1A0423), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***A speech recognition system converts the sound of speech into corresponding text. The device first understands the spoken language, then the corresponding text is displayed. This article describes how to develop an efficient speech recognition system for independent, real-time, speaker-isolated English words. Speech is a useful and efficient way to communicate with machines, especially in an environment where keystrokes are tedious or impossible. This article is a study of the technology and modeling techniques that have been used for speech processing and the application of ASR in the online review system. The online exam system with speech recognition is very useful for educational institutions to prepare for the exam, save time checking paper, and prepare music sheets. It is particularly useful for students with disabilities to take tests and university exams. The built-in speech recognition system makes the investigation, follow-up and closure process more efficient, organized, less chaotic and extremely convenient.***

Keywords: independent speaker, isolated, ASR, online exams, students with disabilities.

.

1. INTRODUCTION

Speech recognition refers to the ability to hear spoken words (input in audio format) and to identify various sounds contained therein and recognize them as words of a known language. Speech recognition in the field of computer systems can be defined as the ability of computer systems to accept spoken words in audio format; the steps that computers need to recognize speech include, for example: voice recording, word boundary recognition, feature extraction, and recognition using knowledge models. Word boundary detection is the process of identifying the beginning and the end of a spoken word in a given audio signal. Knowledge models refer to models like the acoustic model, language models, etc. that helps the recognition system. In order to generate a knowledge model, the system must be trained by providing speech samples to the corpus.

2. RECOGNITION OF THE SPEECH

2.1 Components of the speech recognition system

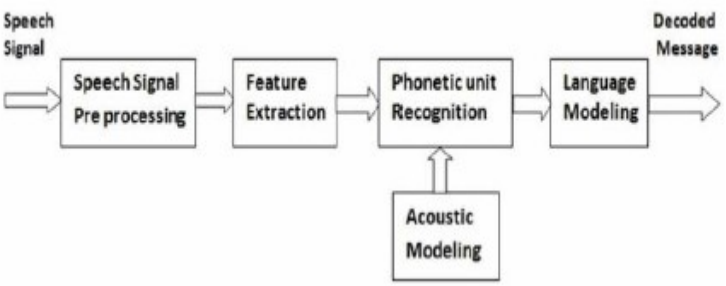


Fig. 1: Speech recognition system modules

In speech recognition, an acoustic waveform is mapped into text (or a series of words) that must match the information conveyed by the spoken words.

2.1.1 Acquisition of the voice signal: At this point in time, the analog voice signal is recorded in WAV format using a high-quality, quiet unidirectional microphone and converted into a digital voice signal.

2.1.2 Feature extraction: Feature extraction is a very important part of SR system development, in which a sparing sequence of feature vectors is computed in order to provide a compact representation of the given input signal. Speech analysis of the speech signal is the first step in the feature extraction process, generating raw features that describe the envelope of the power spectrum.

2.1.3 Acoustic modeling: Acoustic models are developed to relate the observed properties of speech signals to the expected phonetics of the hypothesis word / phrase.

2.1.4 Linguistic and Lexical Modeling: The ambiguity of words is a problem that needs to be treated with caution and that the acoustic model alone cannot address. The lexical model provides the pronunciation of words in the specified language and contains the correspondence between words and telephones [3], [4] Generally, canonical pronunciation is used, which is available in traditional or standard dictionaries. The main idea of the adaptation is to minimize the dependence of the system's performance on the voice, microphones, transmission channel and acoustic environment of the speaker, so that the generalization of the system can be improved.

2.1.5 Detection: Detection is a mechanism in which an unknown test sample is compared with each reference standard for sound classes and therefore a measure of similarity or proximity is calculated.

2.2 Basics of speech recognition

Speech recognition is essentially the science of speaking to the computer and making it recognized correctly [9]. To develop it, we need to understand the following terms [8], [11].

2.2.1 Terms

If the user says certain things, it is a statement; In other words, saying a word or combination of words that mean something to the computer is called a statement. The instructions are then sent to the speech engine for processing.

2.2.2 Pronunciation

A speech recognition engine uses a process word for its pronunciation that represents how the speech recognition engine thinks a word should sound. Words can be linked to multiple pronunciations. The language model predicts the probability that a word will appear in its context. In some cases, there may be phonetically similar words but they have different meanings and are called homophones. Dealing with these homophones is an important issue for any ASR as they generally increase acoustic confusion. Different languages have different numbers of homophonic words. For example, the French language supports a large number of homophones; Hidden Markov processes are statistical models that attempt to characterize the statistical properties of the signal with the underlying assumption that a signal can be characterized as a random parametric signal, the parameters of which can be precisely estimated and precisely defined. To implement a single word recognition system with HMM, the following steps must be performed:

(1) For each spoken word, a Markov model must be built using parameters that optimize the observations of the word.

(2) The maximum likelihood model is calculated for the spoken word. [5], [9], [10], [11].

2.2.3 Grammar

The grammar uses a certain set of rules to define the words and sentences that are recognized by the language engine. More precisely, the grammar defines the area with which the language engine works. The grammar can be as simple as a list of words or flexible enough to accommodate different degrees of variation.

```
Choices commandChoices = new Choices("A", "B", "C", "D", "E", "F", "G", "H", "I", "J", "K", "L", "M", "N", "O", "P", "Q", "S", "T", "U", "V"
GrammarBuilder grammarBuilder = new GrammarBuilder();
grammarBuilder.Append(commandChoices);
Grammar g = new Grammar(grammarBuilder);
g.Name = "Available programs";
```

Fig. 2: Grammar Builder

2.2.4 Accuracy

The performance of the speech recognition system can be measured [8]; The capacity of the detection device can be measured by calculating its accuracy. It is useful to identify a statement.

Word	Recognition%
Male	80%
Female	85%
Computer	85%
Robot	78%

Table 1: Accuracy of detection

Word Error Rate If you are checking the number of words in the test data transcript that your system has mistakenly recognized from the transcript, you will do so manually. Sentence Error Rate If you are checking the number of sentences in the transcript of test data that your system misrecognized from the transcription, perform them manually.

2.2.5 Vocabulary

Vocabulary is the list of words that the speech recognition engine can recognize. Smaller vocabulary is generally easier to identify with a speech recognition engine, while a large list of words is a difficult task for the engine.

2.2.6 Training

Training can help users who have difficulty speaking or pronouncing certain words. Trained speech recognition systems must be adaptable.

3. Proposed model

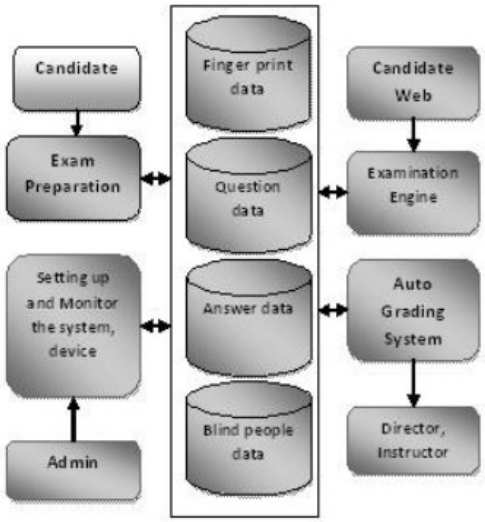


Fig. 3: Architecture of the proposed model

Database Tier

Here the data is saved as data records in the server-side database tables.

Exam system data

It contains all the data for the questions; For all response data, these data are explained as follows:

Exam Preparation:

It is used to manage and process the questions asked during the exam. It also contains the logic behind the instructor-course relationship, the instructor-term relationship, and the letter behind those relationships. This logic is used to manage all of the administrator relationship information stored in the database. A detail of this logic is described below:

Add questions: The administrator can add the questions to the database entry first.

Create Exam: The admin can create an exam by selecting the questions previously added.

Update Exam - Admin can update the previously passed exam.

Schedule Exam: The administrator can schedule the exam for the blind student.

System Configuration and Monitoring: This is used to configure and manage the candidate information listed below: The login administrator can insert or update the candidate information. There are a few scenarios for this event. The administrator logs in and can insert or update instructor information which can first check if the instructor is absent. The administrator can create a new instructor record by adding the instructor's data to the instructor.

Automatic Assessment - This enables our system to automatically rate candidates' responses collected by the examination system. The system compares the students' answers with the correct answers entered by the administrator.

4 RESULTS

Fig. 4: Language libraries integrated into the Windows platform

Speech Application Programming Interface (SAPI) is an API developed by Microsoft that enables the use of speech recognition and text-to-speech in Windows applications. In general, the speech API can be viewed as an interface between applications and speech modules (recognition and synthesis).

SAPI 5.1 This version was released in late 2001 as part of version 5.1 of the Speech SDK. Interfaces have been added to the API that support automation to enable the use of Visual Basic, scripting languages such as JavaScript, and managed code. This version of the API and TTS engines ships with Windows XP. [10] Windows XP Tablet PC Edition and Office 2003 also include this version.

Microsoft SQL Server 2008 platform was used for the back-end development of this system, where the entire database of the proposed system is systematically created and maintained.

5. CONCLUSION

This project would be very useful for any blind or disabled student so that we can test their skills more easily and effectively like any other normal student through an online exam. And we will also try to make any improvements in the future by collecting feedback. One of the main goals for the future will be to include Hindi and other mother tongues so that the system can be expanded to help the illiterate as well.

REFERENCES

1. Watcher, M. D., Matton, M., Demuynck, K., Wambacq, P., Cools, R., “Template Based Continuous Speech Recognition”, IEEE Transaction on Audio, Speech, & Language Processing,2007.
2. Watson, B. and Chung T. (1992) ‘Second order Hidden Markov Models for speech recognition’. Paper Presented at Fourth Australian International Conference on Speech Science and Technology, pp.146-151.
3. Dev, A. (2009) ‘Effect of retroflex sounds on the recognition of voiced and unvoiced stops’, Journal of AI and Soc., Springer, Vol. 23, pp. 603-612.
4. Polur, P. D., Zhou, R., Yang, J., Adnani, F. and Hobson, R. S. (2001) ‘Isolated speech recognition using artificial neural networks’. Paper Published in Proc. of the 23rd annual EMBS international conference, IEEE, Turkey, pp.1731-1734.
5. “Speech recognition- The next revolution” 5thedition.
6. Forgie, J. W. and Forgie, C. D. (1959) ‘Results obtained from a vowel

recognition computer program, J. Acoust. Soc. Am., 31(11), pp.1480-1489.

Hemdal, J.F. and Hughes, G.W., A feature based computer recognition program for the modeling of vowel perception, in Models for the Perception of Speech and Visual Form, Wathen-Dunn, W. Ed. MIT Press, Cambridge, MA.

CROP PREDICTION AND PLANTATION FOR DIFFERENT CLIMATIC CONDITIONS USING HADDOP HDFS BASED ANALYSIS OF WEATHER DATA

Ch. Keerthi[1]., G.Bharani[2]., J.Lasyavi[3]., M.Sana[4]., S.Yeshwitha[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (: krith@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0424, 17RG1A0432, 17RG1A0446, 17RG1A0454),

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***Big data is an extensive collection of data from many sources such as remote sensing data, data posted on social media websites, electronic purchase transactions, etc. It becomes more difficult to process this data and then use it for forecast analysis. with older methods. The best way we can make improvements is to use Big Data Analytics (BDA) as this type of data is generated over and over again from many resources. With BDA we can find some trends and patterns that will be useful in the next phases of the project. In this project, we analyze weather data and use the result obtained to predict what types of crops can be grown under different climatic conditions in all districts of Tamilnadu using Hadoop ecosystems such as HDFS. The methods we used overcome problems like data limitations, data loss problems, processing one record at a time, and other additional limitations that the previous methods had.***

Keywords : Big Data Analytics, HDFS, SQOOP, VM, card reduction.

1. INTRODUCTION

Agriculture is an important part of your country. Farmers use various manual methods to find out which crops can be grown and when. As technology advances, precipitation can be predicted based on several well-known methods. There are several forecasting methods that can be used to grow crops depending on climatic conditions. The rationale for this project is to incorporate these methods and predict which crops can be grown under certain conditions. This project uses the map reduction algorithm to analyze the meteorological data present in all districts of Tamilnadu from 2004 to 2015. Based on the result obtained, the crops to be grown can be predicted using fuzzy reasoning, thereby maximizing the benefits.

1.1 LIMITATIONS OF THE EXISTING SYSTEM

The above system uses K-Means Pooling to analyze and predict which crops to grow. Some of the limitations were the longer run time, the inability to use other data sets for processing such as the ground based data set, and only one data set can run at a time, that is, only one year or one district. at a time. The maintenance time and cost of the existing system were also high. The proposed system, on the other hand, can handle larger data sets than the existing system.

2 SYSTEM ARCHITECTURE

HDFS cannot directly access weather data, which contains information about the amount of precipitation in different districts of India obtained from different sources. In order to continue processing the data, the raw data must be converted into a suitable HDFS-compatible format. With MySQL Administrator weather data in the form of. csv (comma separated values) is saved and stored in a convenient location. This is the first part of the first module. Since we are processing the data via HDFS and Cloud-Era, this is an obvious option as the free open source file needs to be transferred to the Cloud-Era VM.

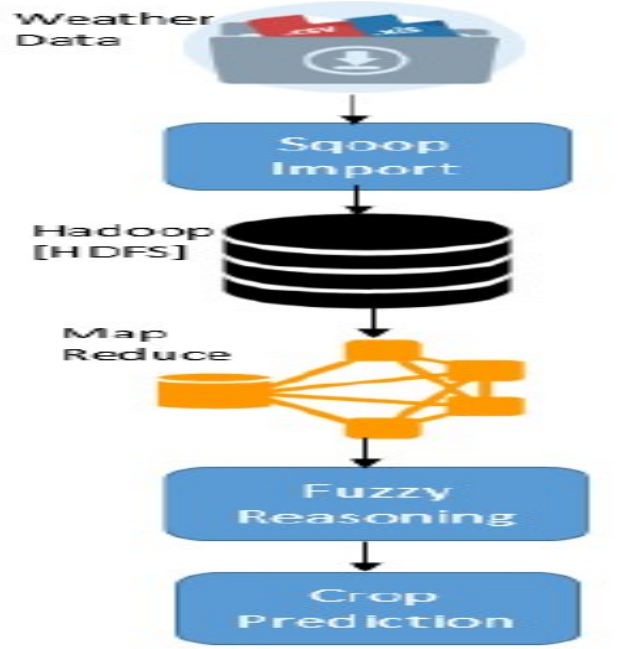


Fig 1 Different phases of the project.

3. PROPOSED METHODOLOGY

3.1 PRE-PROCESSING AND MIGRATION OF DATA WITH SQOOP

The backup of the meteorological data is moved to the VM and saved in the current working directory. This backup must be moved to HDFS for further operations. With the integrated SQOOP tool, we move the data to HDFS. The reason SQOOP is used is because analyzing all the data at once is an impossible task since we are dealing with a lot of data. Therefore we will analyze them in parallel, which is why the task would be so easy with the data was stored in groups in HDFS. This is where SQOOP comes in. By using this tool, the data is automatically stored in clusters so that the analysis part can run in parallel, that is, multiple virtual machines are running at the same time and the output is obtained faster than any other traditional method.

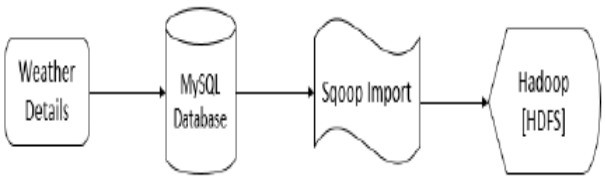


Figure 2 Importing with Sqoop

3.2 DATA ANALYSIS WITH REDUCTION CARD

After the data has been moved to the distributed file system, other operations can be initiated. Using the map reduction algorithm, the data can be analyzed and the required output obtained. In general, Map Reduce is a Java-based processing technique. The Map Reduce algorithm contains three important tasks: Driver, Mapper, Reducer. The controller is used to create jobs and configure the mapper and reducer. Mapper takes a record and converts it to another record. The reducer takes the output of a card as an input. In this project module, the minimum, maximum and average precipitation values for the years 2004-2015 for all districts of Tamil Nadu are determined using the data obtained in HDFS.

3.2.1 PILOT

This is part of Map Reduce, where the jobs that will be run by the mapper and reducer are created. Mapper and reducer are configured here. The input and output parts are created. The Mapper and Reducer classes are created. The input format and the output format of the mapper and reducer are specified here. In fact, this is where the main () function is located, and this is where the allocator and reducer are called.

3.2.2 MAPPING

This part of the program is used to extract the data required for further processing, as not all data has to be sent for each run. The data to be sent is determined by the user. There are options like sending the full dates so we can get the total precipitation in Tamil Nadu for all those years, or sending just the months users want for a specific district which is entirely up to the user.

3.2.3 REDUCER

All arithmetic operations take place here. Taking this project into account, we can find the minimum, maximum, and average values for all districts of Tamil Nadu. These operations are key to finding the required output, which is sent to the next module where the actual prediction takes place.

District	Minimum	Maximum	Average
Coimbatore	1.3	17.7	7.7285714
Cuddalore	0	73.3	20.833334
Dharmapuri	0	196.1	39.491665
Dindigul	0	100.5	17.125
Erode	0	218.7	47.416668
Kanchipuram	0	28.8	10.033334
Kanyakumari	0	114.2	20.625
Karur	0	43.8	6.9166665

Table 2.3.1: Example of a production card reduce

4 RESULT ANALYSIS

4.1 Crops Prediction

This part of the project is done using Python because of its ease and robustness. After getting the output of the card reduction, the output data is exported from HDFS to MySQL using the SQOOP export, which is exactly the opposite of the SQOOP import command. In MySQL, data is stored in Python, which is used for additional calculations. Since we are using fuzzy reasoning, there should be classifications. Heavy rainfall is one of the

classifications and low rainfall is the other. With this and the data already collected for specific cultures in each district, fuzzy logic can be applied. The data containing specific crops for each district is only in place to ensure that the crops we receive as production can be planted there. The yield that can be achieved depends on the user. The user has to select the desired quarter and month in which to plant the plants. This last part of the project will restore the average rainfall in this district, especially this month, as well as the crops to be successfully planted there, and help us to get the maximum benefit from it.

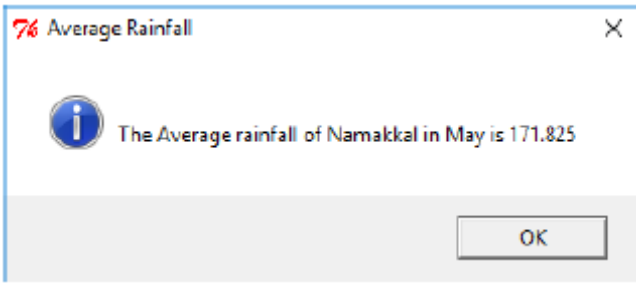


Figure 3 Average rainfall

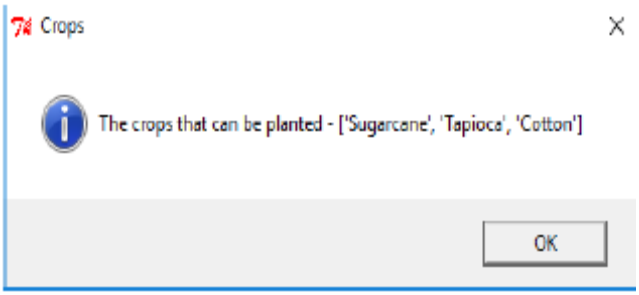


Figure 4 Plants that can be planted

4. FUTURE IMPROVEMENTS

Although the amount of data analyzed and forecast is large, more data can be added. This project processes data on all districts in Tamil Nadu. However, in the future, all districts in our country can be processed, analyzed and predicted. Here only rainfall data is used to predict the cultivation of crops. However, in the future, soil, moisture, and other products can also be added to make the project more accurate and useful to people. Given the methods that will be used in the future with the rapid advancement of technology, new methods may be introduced day in and day out to make this project more profitable.

5. CONCLUSIONS

As technology advances, it must be used optimally. The complexity of the prediction algorithms will increase from year to year. This is another step towards realizing the perfect crop prediction algorithm that will be useful to farmers and colleagues who should also help refine the crop prediction program further the program.

REFERENCES

1. Yaser Jararweh, Izzat Alsmadi , Mahmoud Al-Ayyoub & Darrel Jenerette “The Analysis of Large-Scale Climate Data: Jordan Case Study”
2. N. Sundaravalli & Dr.A.Geetha “A Study & Survey on Rainfall Prediction And Production of Crops Using Data Mining Techniques”
3. Awanit Kumar & Shiv Kumar “Prediction of Production of Crops using K-mean & Fuzzy Logic”

EFFICIENT PROCESSING OF AJAX DATA USING TOP-K ASSOCIATION RULES AND SEQUENTIAL PATTERN EXPLORATION BASED MINING ALGORITHMS

Dr. I. Selvamani[1]., G.Chandralekha Maheshwari[2]., G.Nithisha reddy[3]., A.Annapurna[4]., J.Gayatri[5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: i.selvamani@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0421, 17RG1A0420, 17RG1A0401, 17RG1A0431), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***One of the basic tasks of data mining is the rules for mining associations. Positive mapping rules are known as typical mapping rules that only consider items listed in transactions. Negative mapping rules take into account the same items, but the canceled items that are missing from transactions. In order to identify products that are in conflict with one another or products that complement each other in the shopping cart analysis, negative allocation rules are used. In order to examine these rules, an exponentially large search space must be examined. Depending on minimal trust and assistance, algorithms can become very slow and generate a large number of results or very few results, regardless of the valuable information. Since users have limited resources to analyze the results in practice, an algorithm was proposed to extract the top-k association rules using sequential pattern exploration. In addition to improving the performance of an algorithm, AJAX is used. This is an important approach to improving the level of interactivity between the web server and the end users. If we adjust the client-server communication based on the AJAX function in the communication between the client and the servers, we will decrease the traffic and increase the transmission speed. The inquiries and answers are better, smarter and more comprehensive.***

Keywords: Association Rules Extraction, Positive Rules, Negative Rules, AJAX, Top-k Association Rules, Sequential Pattern Exploration.

1. INTRODUCTION

A mapping rule is an implication of the form X ⇒ Y, where X and Y are frequent sets of elements in a transactional database and X∩Y = O. In practical applications, the rule X ⇒ Y is used to predict that 'when X. occurs in a transaction, then Y will likely appear in the same transaction ', and we can apply this mapping rule to place' Y near X 'in the supermarket management item placement [1]. Today, data mining is extremely important for business areas such as marketing, finance, commerce and telecommunications [2]. Users have limited resources to analyze the results, so they are primarily interested in discovering a range of results. Since it takes a long time to get a complete result, Top-k's mining rules are useful [3]. Media counting is one of the main advantages of the vertical bitmap representation of data in sequential pattern mining [4].

2. LITERATURE REVIEW

Research into association rules is interpreted as the extraction of positive association rules. The positive rule of association is as follows: "If a person buys the product in the form of bread and butter, that person will likely buy milk at the same time." It is a known fact to take into account the established negative association rules such as "Birds can fly, but penguins cannot fly although they are birds" [2]. A negative match rule can be illustrated by the following example: Ayres, et al. [4] proposed a SPAM algorithm based on the idea of SPADE. The difference is that SPAM uses a bitmap representation of the database regardless of the sid-tid pairs used in the SPADE algorithm. SPAM has to be one of the best research strategies to extract sequential patterns. Another outstanding feature of SPAM is the ability to generate sequential patterns of different lengths online. The vertical arrangement of bitmap data is used in the SPAM implementation to enable simple and efficient counting.

The Top-K problem with mapping rules uses a new approach to generating mapping rules called "rule extensions" and various optimizations. An evaluation of the algorithm with data sets used in the literature shows that TopKRules has excellent performance and scalability. In addition, the results show that

Top K-Rules are a beneficial option for association rule mining algorithms for users who want to control the number of association rules generated [3].

3. PROPOSED WORK

In the proposed work, sequential model mining is combined with top-k-rule mining to get better exploration results, and analysis based on non-AJAX mining and AJAX mining is performed to correlate the performance of an algorithm. The proposed work focuses on getting efficient results with AJAX using various mining techniques such as Patten Sequential Mining, Top-k Mining, and Pruning Deep Search Strategy First. The proposed algorithm follows the following steps:

Step 1. Enter the item set, pattern length, and support threshold.

Step 2. Analyze the database for multiple sequences.

Step 3. Perform the classification and investigation of transactions.

Step 4. Find the relationship between the data using the top k rule.

Step 5. Separate the positive and negative rules.

Step 6. Display the result of mining with AJAX and without AJAX.

The proposed mining algorithm works as follows:

Step 1. Search the database to save the position of the first bit of each sequence and calculate the total number of bits for each bitmap.

- For each sequence, play a file to the end.
- Save the length of a current sequence
- Order divided according to the fields on the cards.
- If each token is not an element separator,

Save the last bit position for bitmaps.

Step 2. Analyze the database to create a vertical representation of the database.

- sid knew which sequence to scan and tid to know which group of items to scan.
- Sequences divided by spaces and if the token is -1, increase tid and if the token is -2, otherwise increase a bitmap for the element
- Save the bit in the bitmap for the current element with sid, tid and stream size.

Step 3. Remove rare elements as they will not appear in common sequential models.

- Browse the elements to get a bitmap image of the element.
- If the cardinality of the bitmap is below the minimum support, delete the element.
- Otherwise, add the item to the list of common items.

Step 4. Perform an initial deep recursive search to find longer sequential patterns recursively.

- For each common element, create a prefix with that element.
- Call the DFS method with a specific prefix.
- Perform a DFS cut.

In the proposed work, the association rule exploration algorithms can generate a large number of association rules depending on the choice of parameters, resulting in a long execution time and high memory consumption. In the case of top k rules for positive and negative elements, an algorithm found that top k rules have the greatest support, with the value of k being defined as a constant by the user in an algorithm.

4. ANALYSIS OF THE RESULTS

According to the analysis of the results of the proposed algorithm, the input support value 0.1, 0.2, 0.3 and 0.4 with the pattern length 3, 5, 10 gives a good set of positive and negative mining rules. In the case of the support value of 0.5, we only received a series of negative rules. A threshold of 0.5 has been set for the class value to separate positive and negative rules.

The results of the proposed algorithm are as follows:

Time Analysis			
Support	Pattern Length	Time (without AJAX)	Time(W
0.1	3	65 ms	16 ms
0.1	5	16 ms	15 ms
0.1	10	20 ms	15 ms

Table -1: Time analysis with the support constant 0.1

Time Analysis			
Support	Pattern Length	Time (without AJAX)	Time(W
0.2	3	65 ms	16 ms
0.2	5	16 ms	15 ms
0.2	10	20 ms	15 ms

Table -2: Time analysis with the support constant 0.2

Time Analysis			
Support	Pattern Length	Time (without AJAX)	Time(With AJAX)
0.3	3	65 ms	16 ms
0.3	5	16 ms	15 ms
0.3	10	20 ms	15 ms

Table -3: Time analysis with support constant 0.3

Pattern length 3, 5, 7, and 10 works well for all media values 0.1, 0.2, 0.3, and 0.4, while pattern length 2 works well for media values 0, 1, 0.2, and 0.3 .

Time Analysis			
Pattern Length	Support	Time(Without AJAX)	Time(With AJAX)
2	0.1	2 ms	0 ms
2	0.2	1 ms	0 ms
2	0.3	2 ms	0 ms
2	0.4	0 ms	0 ms

Table -4: Time analysis with a sample length constant of 0.3

Time Analysis			
Pattern Length	Support	Time(Without AJAX)	Time(With AJAX)
3	0.1	5 ms	3 ms
3	0.2	5 ms	0 ms
3	0.3	2 ms	0 ms
3	0.4	1 ms	0 ms

Table -5: Time analysis with pattern length constant 3

Time Analysis			
Pattern Length	Support	Time(Without AJAX)	Time(With AJAX)
5	0.1	57 ms	16 ms
5	0.2	21 ms	16 ms
5	0.3	35 ms	32 ms
5	0.4	3 ms	0 ms

Table -6: Temporal analysis with pattern length constant 5

Taking into account the results of the previous analysis, it is shown that examining association rules using top k rules with a sequential examination of models gives more efficient results than without AJAX.

6. CONCLUSIONS

The method proposed in this document to restore rule extraction uses the classification and extraction algorithm to effectively improve the results. The proposed method tries to present results effectively by separating positive and negative rules that can be used for product placement in supermarket management.

REFERENCES

1. Jay Ayres, Johannes Gehrke, Tomi Yiu, and Jason Flannick, "Sequential Pattern Mining using A Bitmap Representation", Dept. of Computer Science Cornell University.
2. Sumayya Khan, Shrikant Lade , "Enhanced Data Processing Using Positive Negative Association Mining on AJAX Data", IOSR Journal of Computer Engineering, Volume 16, Issue 2, Ver. II (Mar-Apr. 2014), PP 15-18.
3. Philippe Fournier-Viger1 and Vincent S. Tseng2 , "Mining Top-K Non-Redundant Association Rules", National Cheng Kung University, Taiwan.
4. Xindong Wu, Chengqi Zhang and Shichao Zhang, "Efficient Mining of Both Positive and Negative Association Rules", ACM Transactions on InformationSystems, Vol. 22, No. 3, July 2004.
5. Mudra Doshi, Bidisha Roy, "Efficient Processing Of Ajax Data Using Mining Algorithms" International Journal of Computer Engineering and Technology (IJCET), Volume 5, Issue 8, August (2014), pp. 48-54.
6. Philippe Fournier-Viger1, Cheng-Wei Wu2 and Vincent S. Tseng2 "Mining Top-K Association Rules", National Cheng Kung University.
7. R.Sumalatha1, B. Ramasubbareddy2, "Mining Positive and Negative Association Rules", International Journal on Computer Science and Engineering(IJCSE), Vol. 02, No. 09, 2010, 2916-2920.
S.Vikram Phaneendra, "Minimizing Client-Server Traffic Based On Ajax", International Journal Of Computer Engineering & Technology (IJCET), Volume 3, Issue 1, January- June (2012), pp. 10-16.

A SECURE VANET AUTHENTICATION SCHEME FOR WIRELESS VEHICULAR AD-HOC NETWORKS USING TWO-FACTOR LIGHTWEIGHT PRIVACY BACKUP CONFIRMATION

B. Sneha Priya[1]., K.Naga ramya[2]., D.Manasa[3]., S.Swaroopa[4]., B.Ananya[5].,

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: budhasnehapriya@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0404, 17RG1A0415, 17RG1A0453, 17RG1A0406), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***The specially designated vehicle system (VANET) has been the subject of extensive research efforts by government, science and industry in recent decades. In this endeavor, he proposed a 2FLIP (TWO-Factor Lightweight Privacy Backup Confirmation Conspiracy) to improve the security of VANET correspondence. 2FLIP uses Decentralized Testamentary Expert (CA) and Secret Word-Based Two-Variable Organic Verification (2FA) to achieve its goals. Given the decentralized certification authority, 2FLIP requires few outrageous and light hashing processes and fast MAC operation for tagging and confirming messages between vehicles. The conspiracy proposal provides solid protection, ensuring that while pursuing a vehicle, enemies can never get their way, even with all negotiated RSUs. Extensive rewrite shows that 2FLIP is achievable and has excellent performance of approx. 0 ms organizational delay and 0% error rate on packages, which are particularly well suited for ongoing retail applications in crisis.***

Keywords : MAC, authentication, secret key, wireless network.

1. INTRODUCTION

In VANET, every vehicle is equipped with a locally available unit (OBU), which you can use to chat remotely with different vehicles and road units (RSU) via at least one jump. In this way, a large remote system could be developed that, using Dedicated Short-Term Exchanges (DSRC) [2], enables fast vehicle-to-vehicle exchanges (V2V) and reliable vehicle-to-road exchanges (V2R), while specially designed and informative ingenious versatile elements are realized. The amazing properties of VANET are enormous for corporate management and road safety. In addition, V2V is used to transfer critical safety data between vehicles and to warn drivers of impending accidents.

In the proposed representation, each vehicle would be connected to a telematics device that is used with biometric innovation [6] (e.g. confrontation, unique fingerprint, iris ...) to confirm the personality of the different drivers and give confirmations, to follow every driver. The flexibility of biometrics is not taken into account. In addition, a carefully designed device (TPD) is implanted in the OBU to save scratches on the frame and to sign / confirm messages. To secure V2V and V2R exchanges, 2FLIP only requires light and outrageous one-way hash operations and MAC era operations for tagging messages, hash job with fast MAC re-era for validation. The advanced brand verification process will only continue if the vehicle needs a frame key update that would not affect execution.

The advantages of the 2FLIP method are:

1. Strong privacy protection
2. Strong non-rejection
3. Secure update of the system password
4. Secure offline password update
5. Extremely light and efficient
6. Low certificate management costs, communication costs, and network delay.

1.1 EXISTING METHOD

In this article, we'll look at advanced and non-optimized tracking calculations. As stated in Dedicated Short Range Communication (DSRC) [10], which is part of the WAVE standard, every OBU has to transmit a message every 300 ms about its area, speed and other telematics data. In such a situation, each OBU can receive a large number of messages every 300 ms and must check the current CRL for all received endorsements, which can result in a long confirmation delay depending on the estimate of the CRL and the number of wills received. The ability to check a

CRL for innumerable and timely results leads to inevitable tests for VANETs. To ensure reliable operation of VANET and to increase the amount of valid data collected from received messages, each OBU must be able to check the rejection status of all declarations received in a favorable manner. Most of the work in progress has neglected the validation time due to the CRL checking for each will received.

2. PROPOSED METHOD

2FLIP basically uses two basic strategies to achieve the general goals mentioned in the previous section: Decentralizing CA and 2FA based on natural secret words. To reduce the AC workload and correspondence load, the AC functions are decentralized to a tight security approach that includes TDi and TPDi. Here are how the neighborhood security process works. In the introductory phase, all vehicles must be registered in California. At this point, CA organizes TPDi and TDi cryptographically. In the login / confirmation organization. Before a driver has to start his vehicle, he must pass the driver attestation test immediately.

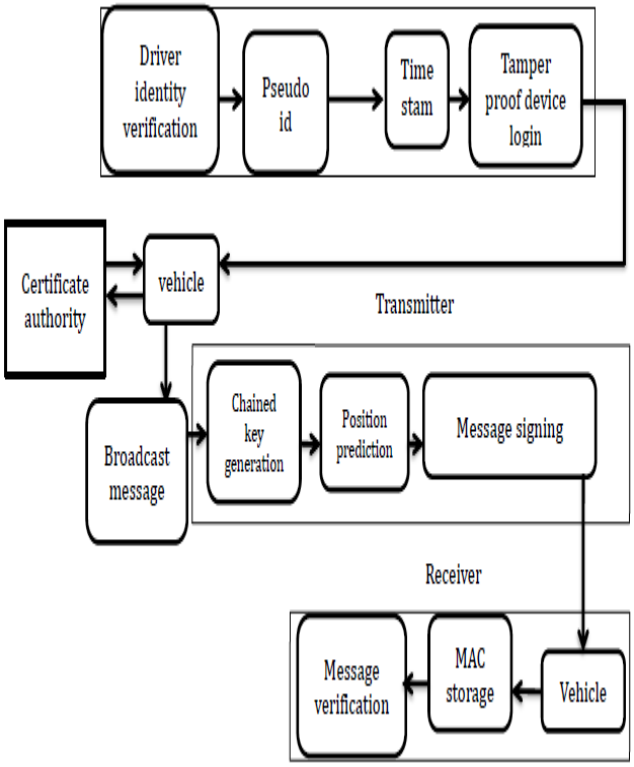


Fig. 1: 2FLIP block diagram

From that moment on, TDi can create a moment to access the TPDi token and use it to log into TPDi. If the connection is successful, TPDi can be used to generate a MAC with a frame key and access the TPDi token. As soon as the vehicle has new status data, TDi would try the TPD connection again. At this point, TPDi frames a packet with three sections: the message payload, which contains the new status data, the MAC and the dynamic pseudo-personality. At this point the property will be communicated to its neighbors. The moment a neighboring vehicle receives the message, all it has to do is perform a light and outrageous hashing operation and a MAC retrieval operation to perform message verification. Obviously, TDi and TPDi work together as CA operators to perform the validation process, while CA does not have a working stack for the V2V correspondence.

2.1 SYSTEM INITIALIZATION

- Before a driver comes to VANET, confirmation of the driver's personality must be sent immediately.
- Thereafter, the TPD connection should be accelerated within a fraction of a second every time the vehicle creates and sends a different message.
- The characteristic ladder test would be confirmed by the cooperation of TDi and TPDi.
- The driver immediately connects the TDi with the vehicle and reports his organic identification data pwi, u in the form of a secret word.
- To check pwi, use a bio-checker. In this case {PIDi, ts} must be used to connect to TPDi. To confirm {PIDi, ts} when the pass-through OBU can use TPDi.
- CA is a specialized and trustworthy professional whom others trust wholeheartedly.

2.2 TESLA SCHEME

- The recipient can check the authentication of a message only after a few time intervals.
- Each TESLA package has the following structure

(My // MAC (Ki, Mi) // Kn).

We send the message // your MAC // a previous key to verify previous MACs (n <i).

2.3 POSITION PREDICTION

Each future position Pi could be represented by:

$$\vec{P}_i = \vec{P}_o + a_i\vec{x} + \dot{b}_i\vec{y}$$

The movement of the interval is

$$\vec{M}_i = \vec{P}_i - \vec{P}_{i-1} = (a_i - a_{i-1})\vec{x} + (b_i - b_{i-1})\vec{y}$$

2.4 MESSAGE SIGNATURE

When the vehicle generates another payload message m, TDi repeats the TPD connection step to encourage TPD with a unique pseudo-personality PIDi in mode la.

• When the TPD connection is established, TPDi calculates the message validation estimate of m as mackm (PIDi, ts // h (m // km) // ts). It also communicates {PIDi, ts, ts, m} to neighboring vehicles.

2.5 CHECK MESSAGES

• TPDj calculates the verification request to confirm the authenticity of the message after vehiclej has verified a packet {PIDi, ts, ts, m} from vehiclei.

• If these two messages are the same, Vehiclej will recognize the message and use it for enforcement. Usually the message is rejected.

3. RESULTS AND DISCUSSION

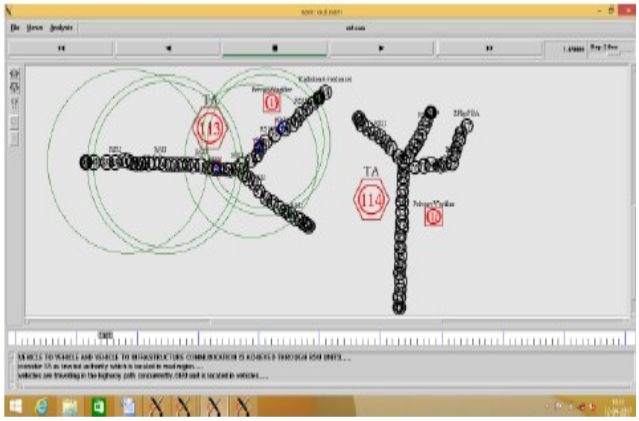


Chart 1: Creating nodes

The above figure shows the 2FLIP authentication processing. The V2V and V2I communication takes place via RSU units. Think of TA as a trusted authority in the highway region. The blue color shows the movement of the vehicles.

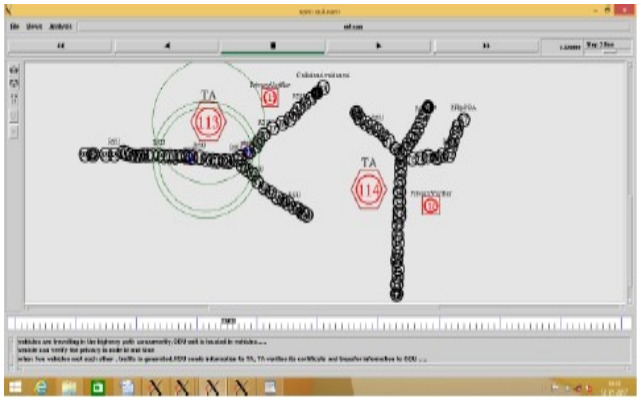


Chart 2: Communication between nodes

This figure shows that the vehicles are driving on the road at the same time and that the on-board units are in the vehicles. Please note that the data protection auditor is used to verify the report on these vehicles.

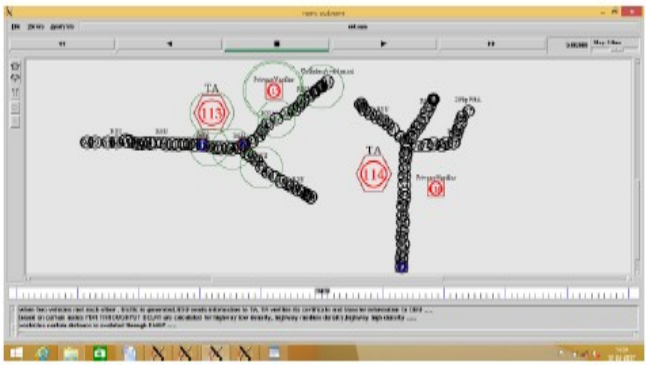


Chart 3: Position prediction

The above figure shows that when two vehicles collide, traffic is generated. RSU sends information to TA. In this TA, your certificate is checked and the information is transmitted to the on-board unit. Vehicles at a certain distance are evaluated using 2FLIP.

Chart 4: Packet Loss

The graphic above shows this packet loss. The X-axis shows the density of the network and the Y-axis shows the loss. The packet loss of the 2FLIP method is 0.3.

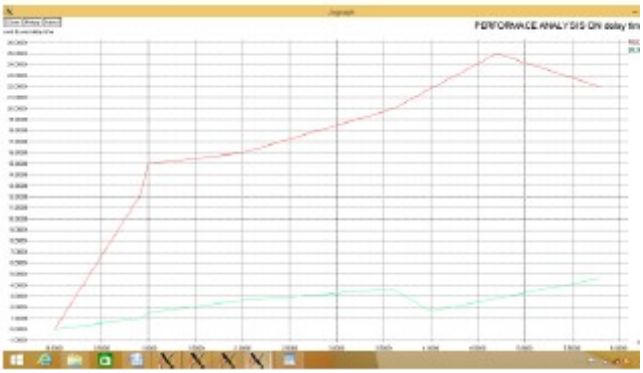


Chart 5: End-to-end delay time

This graph shows the number of on-board unit densities in relation to the end-to-end delay time. The end-to-end delay time is 3.5 ms.

4. CONCLUSION

This article suggests a lightweight two-factor authentication system that protects privacy and uses two main methods: CA decentralization and biological password-based 2FA. Based on the decentralization of AC, the proposed scheme only requires some extremely light hashing processes and fast MAC generation is required to sign messages. This hash function is combined with a fast MAC regeneration for verification, which increases the efficiency of the calculation and communication. A thorough simulation shows that the new scheme is feasible and has excellent performance in terms of message signing / verification, message loss rate and network delay.

REFERENCES

1. Erich Wenger and Thomas Unterluggauer, (2014), "Efficient Pairings and ECC for Embedded Systems ", IEEE Transactions on Information Theory, vol. 7,no. 3, pp. 298-315.
2. Filali.F, Drira.W, and D. Puthal, (2014), "ADCS: An adaptive data collection scheme in vehicular networks using 3G/LTE," in Proc. IEEE ICCVE, Vienna, Austria, vol. 4,no. 2,pp. 753–758.
3. Ahren Studer, Elaine Shi, Fan Bai, Adrian Perrig, (2009), "TACKing Together Efficient Authentication, Revocation, and Privacy in VANET", IEEE Communications Society Conference on Sensor, vol. 5,no.3, pp. 484-492.
4. Bhagyashree .R, (2007), "EMAP: Expedite message authentication protocol for VANETS" IEEE Journal on Selected Areas in Communications, vol. 3,no.5, pp. 497-452.
5. Cherif.M, S.-M. Secouci, and B. Ducourthial, (2010), "How to disseminate vehicular data efficiently in both highway and urban environments?" in Proc. IEEE 6th Int. Conf. WiMob Comput., Netw. Commun. vol.6,no.4, pp. 165–171.
6. Delot.T, N. Mitton, S. Ilarri, and T. Hien, (2011), "GeoVaNET: A routing protocol for query processing in vehicular networks," Mobile Inf. Syst., vol. 7, no. 4, pp. 329–359.
7. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, (2010), "Security Analysis of Vehicular Ad Hoc Networks (VANET)", Second International Conference on Network Applications, Protocols and Services, vol. 5,no. 4, pp. 55-60.
8. Gupta.A, and R. Singh, (2011), "Information dissemination in vanets using zone based forwarding," in Proc. IFIP WD, vol. 2,no. 5,pp. 1–3.
9. Hesham Rakha, Wassim Drira, and Kyoungho Ahn, (2016), "Development and testing of a 3G/LTE adaptive data collection system in vehicular networks", IEEE transactions on intelligent transportation systems, vol. 17, no. 1, pp. 240-249.
10. Hai Yan and Zhijie Jerry Shi, (2007), "Software Implementations of Elliptic Curve Cryptography", IEEE Transactions on Wireless Communications.

LAB AUTOMATION VIA ANDROID APPLICATION USING SUPPORT VECTOR MACHINE FOR SPEECH RECOGNITION AND MOTION DETECTION

R. Srinivas[1]., K.Richa[2]., CH.Sai priya[3]., S.Swaroopa[4]., B.Ananya[5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: srinivasr.@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0437, 17RG1A0410, 17RG1A0435, 17RG1A0436), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***In this project we describe a system that integrates a large number of wireless motion sensors and strategically placed cameras and its application for real-time indoor surveillance. Electrical devices such as fans, light switches, light sensors and current sensors are integrated into a system that is then connected to a microcontroller that controls and executes the user's commands in the laboratory. We use motion sensor data to set camera control guidelines and detect motion. This project aims to secure the laboratory through motion detection and speech recognition. The laboratory automation system plays an important role in maintaining security and provides a safe and flexible environment. While laboratory safety is an important issue, safety is not a priority. The aim of this project is to develop a laboratory automation system that enables the operation of household appliances and motion detection thanks to laboratory sensors via an Android application. Speech recognition is carried out by Support Vector Machine. Motion sensors are much more data efficient and cheaper, but have limited detection capabilities.***

Keywords : speech recognition, infrared (infrared sensors), security, Android application, laboratory automation.

1. INTRODUCTION

As technology advances, automation is easily visible in various areas. Day by day, the hassle of daily routine work decreases, and it is necessary for people's busy schedules as well as profitability. By introducing automatic switching systems that allow switching control of various household appliances, as well as some of the other tasks that make up the home automation system. Implementing a fully integrated, professional computer laboratory management system can significantly increase the efficiency, safety, and cost effectiveness of computer laboratory operations. Workstation access control, user registration and security. Colleagues in the lab need to be able to integrate clients assigned to workstations into the database, remotely screw in and open the workstations, deal with the selection list, approve clients with a list of alerts, and the presence of all Research rooms to evaluate facilities found remotely. Lab assistants and specialists should be able to keep problem logs for each workstation, representatives should be able to work as a team to resolve problems, and unwanted workstations should be separated as inaccessible so that lab assistants cannot influence customers themselves.

2. EXISTING SYSTEM

Today, computer labs in schools and universities are not automated or properly protected. Students and staff use lab lights, fans, and computers at work, but often forget to turn them off after scheduled college / lab hours. This leads to excessive energy consumption and heating of the systems. Unauthorized users or intruders can easily and illegally enter the labs after college hours due to the lack of security in the labs. These people can illegally hack the university system's server and gain unauthorized access to confidential data by cracking passwords. The process is known as phishing, in which the intruder gathers critical credit information for financial passwords by electronically sending fake emails.

Intruders hack into the system, steal important data, and disappear. This results in a huge loss of university / laboratory data and the students suffer as a result. The labs need to be so secure that the guards need to be alerted if an intruder tries to enter the lab after college hours.

3. PROPOSED SYSTEM

There are 3 types of modules in this project:

- Work package 1
- Work package 2

- Work package 3

1) Work package 1

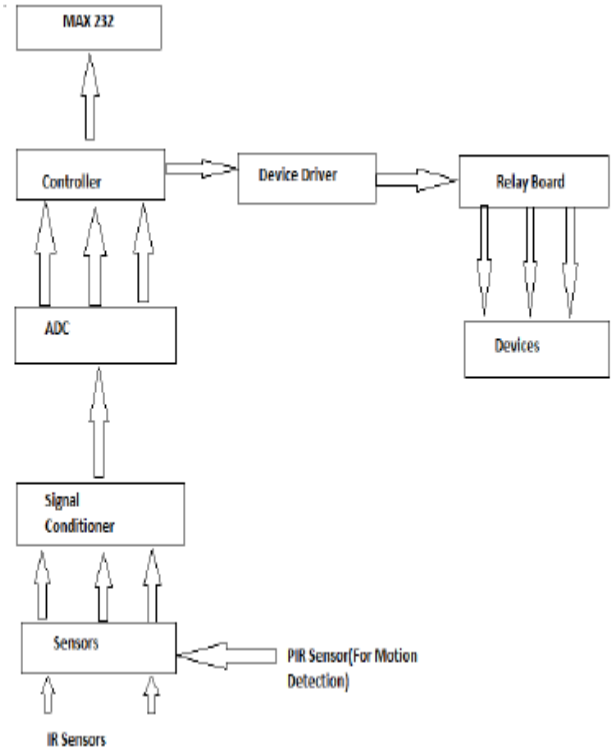


Fig. -1 : Work module 1

In this module, the hardware module contains the microcontroller, device drivers, serial communication, relay board, peripherals and sensors. The max. 232 cable is used for serial communication between the PC and the printed circuit board. Two types of sensors are used. Sensors) and PIR sensors IR sensors are used to track the number of people entering and leaving the laboratory. PIR sensors are used to detect movement in the laboratory in case there is an entrance other than the main entrance. There is also an ADC converter that converts the analog signals sent by the signal conditioner into digital signals. There is a 32-bit microcontroller that has high performance with low power during operation. The device works between 1.8 and 5.5 volts. ULN2003 is known for its high presence and high voltage limit. Drivers can be connected in parallel for an even higher current output. Rather, a chip was stacked on top of each other both electrically and physically .

It can generally be used to interface with a stepper motor where the motor requires high powers that other connection devices cannot provide. There is a relay board that has devices such as fans, lights, etc. installed on it. are connected. for its functionality. A device driver is attached to the relay card. Now this entire circuit board is connected to the PC database with a MAX 232 cable that is specially used for serial communication.

2) Work package 2

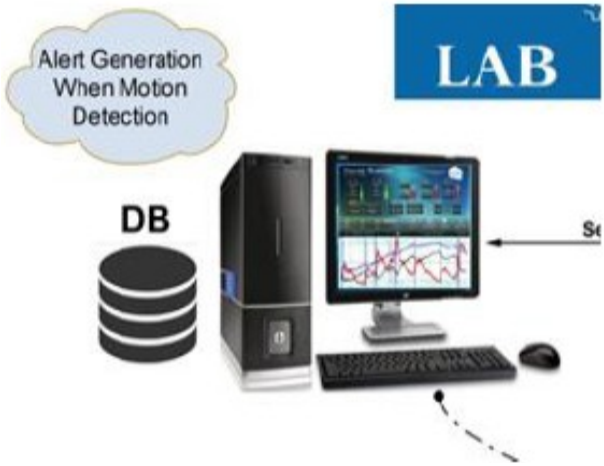


Fig. -2 : Work module 2

In this module, Glassfish is used as the database. It's a desktop application. This is connected to the circuit board via serial communication with a MAX 232 cable. The database checks the number of people entering and leaving the laboratory. It also checks the time, which is the time people enter and leave the laboratory. If movement is detected after the lab hours, a warning is generated and a corresponding warning message is sent to the laboratory manager.

3) Work package 3

Fig. -3 : Work module 3

In this module 2 concepts are described.

1. Remote monitoring and
2. Remote control.

These two concepts are often used to protect laboratories.

1) Devices (fans, lights, computers) can be controlled in the remote control, i.e. they can be switched on and off by an Android app using voice recognition. As soon as the laboratory manager enters the laboratory in the morning, lights, fans and other devices are switched on automatically thanks to voice recognition.

2) During remote monitoring, infrared sensors track people entering and leaving the laboratory. If the number is 0 there is no problem, but if the number is 1 there is a warning.

If there is unauthorized access in the lab or if movement is detected after the lab hours, an alert will be sent to the lab administrator on your Android phone via the Android app via WiFi.

4. RESULT ANALYSIS

In this project we will develop an Android application that will be made available to the laboratory assistant. The Android app offers the following functions:

1. Administrator login and authentication.
2. Voice command to control electrical appliances.
3. Android app and microcontroller connect via a server.
4. Infrared sensors for motion detection
5. In the event of theft, a warning SMS and an email are sent to the administrator.
6. An alarm SMS and an email will be sent to the administrator when a sensor value above the threshold is reached.

5. CONCLUSIONS

The laboratory is insured. If the fans and lights are on when staff and students are absent, they will turn off automatically. Any intruders can be detected with the help of motion detection sensors after the lab has been working. IR sensors (infrared sensors) monitor the number of people entering and leaving the laboratory. When an intruder walks in, the doorbells work automatically, alerting security guards and catching the intruder in the act trying to steal confidential information or hack into the system server.

REFERENCES

1. Nicholas Dickey, Darrell Banks, and Somsak Sukittanon ,“Home Automation using Cloud Network and mobile devices”.
2. Ranjith Balakrishnan and Pavithra.D,”IoT based Monitoring and Control System for Home Automation”.
3. James O. Hamblen, Senior Member, IEEE, and Gijsbert M. E. van Bekkum, Member, IEEE,” An Embedded Systems Laboratory to Support Rapid Prototyping of Robotics and the Internet of Things”,
4. IEEE Transactions on Education, Vol. 56, No. 1, February 2013
5. Rupali Shanbhag and Radha Shankarmani,” Architecture for Internet of Things to Minimize Human Intervention”.
6. Qingping Chi, Hairong Yan, Chuan Zhang, Zhibo Pang, and Li Da Xu, Senior Member, IEEE," A Reconfigurable Smart Sensor Interface for Industrial WSN in IoT Environment", IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, May 2014.

Sushant Kumar and S.S.Solanki,“Voice and Touch Control Home Automation”, 3rd Int’l Conf. on Recent Advances in Information Technology . RAIT-2016

ANT COLONY MODEL FOR SIMPLIFIED SECURITY SOLUTIONS IN CLOUD DATA PROTECTION

CH.Rajkumar[1]., K.Naga ramya[2]., T.Rohitha[3]., K.Dhana lakshmi[4]., M.Pravalika[5].,

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: chunchurajkumar@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0433, 17RG1A0458, 17RG1A0434, 17RG1A0441), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***After the invention of the cloud model, there was a growing awareness of storage sharing. When you invest in hardware to store large amounts of data and keep it safe in the cloud, you get simple solutions. Because of this, data storage in the cloud is increasing. The above algorithms for protecting data in the cloud are used to encrypt content without knowing the type of data. However, the proposed AnCoMoDaS (Ant Colony Model for Cloud Data Security) algorithm for encrypting content depends on the type of content available in the document. It has therefore been proven that the size and time are reduced compared to previous algorithms.***

Keywords: ant colony, encryption, cryptography.

1. INTRODUCTION

The cloud is nothing more than a group of servers and data centers in different locations. These servers and data centers are responsible for providing on-demand services to their users over the Internet. The service provided by the cloud does not exist on the user's computer. The user must access these services through a subscription internet connection. The main benefit of cloud computing is that it eliminates the need for the user to be in the same place as the hardware software and storage space physically resides. The cloud enables you to save and access your data from anywhere, anytime, without having to worry about maintaining hardware software and storage space. All of these services are made available to the user at a low cost. The user has to pay according to the storage space he uses. Thanks to this flexibility, everyone transfers their data to the cloud.

Cryptography is a technique of converting data to an unreadable format during storage and transmission that would seem unnecessary to an intruder. The illegible form of the data is known as ciphertext. When the data is received by the recipient, it appears in its original form, which is known as plain text. Converting plaintext to ciphertext is called encryption, and the reverse (ciphertext to plaintext) is called decryption. The encryption takes place on the sender side, while the decryption takes place on the recipient side.

2. RELATED WORKS

To ensure the data integrity of a file that consists of an ordered finite set of data blocks on a cloud server, Qian Wang et al. In [2] several solutions. The first simple solution to ensuring data integrity is for the data owner to precompute the MACs for the entire file with a set of secret keys before our data is sent to the cloud server. During the verification process, when the data owner reveals the secret key to the cloud server and requests a new MAC for verification. With this method, the confirmation number is limited to the number of secret keys. After the keys are exhausted, the data owner must fetch the entire file from the cloud server to calculate the new MACs for the remaining blocks. This method requires a lot of communication to verify the entire file, which affects the efficiency of the system.

Qian Wang et al. Developed in [4] an efficient solution to support the public examination function without fetching data blocks from the server. Designing dynamic data operations is a difficult task for the cloud storage system. They proposed an RSA signature authenticator for verification with dynamic data support. To help efficiently manage the multiple verification task, they developed the bilinear aggregated signature technique and then introduced an external reviewer to perform the multiple verification task at the same time. In the recent paradigm of resource sharing in

distributed systems like cloud computing, this is the most difficult task.

3. PROPOSED ALGORITHM

Figure 1 shows the complete architecture of the proposed algorithm.As in the architecture diagram, the contents of a particular document are read and the initialized ant is scanned, drawing all characters and increasing the promon for each character according to its type. Ultimately, the size of the promon indicates the type of encryption. Depending on the size of the promon, either character-based encryption or value-based encryption was carried out.

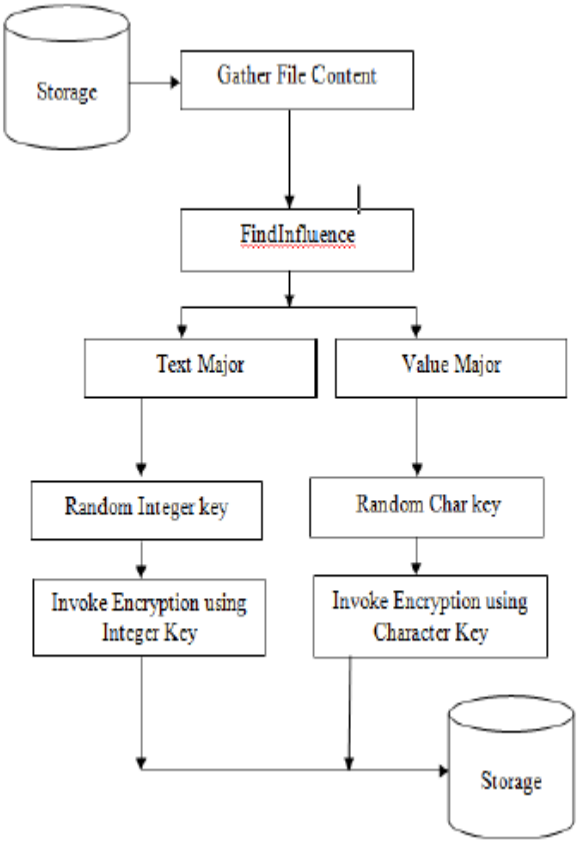


Fig. -1: Architecture diagram of the proposed algorithm

ALGORITHM 1
ANT COLONY MODEL FOR DATA SECURITY IN CLOUD

1. FC<=READ(File)
2. ET<=FINDINFLUENCE(FC)
3. If(ET equals "TM")
   EK=Random(Integer)
4. If(ET equals "NM")
   EK=Random(Char)
5. EF=Encrypt(FC,EK)

Where FC means File Content
ET means Encryption Type
"TM" means Text Major
"NM"means Value Major
EK means Encryption Key and
EF means Encrypted File

Fig 2: Algorithm 1 for Ant Colony Model

ALGORITHM 2
FINDINFLUENCE

1. Let ETA as Ant
2. For All Text
3. If Ant travel Character
   TPromon++
4. Else
   VPromon++
5. If TPromon>VPromon)
   Return "TM"
6. Else
   Return "NM"

Where ETA means Encryption Type Ant

Fig 3: Algorithm 2 – Find Influence

Algorithm 1's file line indicates that the contents of the file are being buffered for other operations. After the content has been buffered, the file is categorized regardless of whether it is a TEXT Major or a Value Major file. To do this, two ants are initialized and allowed to search through the entire buffered content. With each move, one of the two ants increases depending on the type of character. Finally, the case of the major text file encrypted with the text element based on the encryption and the major value file encrypted with the encryption based on the number. If both are the same and both are present,

encryption is called to give the content maximum security.

The result obtained with this algorithm shows that the size of the encrypted file is smaller compared to conventional encryption algorithms. A tool will be developed to show the accuracy of the proposed algorithm.

4. EVALUATION AND RESULTS

A file for checking the functionality of the proposed algorithm.

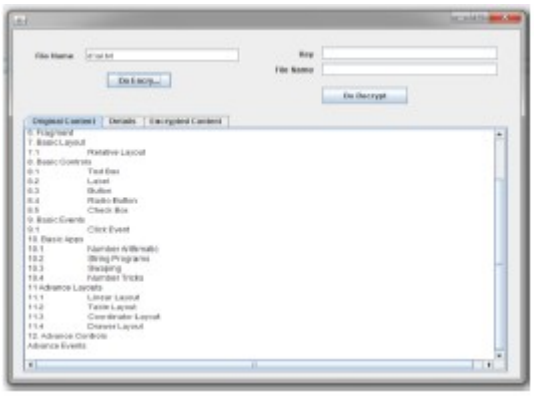


Fig 4: results are returned from the tool

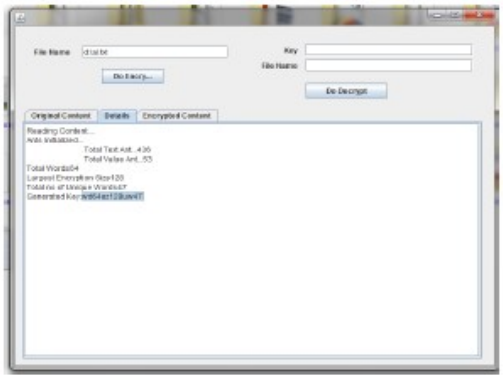


Fig 5: key generated by the proposed algorithm

The key generated by the proposed algorithm is highlighted in gray on the output screen to ensure a clear display.

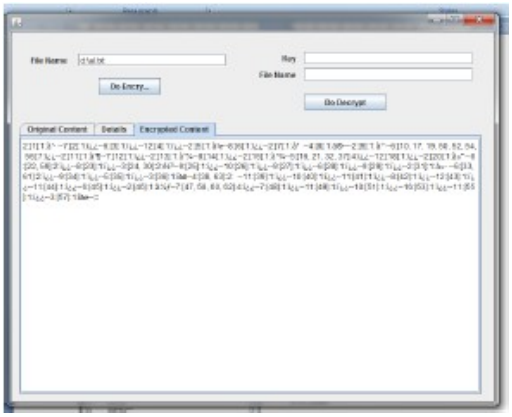


Fig: Encrypted content

5. CONCLUSION

This article explains the problem of data security in the cloud storage system. In order to control outsourced data and provide users with a high quality cloud storage service, we offer efficient data encryption using the Ant Colony model and cryptographic techniques. It is concluded that the proposed algorithm produces more secure encrypted content with reduced size and the time required is significantly shorter than previous conventional algorithms.

REFERENCES:

1. Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. (2011).
2. Cong Wang, Kui Ren, and Jia Wang, Secure and Practical Outsourcing of Linear Programming in cloud computing, In IEEE Internationa Conference on INFOCOM, pages 820-826, 2011.
3. Q. Wang, C. Wang, J. Li, K. Ren,and W.Lou, Enabling Public Verifi-ability and Data Dynamics for Storage Security in Cloud Computing, In Proceeding of 14th European Symposium, Research in Computer-Security (ESORICS 09), pages 355-370, 2009.
4. Neha Jain and Gurpreet Kaur, 'Implementing DES Algorithm in Cloud for Data Security', VSRD International

Journal of CS & IT. (2012), Vol.2 Issue 4, pp. 316-321.

Dubey A K, Dubey A K,Namdev M, Shrivastava S S, Cloud-user Security based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment, Software Engineering (CONSEG), CSI Sixth International Conference on, pages 18, September 2012

ANALYSIS OF DYNAMIC SUPPLY MANAGEMENT FOR SMART CITIES USING IOT IN SMART WASTE MANAGEMENT

K. Surekha[1]., G.Shivani[2]., T.Laxmi Priya[3]., S.Mounika[4]., CH.Manisha[5].,

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: surekhakorudu413@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0427, 17RG1A0457, 17RG1A0455, 17RG1A0411), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: Cities in the world place measure in no time to get smarter some of them have had the opportunity to implement dedicated municipal access networks to support all types of city management and maintenance services that require data affiliation from caregivers. However, we tend to show that integrating the network of things (IoT) with statistics between networks, geographic data systems (GIS), combinatorial improvements and digital engineering will help advance the management systems of cities. We tend to provide a sustainable answer to the waste range by throwing information into the trash, using some form of Image IoT combined with a care built into sensors that examine information about the volume of waste on the web and can transfer. These recordings, which are placed in a spatiotemporal context and processed by algorithms to improve graphical thinking, could also be used for the dynamic and efficient management of residual production techniques.

Keywords: waste assortment, smart city, network of objects (IoT), geographical data system (GIS), dynamic supply management, location information.

1. INTRODUCTION

We are currently witnessing the rapid development of wise cities in which engineers, town planners, architects and city administrators are changing the unity of integrity forces in order to increase the efficiency of municipal services and to increase the efficiency of municipal services. Blessings and luxuries for them groups. [1]. In this state, the measure of efficiency is usually associated with an oversized spectrum of things that resemble the extraordinary management of existence, economic system, property, or infrastructure. ICT have been suggested as key elements for wise cities / societies, despite the particular context or dreams of each provider, application or movement under that umbrella.

In this article we are inclined to explain, but Associate in Nursing has bypassed the craze for body cybernetic devices based solely on the blending of various technical disciplines, and an intelligent factor related to community wireless access to networks to an increase of smart approaches. City administration. The planned system is based on the inspiration of geostatistical structures (GIS), the graphic principle of improving graphics and searching for devices.

2. SYSTEM DESCRIPTION

2.1 Summary of functions

In simple terms, the planned garbage sorting machine is based entirely on level statistics of waste from trash cans located in an extremely metropolitan location. Recordings collected by sensors are sent over the Internet to a server, where they are stored and processed. The information collected is then used to monitor and optimize the daily selection of containers to be collected. The routes are therefore difficult. Employees record newly calculated routes from their navigation devices every day. The main feature of this device is that its miles are designed to be fun and allow choices not only in terms of the daily amount of waste but also in terms of target area prediction, congestion, functions with balanced value efficiency and other moving parts to meet. that parents cannot predict a priori. The value of the overflow measure for the garbage can is also fully analyzed on the basis of the old data and thus the expected overflow before it occurs. An optimized selection of the containers to be collected is planned in order to minimize and improve costs

3. PROPOSED SYSTEM ARCHITECTURE

The zero-waste approval claims are questioned, followed by a discussion of the

requirements in UL 2799. Adoption of the principles for the reduction, use, and recycling of zero-waste is believed to be essential to the value and effectiveness of any recycling effort. Companies. Achievement or anyone waiting for pre-defined financial desires. Figure 1 shows the analysis of the system.

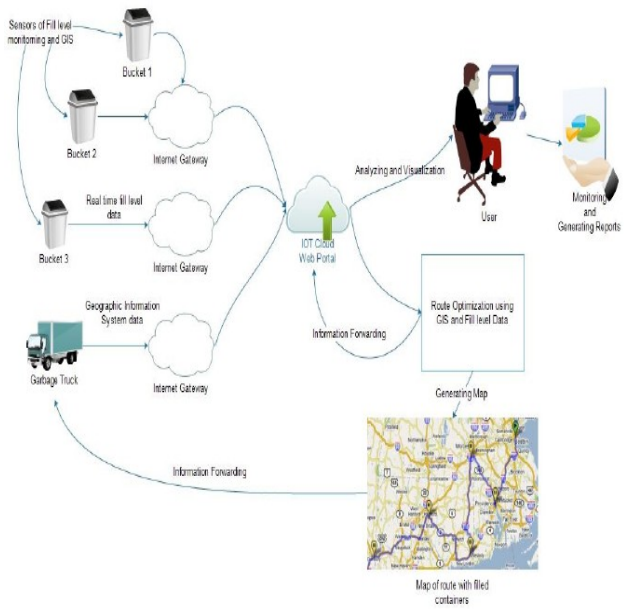


Fig. 1: System architecture

3.1 Recognition as a service model for good cities supported by the Web of Things:

Waste management is one of the toughest challenges fashion cities are likely to face. Waste management includes various processes such as sorting, transporting, treating, disposing, disposing and handling of waste. These processes add a significant amount of money, time, and labor to the value. Optimizing waste management processes is an easy way to save a lot of money to face the various challenges good cities can face. However, they illustrate that the detection-as-a-service model works in the field of waste management.

3.2 A review and evaluation of the algorithms for shortest paths:

From this work we tend to investigate that the most objective goal is to measure the Dijkstra algorithm program, the Floyd-Warshall algorithm program, the Bellman-Ford algorithm program, and the genetic algorithm (GA) in the resolution wrong side.

3.3 Disadvantage of transporting vehicles with various waste with time slots:

It is for this reason that the bias towards an irrefutable way of addressing the question of whether it is an inadmissible cost collection solution (VRPTW) related to the length of the visit is drivers. Solomon's well-known algorithmic inserter thrives on this problem. Although minimizing the number of cars and the total driving time is the main goal of driving problems in the literature, we tend here to consider more compactness of routes and a balance of workplaces. “An answer because these are important aspects in sensitive areas. Applications. In order to increase the compactness of the path and the equalization of employment, an algorithmic VRPTW waste sorting program based on an educated group is being developed.

3.4. Shortest path that covers the tree

This algorithmic program is used to calculate the shortest distance between 2 points in space (e.g. 2 trash cans) in combination with GIS information from city streets. The road network can be described as a graph in which the road segments measure the square edges and also the square connection points of the erasure vertices. Therefore, it is possible to calculate a shorter practical driving distance between the points by applying the SPST. Square distances are required as a related input to the route optimization method. For reasonable reasons, it is a good idea to recalculate the distance of all trash cans to speed up the route optimization method.

5. ANALYSIS

Calculation of the general prices of the 3 methods in A) over a period of two years (estimated based on the minimum battery life of the device). The total prices are the sum of the prices of the quantity (C) and the CapEx and OpEx of the system, as shown in Table 3

and the equations. Square measure (1a), (2a) and (2b) used for calculations. Las suposiciones creadas para el parámetro especificado son: Cdev = 20 USD per bote de basura, Cacc = 0, eq = 5000 USD, Cnet = 0, Cfal = 0, Cm = 11.4 USD per day, sys = 11.4 USD per day. The quadratic measure of Cm and Csys results from the fact that an employee spends eight hours a week on the task at a value of $ 10 / hour. Cacc, Cnet and Cfal squares are set to zero as examples of the use of municipal access networks and ICT infrastructure that are shared by all intelligent services provided on site. The results show that the implementation and maintenance of the system are associated with higher overall costs. Also, as performance improves, the value may be a limitation for city administrators or call managers to implement such a system.

$$C_i = C_{km}D_i + pC_wT_i \quad (a) \qquad T_i = \frac{p_i}{s} + t_cN_i \quad (b)$$

$$S_{CapEx} = C_{dev} + C_{acc} + C_{eq} \quad (a) \qquad S_{OpEx} = C_m + C_{sys} + C_{net} + C_{fal} \quad (b)$$

Method	C (k$)	S_{CapEx} (k$)	S_{OpEx} (k$)	Total Cost (k$)
Sectorial	568.88	0	0	568.88
Dynamic A	642.96	65.92	16.68	752.76
Dynamic B	715.31	65.92	16.68	797.91

Fig 2 Economic analysis of equal performance

The results discussed above clearly show that an increase in the survey methods through the use of an intelligent system of associate degrees can lead to financial costs. In this experiment, the dynamic methods agree with the modified flat-digit approaches to estimate their total prices as soon as they deliver similar figures of merit. The staggered planar figure approaches the square dimension that is created by more and more reducing the number of groups per team from seven to six, five and four. As the diversity of groups decreases, the containers in which they are collected become more common. The scope of the experiments was limited to the first team with 291 containers due to the high procedural resources required to examine the entire city. However, the results are indicative of the impact of the modified SWAps on the situation.

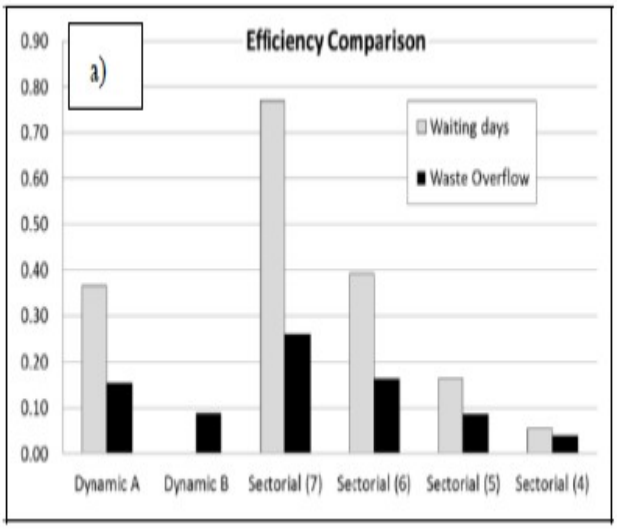
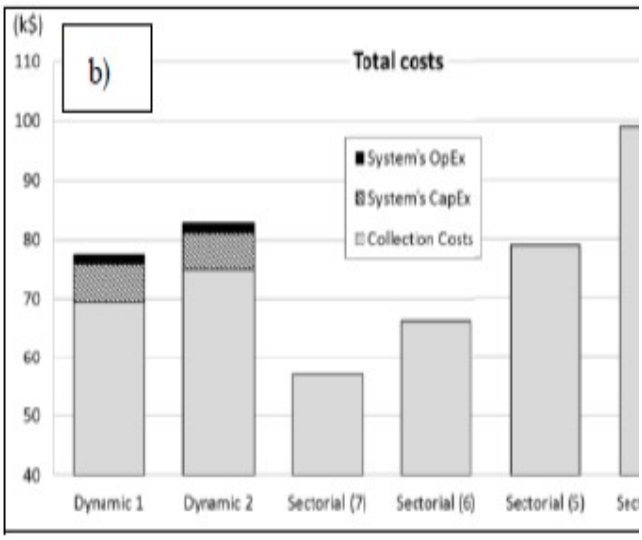


Fig 3Efficiency comparison for devices 1

Figure 3 shows the average number of days waiting for collection when the bins are full and the waste overflow (in% of bin capacity) for the above cases. We see that the same residual overflow for dynamic B can be obtained by applying the sectoral approach to 5 clusters. However, the waiting times do not become 0 for any of the sector strategies. Therefore, it can be assumed that the degree of effectiveness of Dynamic B can (to some extent) be comparable to sectoral strategies with 4 to 5 clusters.

Figure 4 shows the cost comparison for the different cases examined after 2 years. The SCapEx and SOpEx values for Team 1 are calculated proportionally to the number of containers compared to the total number in the city (ratio 291/3046). The results shows that the savings achieved by applying Dynamic Strategy B can offset (or close to) additional costs for the implementation and maintenance of the system compared to sectoral approaches with similar efficiency (4 to 5 clusters) per team. Therefore, it can be concluded that

similar efficiency in the cases studied may mean similar overall costs, whether or not an intelligent waste collection system is used.



b) Comparison of the total costs for team 1 after 2 years

6. CONCLUSION

The system is based on an outstanding things recognition network that measures the amount of waste in garbage cans and sends this information over the network to a server for storage and processing. Based on this information, an improvement method makes the assortment routes more efficient and these divisional units are sent to the employees. Their goal is the efficiency and economy of the system in order to induce potential stakeholders to implement intelligent solutions for common municipal services. The experimental area has dispensed with a simulation environment for geographic information systems that uses algorithms to improve graphics and uses open and accessible information about the city. The results show that, under identical conditions, using waste collection forms on the real-time ash collection improves waste collection efficiency by ensuring that once the bins are full, they are collected on the same day and the residue is reduced by one in four . Overflow that cannot be picked up once the garbage room unit is full. However, the gap required to drive triples, implying an increase in the NA value of the daily supply between thirteen and twenty-five.

REFERENCES

Petit, J., Experiments on the minimum linear arrangement problem, Sistemes Informatics, 2001., vol. 8, pp. 112–128, 2001.

Gutierrez J. M., Imine M., and Madsen O. B., Network planning using GA for regular topologies, Proceedings of IEEE International Conference on Communications, ICC 2008, Beijing, China, 19-23 May 2008, pp. 5258–5262, 2008. Kunzmann K.R., Smart Cities: A New Paradigm of Urban Development. Crios, 1/2014, pp. 9-20, doi: 10.7373/77140

Komninos, N., Intelligent Cities: Innovation, Knowledge Systems, and Digital Spaces, 2002, Spon Press

Spira, P. M., and Pan On, A., Finding and Updating Spanning Trees and Shortest Paths. SIAM Journal on Computing 1975 4:3, 375-380

Steinbach M., Karypis G. and Kumar V., A Comparison of Document Clustering Techniques, KDD Workshop on Text Mining, 2000

Vicentini F., Giusti A., Rovetta A., Fan X., He Q., Zhu M., Liu B., Sensorized waste collection container for content estimation and collection optimization, Waste Management, Volume 29, Issue 5, May 2009, Pages 1467-1472, ISSN 0956-053X.

MANAGING QUALITY OF EXPERIENCE (QOE) FOR END USERS IN WIMAX NETWORK USING FREEWAY MODEL AND SCHEDULING ALGORITHM

Y. Kalavathi[1]., B.Akhila[2]., Christy mary bose[3]., M.Harshitha[4]., T.Sruthi[5]

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: vimireddy.kalavathi.@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0408, 17RG1A0413, 17RG1A0494, 17RG1A04A8), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***The global interoperability of microwave access networks (WiMAX) should be the primary BWA (Broadband Wireless Access) technology, which provides various services such as data, voice and video services including various QoS (Quality of Service) classes was established by the IEEE 802.16 -Standard defined. WiMAX programming has become one of the toughest problems. During the current centenary, the performance of wireless technologies has increased. QoS was introduced in WiMAX. It can meet the QoS requirements for a wide variety of applications and data services, especially with high-speed connectivity, asymmetric capacities, and flexible resource allocation mechanisms. Some services are very demanding, VoIP cannot tolerate delays in data transmission. The concept of QoS clearly depends on the service under consideration, its response time requirement, its sensitivity to transmission errors, and so on. For video transmission, we need a transmission in almost real time with very low latency and little jitter. Network delays and retransmissions not tolerated during VoIP traffic.***

Keywords: QoE, WiMAX, QoS, VoIP, QoE2M.

1. INTRODUCTION

An everyday mobile user needs more services provided by wireless carriers for daily activities and entertainment. This requirement requires higher network performance to provide similar services that are provided by landline networks.The network has been objectively examined by evaluating a number of parameters to assess the quality of the network service. This assessment is known as network QoS. It refers to the network's ability to achieve more deterministic performance. Therefore, data can be transported with minimal packet loss, minimal delay, and maximum performance. QoS does not take into account the user's perception of the service provided. Another approach that takes into account the user's perception is known as QoE. It is a subjective assessment that associates human dimensions. brings together the perception, expectations and user experience of application and network performance. To understand the quality perceived by end users, QoE has become a very active research area. Much related work has been published on QoE analysis and enhancement of the WiMAX network. The study proposed a method for estimating QoE metrics based on QoS metrics in the WiMAX network. The QoE was assessed using the free way model. The results show an efficient estimate of the QoE metrics based on the QoS parameters.

2. METHODOLOGY

QUALITY OF EXPERIENCE

Quality of Experience (QoE) is a subjective assessment of a customer's experience with a service, focuses on the entire service and includes subjective human perception. QoE is in part related to QoS and these are two complementary concepts.

QoS and QoE are ambiguous terms that are sometimes used interchangeably. It is good to redefine the terms QoS and QoE. QoE refers to QoS, but differs from QoS, which tries to objectively evaluate the service provided by the provider, with the measurement of QoS mostly not related to the customer but to the hardware and / or software. QoS ensures the proper delivery of sensitive network traffic such as voice or applications. With the rapid development of multimedia applications, QoS metrics such as bandwidth, delay, jitter, and packet loss cannot assess the subjectivity associated with human perception, and hence QoE was born, which is a measure of the

user's personal judgment based on their own Experience is. In fact, Dr. Donald Norman first introduced the concept of user experience and referred to the importance of designing a user-centered service [18]. Gulliver and Ghinea [11] divide QoE into three components: assimilation, judgment and satisfaction. Assimilation is a quality measure for the clarity of content from an informative point of view. The quality rating reflects the quality of the presentation. Satisfaction indicates the level of general appreciation for the user.

3. PROPOSED PLANNING ALGORITHM BASED ON QOE

The proposed QoE-based planning algorithm is based on two QoE requirements. Each user has an initial maximum transfer rate and a minimum subjective rate requirement. The scheduler works as follows: Each node begins to send data traffic at the maximum speed. If a particular user experiences a packet loss, the system checks for each user whether the transmission rate is greater than the subjective minimum requirement. In this case the transfer rate is reduced, otherwise the transfer is continued with the same direct debit. The bit rate returns to the original maximum value during the simulation. It rests every 20 seconds. It is observed that it takes all users 18 seconds to reach the minimum transfer rate. The figure shows the activity diagram of the proposed programming algorithm.

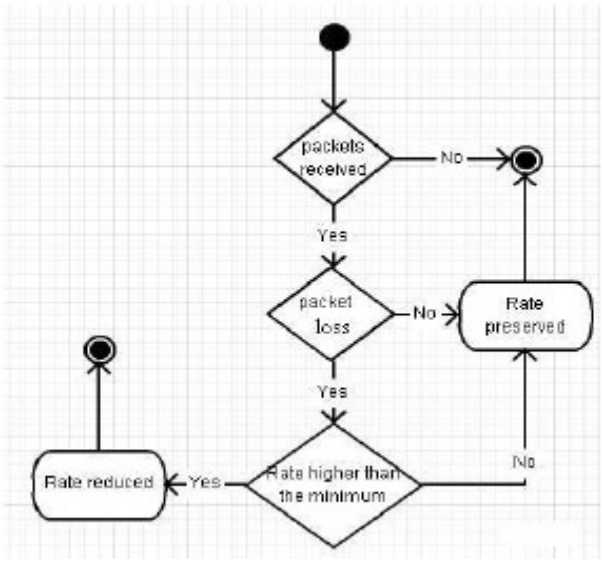


Figure 1: Activity diagram of the proposed QoE-based planning algorithm

3.1 Simulation Environment

In this article, we analyze the performance of the proposed QoE-based scheduling algorithm. Since we are looking at the wireless OFDM PHY layer, our QoE-based scheduling algorithm is compared to the famous WiMAX module developed by the NIST (National Institute for Standards and Technologies), which is based on the IEEE 802.16 (802.16-2004) and Mobility Extension (80216e-2005) provides a number of features including the OFDM PHY layer. The network simulator (NS-2) is used. Our simulation scenario consists of creating five wireless nodes (SS, subscriber stations) and connecting them to a BS. A receiving node is created and connected to the base station to accept incoming packets. A traffic broker is created and then attached to the source node. Finally, we configure the traffic generated by each node. The first node operated with a CBR packet size (constant bit rate) of 200 bytes and a range of "0.0015", the second node operated with a CBR packet size of 200 bytes and a range of "0.001". The third node was The fourth node was running with a CBR packet size of 200 bytes and a range of "0.001", the fourth node was running with a CBR packet size of 200 bytes and a range of "0.001" and the fifth node was II with a CBR

packet size of 200 bytes and an interval of "0.0015". The initial transmission speed generated by each node is approximately "133.3 Kbit / s", "200 Kbit / s", "200 Kbit / s", "200 Kbit / s" and "133.3 Kbit / s", respectively. s ". All nodes have the same priority.

Every user has a minimum requirement, so the first user needs a minimum traffic rate of "120 Kbit / s", the second "150 Kbit / s", the third "150 Kbit / s", the fourth "150 Kbit / s" and the fifth "120 Kbit / s".

Traffic rate / Users	Initial traffic rate (Kbps)	User m require (Kbps)
User 1	133,33 (200byte/0. 0015)	120
User 2	200 (200byte/0. 001)	150
User 3	200 (200byte/0. 001)	150
User 4	200 (200byte/0. 001)	150
User 5	133.33 (200byte/0. 0015)	120

Table 1: User Traffic Parameters

The NS-2 network simulator was used to perform this simulation. We implemented the WiMAX module included in QoS in NS-2. This module is based on the NIST implementation of WiMAX and consists of adding QoS classes and managing QoS requirements. The resulting trace files are interpreted and filtered based on a PERL script. This is interpretation script software that extracts data from the trace files related to performance, packet loss rate, jitter, and delay. The extracted analysis results are recorded with the EXCEL software.

B. Simulation parameters

The same simulation parameters are used for planning algorithms based on NIST and QOE

Parameter	Value
Simulator	NS-2 (Version 2.29)
Network interface type	Phy/WirelessPhy/OFDM
Propagation model	Propagation/OFDM
MAC type	Mac/802_16/BS
Antenna model	Antenna/OmniAntenna
Service class	BE
packet size	200 bytes
Frequency bandwidth	5 MHz
Receive Power Threshold	2,025e-12
Carrier Sense Power Threshold	0,9 * Receive Power Threshold
channel	3,486e+9
Mobility Model	ManhattenGrid
Speed	15 m/s
Simulation time	200s

Table 2: Simulation Parameters

4. RESULTS AND ANALYSIS OF THE SIMULATION

In this section we present the results of simulations for the two traffic scenarios considered, which reflect the performance of the algorithm of the QoE-based scheduler and the NIST scheduler in terms of average throughput, packet loss rate, delay, medium and mean jitter. the WiMAX network with BE. Service class. Figure 2 shows the average performance values of the two modules considered in our simulations. It is observed that the average performance values using the WiMAX module are higher than those of the module using the mechanism proposed for all flows. In fact, the QoE-based mechanism controls the transmission speed so that different users adapt to the minimum subjective requirements of each user, with the main goal of reducing network congestion and thus delay, jitter and transmission rate.

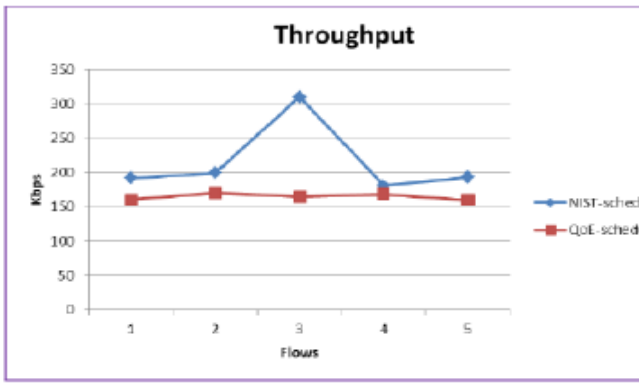


Figure 2. Average performance at speed / fixed 15 m / s

Figure 3 shows the improvement in packet loss rate by applying a QoE-based scheduler algorithm for all flows. In general, the rate of packet loss is reduced. In the case of Stream 4, the values are similar

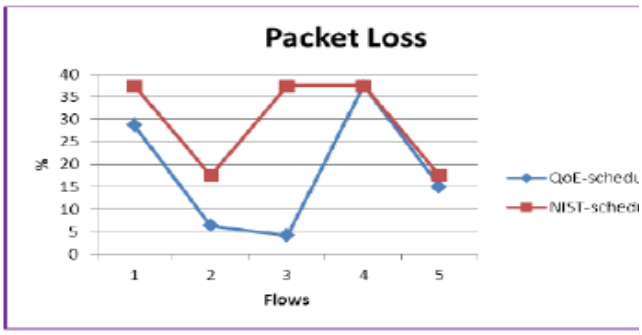


Figure 3. Fixed speed packet loss rate / 15 m / s

In Figure 4 it can be seen that the proposed mechanism based on QoE is more efficient in terms of average jitter compared to the WiMAX module. Indeed, the average jitter values that correspond to the proposed mechanism are lower than that of the WiMAX module.

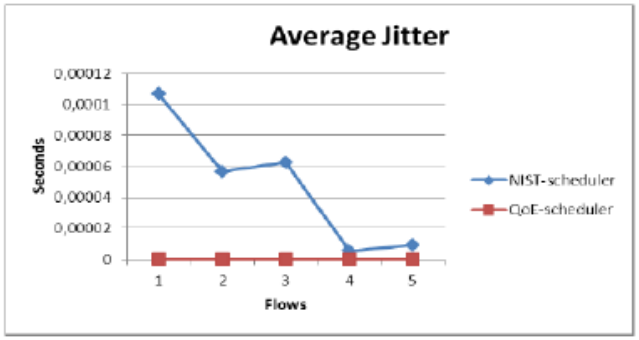


Figure 4. Average jitter at speed / fixed 15 m / s

As we can see in Figure 5, the average packet transmission delay is reduced by the QoE based mechanism. In the case of currents 4 and 5, the two modules give similar average delay values.

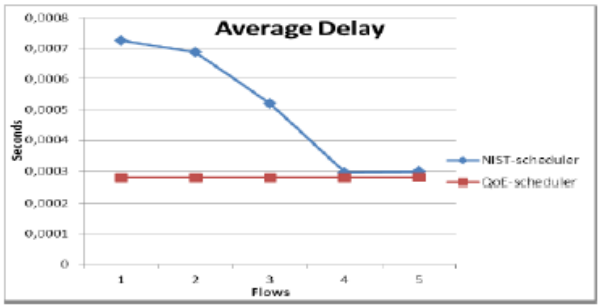


Figure 5. Average deceleration under the speed / fixed 15 m / s

5. CONCLUSION

In this article we have used a QoE-based scheduling algorithm where, depending on whether there is packet loss or not, the system will reduce the baud rate of each connection to meet the baud rate requirement. Minimum allowed (subjective minimum requirement of the user)). The simulations performed show that the use of different MOS levels improves the QoE made available to users of the WiMAX network. The proposed QoS-based scheduling algorithm significantly reduces packet loss, jitter and delay when using the UGS class of service. In future work we can extend this study to include other classes of service and

other subjective parameters for managing VoIP traffic.

REFERENCE

1. Belghith, L. Nuaymi "Design and Implementation of a QoS-included WiMAX Module for NS-2 Simulator",
2. SIMUTools 2008, Marseille, France, March 3-7, 2008.
3. P. Brooks, B. Hestnes,"User measures of quality of experience:Why being objective and quantitative is important". IEEE Network 24(2): pp. 8–13, 2010.
4. P. Calyam, P. Chandrasekaran, G. Trueb, N. Howes, R. Ramnath, D. Yu, Y. Liu, L. Xiong, &D. Yang, "Multi-Resolution Multimedia QoE Models for IPTV Applications", Volume 2012, Article ID 904072, 13 pages doi: 10.1155//904072, 2012.
5. Z. Abichar, Y. Peng and J. Morris Chang, "WiMax: The Emergence of Wireless Broadband", IT Professional,
6. Vol. 8, Issue. 4, pp. 44-48, Doi:10.1109/MITP.2006.99 July-Aug. 2006
7. M. Alreshoodi, J. Woods, "Survey on QoE\QoS Correlation Models for Multimedia Services", International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.3, May 2013.
8. T. Anouari and A. Haqiq, "A QoE-Based Scheduling Algorithm for UGS Service Class in WiMAX Network", International Journal of Soft Computing and Engineering (IJSCE) ISSN 2231-2307, Volume-4, Issue-1, March 2014.

H. Du, C. Guo, Y. Liu& Y. Liu, (2009)"Research on Relationships between QoE and QoS based on BP Neural Network", In: Proceedings of IC-NIDC, pp. 312-315, 2009.

IMPLEMENTATION OF AGILE SOFTWARE METHODOLOGY IN MEDICAL COMPUTING AND DEVICES IN HEALTHCARE INDUSTRY

K. Manasa[1]., M.Pravalika[2]., D.Sravani[3]., R.sandhya rani[4]., T. S.Shirisha[5].,

1Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (:manasareddy.@mrcew)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0441, 17RG1A0417, 17RG1A0450, 17RG1A0456), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***One of the most common models for software development is agile methods. The main reason for using Agile is that if the requirements are unclear, they can be adopted and the software can be developed without too many errors. It promotes organization, progress, early delivery and constant change and enables a quick and adaptable reaction to change. These standards support and promote the further development of many methods for product improvement. However, the use of agile methods in critical systems such as the medical industry is very low. Agile methods can be used in the medical industry because the requirements for developing a device may not initially be clear and the system must be risk-free. The agile method discusses the barriers to using the method and how to remove them.***

Keywords : agile software methodology, medical IT, scrum, etc.

1. INTRODUCTION

The medical industry is the branch that offers services for the palliative, curative and preventive treatment of patients. This is due to its great importance in saving people's lives. Technology plays an important role in the whole field and is also part of the critical systems for life. Many devices are used in the medical industry that are controlled by software devices. . A small delay in providing incorrect information or delivering a message can cost you your life. The medical industry is concerned with human life and must therefore be treated with extreme caution and care. The best medical industry can be supplied with reliable software. Agile methods can be used to develop medical devices. It can be used in emergency services to identify limitations of the existing system, increase transparency and improve collaboration between people. Developing software for critical systems is difficult because it must save lives.

1.1 Types of software engineering methods:

Waterfall Model: The waterfall model is a rolling diagram in which the layout is viewed as a cascade through the organization, review, planning, execution, and testing phases. Problems such as lengthy and indistinct requirements in the early stages are seen as obstacles to the waterfall model. Because of these problems, new waterfall models are used.

Iterative model: In this model, the entire life cycle consists of a few focal points. The cycle consists of two or three exercises: organize, examine, plan, use, and test. Towards the end of the cycle there should be an accent transfer which is mainly the accent discharge. Most accent downloads are done indoors. The final focus is the finished article.

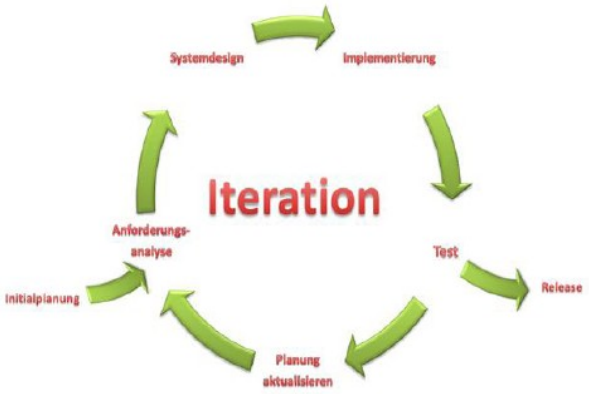


Fig 1 Spiral model

Spiral model: The model identifies an arrangement of standards and practices that implies a limitation of the documentation exercises. The main goal of a spiral pattern is to do the exercises with highly polished skill and less effort and ratio forward. The significant favorable position in using a model is the improvement time. The importance of this approach lies in your high learning and experienced group needs.

2. PROPOSED SYSTEM

2.1 Development of the V Agile model

The path to building the Agile V-Model is divided into clear and indisputable phases:

- Determination of the SDLC according to the facility plan;
- Planning to incorporate skillful practices into the plan powered by SDLC;
- Obvious evidence of skillful material practices through
- Improving the programming of medical devices.

2.2 Selection of the SDLC using the personnel table: When selecting the facility for the SDLC mix, several SDLC were analyzed using the table. It was concluded that the V-model is the most suitable model for making half and half of the SDLC. The explanations for choosing the V model are:

Associations for programming medical devices often follow the V-model for creating therapeutic device programs. Hence, from now on they are familiar with the structure and periods of the V-Model and would be more willing to take an average show of one and a half to prepare for an SDLC that they are natural with. Medical device programming associations may have received administrative assistance to adopt the V-Modell in creating the restorative device programming. In the event that these mappings are moved to a completely single SDLC, they may need to reapply for regulatory approval for the new SDLC.

2.3 Prepare to include agile practices in the plan

Driven SDLC: Any successive bay driven SDLC has the problem of being inflexible and determined to make changes. Iterative procedures allow changes to be familiarized with an extension extension without waiting to return to several different phases of the SDLC. The cycles that present the greatest risk are run as far ahead of schedule at this point as the business can imagine. If a randomly identifiable test is included, each phase of the V-Modell is evaluated to determine which steps could be performed iteratively. As a result, most stages of the progress lifecycle are divided into two classes: fixes that can be done iteratively and steps that need to be done in a single step.

2.4 Identify appropriate business practices for the

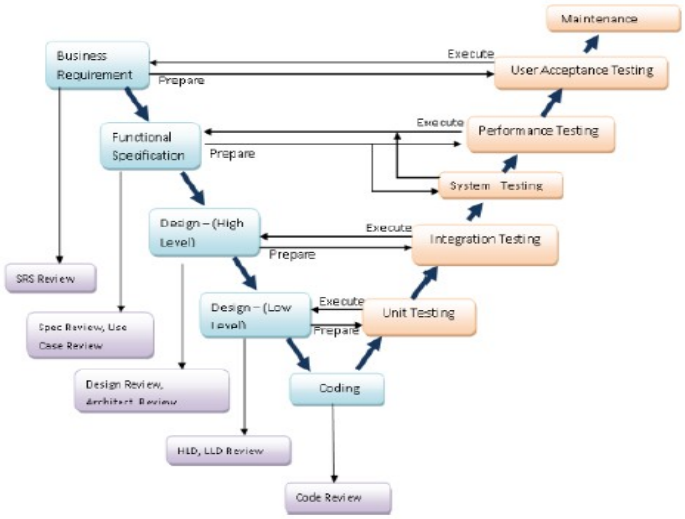


Fig 2 Progress in programming therapeutic devices:

The improvement in medical device programming was verified using each of the following techniques: Scrum, XP, DSDM, and Crystal Clear. . These three practices were then assigned to the appropriate phase of the SDLC. A problem when moving to a contract-based SDLC. This can happen if a change occurs after the upgrade has started. Through iterative improvement, point-to- point requirements can be efficiently reversed, and if an adaptation is made to the requirements, that change can be suitable for a promising cycle. The ongoing investigation will determine how many remaining practices are appropriate to advance medical device programming. Some of the other practices that are checked for relevance include continuous improvement, de facto relevance, and evidence-based development.

2.5 Display validation

The aim of improving this model is to solve the problems associated with the introduction of contract-driven planning progress while taking advantage of the use of agile practices. As the model is under development, it has not yet

been fully approved. There are two phases during the approval period: Expertise and Implementation. The further development of the AV model takes place iteratively. Once the approval phase is complete, the input is connected and the model proceeds to the next approval phase. The information is captured using a synthesis tool with open questions filled in.

2.5.1 Expert opinion: As soon as the model has received the approval customary in the industry, it is passed on to specialists in the field of further development of the programming of therapeutic devices.

2.5.2 Implementation: A medical device programming association has agreed to update the template once it has been fully completed and submitted to each of the approval media.

2.5.6. Advantages

- Scalability is important for associations to manage large amounts of information and contain costs.
- Compliance is important for health sector associations to refrain from deliberate principles that could result in costly punishment, death or actual harm to patients.
- Agility the ability to adapt to change and enables companies to adapt new metrics without making costly breakthroughs.
- Access to the information that is available everywhere improves the joint effort within the association.

3. RESULTS ANALYSIS

3.1. Change of requirements / changes:

Testers need to be able to respond to changes because changes are inevitable. As the requirements change, especially in the middle of the sprint end when there isn't enough time to run the tests correctly, the analyzers need to be clear about which tests are running and which part of the application has not been tested well in order for the group to have an informed Decision can be made (possibly in terms of risk) whether or not to download the article.

3.2. There is no clear information:

Evaluators should begin testing by considering unusual situations in which the business idea is being tested, rather than waiting for complete information about the component. When recording test situations with abnormal conditions, the settings should be the same even if subtle things change.

3.3. Complete test:

The tester should begin experimenting so that if the object is accessible for testing, he can begin testing immediately. Testers should encourage engineers to gain greater visibility by regularly setting the test conditions under which to run tests rather than waiting for the component to be fully built. We should mechanize relapse testing to improve some of the testing effort and free up our time for exploratory testing.

3.4. Technical / automation skills:

One should understand how each of these tools does programming, and you will find that you can get help from engineers. Part of extremely useful devices like selenium and JMeter and so on.

3.5. Communication problems:

In order to overcome these situations, there should be better communication between the teams. There must be constant collaboration with the developer and the owners of the items.

4. CONCLUSION

The integration of agile practices can lead to devices being developed for the healthcare industry. Medical devices and model improvements are subject to administrative controls. A standard agile method may not be suitable for creating medical device programming. The benefit can be achieved by linking different practices with a matrix-driven programming progress lifecycle. Further development of a V-model with spiral practices is beneficial for improving medical device programming. To configure this, the practices need to be integrated into the V-Modell, each practice in each of the agile practices, i.e. H. Scrum, XP, Test Driven Development, Crystal etc. When the match is resolved, the best

practices are incorporated into the custom V-Modell. The V-Modell is created in collaboration with medical programming associations. Once the V-model is ready, the industry will fully test it. Once this model is established, the goal is to have a fully built medical device programming trailer based on the finished V-model.

REFERENCES

1. Adopting Agile Practices when Developing Medical Device Software M Mc Hugh, F McCaffery, G Coady - 2015
2. Integrating agile practices with a medical device software development lifecycle ,M Mc Hugh, F Mc Caffery, V Casey, M Pikkarainen - 2012
3. A New Proposed Software Engineering Methodology for Healthcare Applications Development, Abdullah AlDahmash, Samir ElMasri Department of Information Systems, College of Computers and Information Sciences.King Saud University, Riyadh, KSA.
4. Martin Mc Hugh, Fergal Mc Cafferyand Valentine Casey Regulated Software Research Group, Department of Computing and Mathematics Dundalk Institute of Technology, Co. Louth Ireland.
5. An Introduction to Agile Software Development by Victor Szalvay, co-founder Danube Technologies, Inc. Bellevue. Whitepaper Medical Technology3 reasons for introducing agile product Development in medical technology.

REAL ORDERING OF RELEVANT RESULTS FROM USER-GENERATED CONTENT

T Sudha[1]., C Umadevi[2]

1 Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- sudhathulluri@gmail.com)

2 Professor, Department of H&S., TKR College of Engineering and Technology Saroornagar, Hyderabad, TS, India

ABSTRACT: ***A growing trend in information systems is crowd sourcing, understood to be the systematic engagement of humans within the resolution of tasks through online distributed work. When data ambiguity can't be reduced algorithmically, crowd sourcing proves a practical approach, featuring its posting tasks to humans and harnessing their judgment for increasing the confidence about data values or relationships. The most popular sign of both sensor data and user-generated submissions are their uncertain nature, because of either the noise natural in sensors or even the imprecision of human contributions. The creation of humans is uncertain, too, and therefore additional understanding should be correctly integrated, particularly by aggregating the responses of multiple contributors. These comes down to asking many questions which are irrelevant for that top-K prefix, given that they could involve tuples which are rated in lower positions. The wasted effort grows tremendously because the dataset cardinality grows. Several offline an internet-based methods for addressing inquiries to an audience are defined and contrasted on synthetic and real data sets, for the exact purpose of minimizing everyone else interactions necessary to obtain the real ordering from the result set. The aim of this paper would be to define and compare task selection policies for uncertainty reduction via crowd sourcing, with focus on the situation of top-K queries. We define and contrast several measures of uncertainty, either agnostic or determined by the dwelling from the orderings. We formulate the issue of Uncertainty Resolution poor top-K query processing over uncertain data with crowd support.***

Keywords: top-K query, Uncertainty Resolution (UR), Crowd sourcing, data ambiguity.

1. INTRODUCTION:

Within the well-known type of applications generally known as “top-K queries”, the aim is to get the best K objects matching the user’s information need, formulated like a scoring function within the objects’ attribute values. Querying uncertain data has turned into a prominent application because of the proliferation of user-generated content from social networking as well as data streams from sensors [1]. In addition, uncertainty might also be a consequence of the user’s information need itself This paper tackles the issue of processing top-K queries over uncertain data with the aid of crowd sourcing for rapidly converging towards the real ordering of relevant results. A viral advertising campaign may attempt to find out the “best” K users and exploit their prominence to spread the recognition of the product. For this reason redundancy, significant budget savings might be achieved by staying away from to publish even a tiny bit of tasks. This issue requires a suitable policy within the formulation from the tasks to undergo everyone else, targeted at reaching the utmost decrease in uncertainty using the tiniest quantity of crowd task executions.

Literature Survey: Crowd sourcing can be used to construct a tree in which the root represents a preliminary status, leaves represent a set objective and every path represents a string of actions to become performed in order to satisfy the objective. a strategy that mixes test inquiries to remove spammers, majority voting to enhance the precision of single workers and estimation of probability error according to task difficulty. A question language where questions are requested to humans and algorithms is described humans are assumed to continually answer properly, and therefore each real question is requested once [2]. The standard score to have an uncertain top-K query on the probabilistic database is computed. An audience of noisy workers and tuples whose scores are totally uncertain. This method doesn't lend itself well to the scenarios, where prior understanding around the score pdf’s is assumed. When addressing a high-K query, their method first disambiguates an order of all of the tuples by asking them questions towards the crowd, after which extracts the very best-K products. This comes down to asking many questions which are irrelevant for that top-K prefix, given that they could involve tuples which are rated in lower positions. The

very best-K tuples are determined using a voting mechanism that refines the group of top-K candidates after each "roundtrip" of tasks, until only K tuples remain. The authors propose an assorted online nd offline approach, in which the selected sequence of questions is annotated partly by machines and partly by users, and minimizes the amount of questions clarified by humans.

2. EXISTING SYSTEM:

Query processing over uncertain data is becoming an energetic research field, where solutions are now being searched for to help with the 2 primary uncertainty factors natural within this type of applications: the approximate nature of users' information needs and also the uncertainty surviving in the queried data. In existing system, the standard score to have an uncertain top-K query on the probabilistic database is computed. Furthermore, the authors address the issue for cleaning uncertainty to enhance the caliber of the query answer, by collecting multiple occasion's data in the real life, in order to confirm or refute what's mentioned within the database.

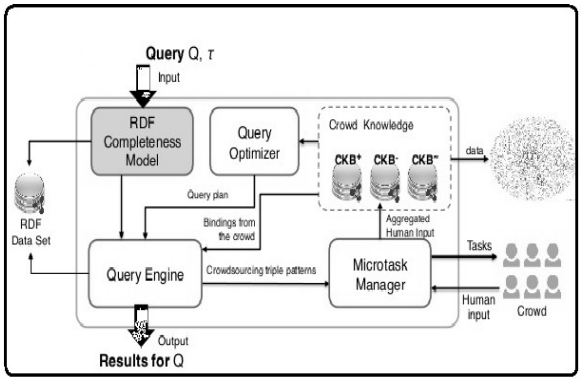


Fig.1.Proposed UR scheme.

3. UNCERTAINTY RESOLUTION POLICY:

Framework: We introduce two groups of heuristics for question selection: offline, where all queries are selected just before getting together with everyone else, an internet-based, where crowd solutions and question selection can intermix. We formalize a framework for uncertain top-K query processing, adjust to it existing approaches for computing the potential orderings, and introduce a process for removing unacceptable orderings, given new understanding around the relative order from the objects [3]. The aim of this paper would be to define and compare task selection policies for uncertainty reduction via crowd sourcing, with focus on the situation of top-K queries. Given an information set with uncertain values, our objective would be to pose to some crowd the list of questions that, inside an permitted budget, minimizes the expected residual uncertainty from the result, possibly resulting in a distinctive ordering from the top K results. We concentrate on the situation by which fi represents a continuing random variable, that the more discrete situation could be derived. Real datasets are frequently characterized by tuples whose score uncertainty can't be symbolized having a uniform distribution. We advise an formula that avoids the materialization from the entire space of possible orderings to attain even faster results The uncertain understanding from the scores induces an incomplete order within the tuples. The synthetic datasets contain collections of tuples with uncertain scores.

Implementation plan: Within this paper we've introduced Uncertainty Resolution, the problem of identifying the minimal list of questions to become posted to some crowd to be able to lessen the uncertainty within the ordering of top-K query results. The primary contributions from the paper are listed below: We formalize a framework for uncertain top-K query processing, adjust to it existing approaches for computing the potential orderings, and introduce a process for removing unacceptable orderings, given new understanding around the relative order from the objects [4]. We define and contrast several measures of uncertainty, either agnostic (Entropy) or determined by the dwelling from the orderings. We formulate the issue of Uncertainty Resolution (UR) poor top-K query processing overrun certain data with crowd support. The UR problem comes down to identifying the shortest sequence of questions that, when posted towards the crowd, ensures the convergence to some unique, or at best more determinate, sorted result set. We introduce two groups of heuristics for question selection: offline, where all queries are selected just before getting together with everyone else, an internet-based, where crowd solutions and

question selection can intermix [5]. For that offline situation we define a relaxed, probabilistic form of optimality, and exhibit an formula that attains it too as sub-optimal but faster algorithms. We generalize the algorithms towards the situation of solutions collected from noisy workers. Benefits of suggested system: We reveal that no deterministic formula will find the perfect solution to have an arbitrary UR problem. We do an extensive experimental look at several algorithms on synthetic and real datasets, with a genuine crowd, to be able to assess their performance and scalability.

Tree of Possible Orderings (TPO): We realize that processing a high-K query over uncertain data only requires computing the orderings from the first K tuples suitable for the pdf's from the tuples scores. The asymptotic time complexity of creating the tree as much as level K is O(KN)2. Reducing uncertainty via crowd sourcing requires obtaining additional understanding in the crowd. As a result it becomes vital that you evaluate the uncertainty reduction that may be expected through the execution of the crowd task. the TPO acquired in the score distributions. The 3rd measure is dependent on the thought of evaluating all of the orderings in T K by having an ordering that's representative in certain sense. On the other hand, the T1_on and C-off algorithms provide a good tradeoff between costs and gratification. With synthetic datasets, both T1_on and C-off achieve significant reductions of the amount of questions wrt. the Naive formula. The amount of orderings inside a TPO could be large should there be many overlaps within the tuple score distributions, Uncertainty Resolution and employ T K like a beginning reason for our analysis, understanding that T K could be constructed with the strategy described [6]. We've two primary methods for reducing uncertainty in T to rapidly converge towards the correct ordering: i) building just the first K quantity of a TPO, and ii) defining crowd tasks for disambiguating the relative order of tuples to be able to prune the TPO. And then we now turn our focus on an attainable type of optimality that's of the probabilistic nature, for the reason that it refers back to the expected quantity of uncertainty that continues to be within the TPO after posing the questions selected by an formula. We consider two classes of algorithms: i) offline algorithms, and ii) online algorithms. In crowd sourcing applications, limitations within the budget employed for rewarding workers or perhaps in the accessible time allotted for collecting solutions usually limit the amount of questions that may be published towards the crowd. A web-based formula is able to determine the it question in line with the solutions collected for the formerly requested i - 1 questions [7]. Inside a crowd sourcing scenario, the collected solutions may be noisy. Observe that, if uncertainty is measured like a distance from the representative ordering, which is really a probabilistic proxy for that real ordering, then minimizing the rest of the uncertainty indeed comes down to minimizing an expectation from the distance in the real ordering. Starting by analyzing the outcome of uncertainty on full datasets that contains all of the N tuples. Observe that the quantity of uncertainty depends upon the mixture of N and d. the uncertainty reduction when asking workers to check pairs of images when it comes to their visual quality. The outcomes read the findings acquired around the synthetic datasets.

4. CONCLUSION:

We advise an formula that avoids the materialization from the entire space of possible orderings to attain even faster results. To begin with, we demonstrated that measures of uncertainty that look at the structure from the tree additionally to ordering odds achieve better performance than condition-of-the-art measures. The suggested algorithms happen to be evaluated experimentally on synthetic and real data sets, against baselines that select questions either at random or concentrating on tuples by having an ambiguous order. The experiments reveal that offline an internet-based best-first search algorithms attain the best performance, but they are computationally impractical. The suggested algorithms happen to be proven to operate also with no uniform tuples score distributions with noisy crowds. Reduced CPU occasions are possible using the incr formula, with slightly

lower quality. Furthermore, since UR doesn't admit deterministic optimal algorithms, we've introduced two groups of heuristics able to lowering the expected residual uncertainty from the result set. These trends are further validated around the real datasets.

REFERENCES:

[1] Eleonora Ciceri, PieroFraternali, DavideMartinenghi, and Marco Tagliasacchi, "Crowd sourcing for Top-K engineering, vol. 28, no. 1, january 2016.

[2] F. C. Heilbron and J. C. Niebles, "Collecting and annotating human activities in web videos," in Proc. Int. Conf. Multimedia Retrieval, 2014, p. 377.

[3] J. Fan, et al., "A hybrid machine-crowd sourcing system for matching web tables," in Proc. IEEE 30th Int. Conf. Data Eng., 2014, pp. 976–987.

[4] S. K. Kondreddi, et al., "Combining information extraction and human computing for crowdsourced knowledge acquisition," in Proc. IEEE 30th Int. Conf. Data Eng., 2014, pp. 988–999.

[5] W. Zhang, et al., "A trust based framework for secure data aggregation in wireless sensor networks," in Proc. IEEE 3rd Annu. Commun. Soc. Netw., 2006, pp. 60–69.

[6] A. Parameswaran, et al., "Human-assisted graph search: It's okay to ask questions," in. Discovery Data Mining, 2008, pp. 614–622.

SIGN-CRYPTION SECURITY ADMISSION DIRECT TO ACHIEVE LEAST COSTS

T. Sudha[1]., M. Dhange[2]

1 Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- sudhathulluri@gmail.com)

2 Associate Professor, Department of H&S., Halakatta College of Engineering and Technology, Vijayapur., Karnataka., India.

ABSTRACT: ***The WBANs boost the efficiency of healthcare since someone is not needed to go to a healthcare facility frequently. The clinical diagnosis and a few emergency medical response may also be recognized through the WBANs. Therefore, you should design a competent access control plan that is capable of doing authorizing, authenticating and revoking a person to gain access to the WBANs. A user's public secret is computed from the identity information, for example identification figures, e-mail addresses and IP addresses. The user's private secret is created with a reliable 3rd party named private key generator. We design an access control plan for that WBANs while using CLSC with public verifiability and ciphertext authenticity. The SP accounts for the registration for the user and also the WBAN and creating a partial private key for that user and also the private keys for that WBAN. Authentication helps to ensure that just the approved user have access to the WBAN. Integrity helps to ensure that a question message in the user is not altered by a few unauthorized entities. Our methodology uses CLSC with public verifiability and ciphertext authenticity. Such design has got the benefits below: i) it's neither key escrow problem nor public key certificates. ii) it enables the controller to determine the valid of query messages without understanding. In contrast to the standard public key infrastructure which uses an electronic certificate to bind a name as well as an public key, the identity based cryptography doesn't need digital certificates.***

Keywords: Clinical diagnosis, Wireless body area networks, security, access control, signcryption, certificate less ciphertext authenticity

1. INTRODUCTION:

Wireless body area systems are anticipated to do something as a huge role in monitoring the information and developing a highly reliable ubiquitous healthcare system. Hu et al. discussed how you can safeguard the communication between exterior users and also the WBANs. Their option would be attribute-based file encryption. However, the ABE might not be the ideal choice because it requires some pricey cryptographic operations. To be able to lessen the energy consumption, they used energy-based multihop-routechoice method and biometrics synchronization mechanism. messages are safe [1]. You should safeguard the query messages for preserving the privacy from the users. Our plan achieves confidentiality, integrity, authentication, non-repudiation, public verifiability and ciphertext authenticity. The general public verifiability implies that a 3rd party can verify the validity of the ciphertext not understanding the controller's private key. this plan cannot be directly accustomed to design an access control plan for that WBANs because it cannot provide public verifiability and ciphertext authenticity. Although BDCPS is extremely efficient, it cannot be directly accustomed to design an access control plan for that WBANs. Gamage et al. modified Zheng signcryption to attain public verifiability and ciphertext authenticity. Ideas make use of the same approach to provide a modified BDCPS plan. Now we describe a concrete access control plan while using modified BDCPS plan. This access control plan consists of four phases: the initialization phase, the registration phase, the authentication and authorization phase, and also the revocation phase. the controller doesn't carry out the 4th step of Unsigncrypt, which saves computational cost and consumption. Such design has got the benefits below: 1) It's neither key escrow problem nor public key certificates. 2) It enables the controller to determine the valid of query messages without understanding. If your user wishes to connect to the WBAN, it should be approved through the SP. The SP accounts for the registration for the user and also the WBAN and creating a partial private key for

that user and also the private keys for that WBAN [2].

2. CLASSICAL APPROACH:

Using the rapid progress in wireless communication and medical sensors, wireless body area systems they are under rapid development and research. An average WBAN consists of numerous implantable or wearable sensor nodes along with a controller. The sensor nodes have the effect of monitoring a patient's vital signs and ecological parameter. The sensor nodes talk to the controller and also the controller functions like a gateway that transmits the collected health data towards the healthcare employees and network servers [3]. The WBANs boost the efficiency of healthcare since someone is not needed to go to a healthcare facility frequently. The clinical diagnosis and a few emergency medical response may also be recognized through the WBANs. Therefore, the WBANs behave as a huge role in developing a highly reliable ubiquitous healthcare system. A great survey concerning the current condition-of-art of WBANs is offered by Movassaghi et al. Disadvantages: An average WBAN consists of numerous implantable or wearable sensor nodes along with a controller.

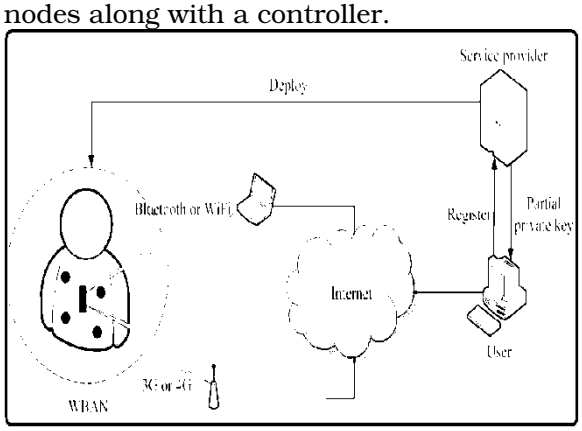


Fig.1.System architecture

3. ENHANCED ARCHITECTURE:

We first give a competent certificate less signcryption plan after which design an access control plan for that WBANs while using given signcryption. Our plan achieves confidentiality, integrity, authentication, non-repudiation, public verifiability, and cipher text authenticity. In contrast to existing three access control schemes using signcryption, our plan has got the least computational cost and consumption for that controller [4]. Additionally, our plan has neither key escrow nor public key certificates, as it is according to certificate less cryptography. Advantages: We suggested an altered certificate less signcryption Plan that satisfies public verifiability and cipher text Authenticity. We gave certificates less access control plan for that WBANs while using modified signcryption. In contrast to existing four access control schemes using signcryption, our plan has got the least computational time and effort consumption.

Methodology: Our plan achieves confidentiality, integrity, authentication, non-repudiation, public verifiability, and ciphertext authenticity. WBANs, and doesn't fit large-scale systems, like the Internet. However, the aim of the access control for that WBANs would be to restrict the web users to gain access to the WBANs. Therefore, total IBC can't fulfill the goal. The important thing escrow issue is prevented. However, Liu et al.'s plan is design to limit you to gain access to a network server, and not the WBANs. CK has got the key escrow weakness as it is in line with the IBC. Our methodology uses certificateless signcryption with public verifiability and ciphertext authenticity. Within this paper, we suggested an altered certificateless signcryption plan that satisfies public verifiability and ciphertext authenticity. The WBAN includes some sensor nodes along with a controller. The sensor nodes can talk to the controller and also the controller can communicates without just the sensor nodes but the Internet. We gave a certificateless access control plan for that WBANs while using modified signcryption [5]. In contrast to existing four access control schemes using signcryption, our plan has got the least computational time and effort consumption. Ideas only consider the price of controller part since its resource is restricted. The primary sign of BDCPS is the fact that BLMQ

identitybased signature, Schnorr signature, and Zheng signcryption are built-into a certificateless signcryption. The communication between your user and also the controller should satisfy four or five security qualities, i.e. confidentiality, authentication, integrity and non-repudiation. The modified BDCPS plan has got the same security because the original BDCPS. Additionally, the modified BDCPS plan has got the public verifiability and ciphertext authenticity. A person should register using the SP to achieve an access privilege from the WBAN. Within this access process, confidentiality, integrity, authentication and non-repudiation are concurrently achieved. Additionally, an essential benefit of our plan would be to achieves the general public verifiability and ciphertext authenticity [6]. The ECDSA requires some point multiplication operation in signing a note and 2 point multiplication operations in verifying a signature.

4. CONCLUSION:

Within this paper, we first give a competent certificateless signcryption plan after which design an access control plan for that WBANs while using given signcryption. The controller can verify the validity of the ciphertext without understanding. In contrast to existing three access control schemes using signcryption, our plan has got the least computational cost and consumption for that controller. Applying this modified BDCPS plan, full non-repudiation can be simply acquired. Additionally, any 3rd party can verify the validity from the ciphertext s not understanding the controller's private key and also the message m. The 4 schemes use different ways to create the access control schemes. CK uses the IBSC, HZLCL uses FABSC, MXH uses PKI-based signcryption and our plan uses CLSC. Our plan has neither key escrow problem nor public key certificates as it is in line with the CLC.

REFERENCES:

[1] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 3156. New York, NY, USA: Springer-Verlag, 2004, pp. 119–132.

[2] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3788. New York, NY, USA: Springer-Verlag, 2005, pp. 515–532.

[3] G. Cagalaban and S. Kim, "Towards a secure patient information access control in ubiquitous healthcare systems uses identity-based signcryption," in Proc. 13th Int. Conf. Adv. Commun. Technol. (ICACT), Seoul, Korea, Feb. 2011, pp. 863–867.

[4] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Secure. Privacy (Hotwire), Budapest, Hungary, 2013, pp. 31–35.

[5] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) cost(signature) + cost(encryption)," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1294. New York, NY, USA: Springer-Verlag, 1997, pp. 165–179.

[6] P. S. L. M. Barreto, A. M. Deusajute, E. de Souza Cruz, G. C. F. Pereira, and R. R. da Silva, "Toward efficient certificateless signcryption from (and without) bilinear pairings," in Proc. Brazilian Symp. Inf. Comput. Syst. Secure., 2008, pp. 115–125.

SIGNATURE BASED CRYPTOSYSTEM FOR ENTRENCHED FACTS DESCEND AND ACCESS CONTROL TREE

Ch. Anusha[1]., ChandraMohan[3]

1 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- chalamalasettianu@gmail.com)

1 Assistant Professor, Department of H&S., St. Martins Engineering College, Maisammaguda., Medchal., TS, India

ABSTRACT: ***Within this paper, we advise a competent attribute-based file encryption and signature plan that is a one-to-many file encryption method. Quite simply, the content is supposed to be read by several users that satisfy certain access control rules inside a BAN. To guarantee the security from the data, we have to have certain degree of protection towards the data sink. However, a Smartphone like device becoming the information sink could be physically stolen or lost, as well as an attacker can see the information once he captures the unit. The information sink is definitely an IMD made to store data or perhaps a Smartphone, which is able to talk to an online healthcare agency through cellular systems or even the Internet. Most existing operates in this category centered on securing the transmissions between an implantable tool and a BAN controller, which may be a cell phone transported through the patient. In comparison, we create a data communication plan within this paper that has considerably lower communication overhead and power consumption. You ought to observe that the key keys would be the crux to decrypt a note, and not the attributes themselves. Our primary idea would be to design a characteristic-based security plan that views a name as some attributes, and enforces a lesser bound on the amount of common attributes from a user's identity and it is access legal rights specified for that sensitive data. We realize that the content size includes a straight line relationship using the security level for creating an association. When the connection is made, the content dimensions are in addition to the security level.***

Keywords: Sensor network, Wireless Body Area Networks; Access control tree; Attribute-based cryptosystem; signature, smart phone..

1. INTRODUCTION:

To safeguard against information exposure because of thievery or compromise from the data controller, and also to control the accessibility data controller or even the BAN devices (implanted or wearable sensors), the attribute based file encryption over IBE will be investigated. Rather of utilizing software or any other mechanism to do access control, we use file encryption and signature method to supply a role-based encrypted access control [1]. The sensor is able to control who can access its data by constructing an access structure for that data. We assess the performance from the suggested plan when it comes to energy consumption and communication/-computation overhead. This can lead to a substantial security threat being a foe having a UWB radar can first capture the IPI after which utilize it to compromise the patient's health information. Having a bilinear map, it's possible to have the following variation from the Diffie-Hellman problem. Observe that report from the decision form of it. An information consumer will be able to convince the KGC that it's the who owns some attributes and also the KGC will produce a secret key for every attribute. It's possible to observe that the key keys are distinctively generated for that data consumer, which means that random figures have to be connected using the group of secret secrets of prevent collusion attacks. Implanted devices are afflicted by very restricted sources when it comes to electric batteries, storage, and computation capacity. Wearable devices, however, cash less stringent resource constraints [2]. They're usually battery-powered and also the batteries could be altered/recharged relatively easily. Wearable devices far exceed implanted ones both in quantity and heterogeneity. The BAN devices must have certain computation capacity to secure the patient's data and keep ciphertext in to the data sink.

2. EXISTING SYSTEM:

Like a sensor that collects patient information, all it cares would be to distribute the data to approved doctors along with other experts safely. However, you will find challenges

everywhere: Data ought to be transmitted inside a secure funnel, and everyone knows the difficulties in securing wireless communication channels. Node authentication is easily the most fundamental step perfectly into a BAN's initial trust establishment, key generation, and subsequent secure communications [3]. There is research that allows embedded sensors to determine a session key with one another by leverage physiological signals for example Electrocardiograph (ECG). Probably the most relevant existing research along three lines: (1) securing individual (implantable) devices inside a BAN (2) securing the communications inside a BAN and (3) identity-based cryptography for BANs. Disadvantages of existing system: The important thing-distribution in symmetric file encryption is challenging. And symmetric file encryption isn't great for broadcasting a note since it involves some challenging issues, for example key-management and access control. Simultaneously, because of the limitation of storage in sensors, an information sink, that has significantly bigger memory and computation power, is utilized to keep data. Recent research disclosed that smart phones are afflicted by severe privacy concerns because so many applications frequently mix the road and browse sensitive data in their freedom (for instance, just about all apps read user's location). A patient's IPI information might be remotely taken by an ultra-wide-band (UWB) radar device. This can lead to a substantial security threat being an foe having a UWB radar can first capture the IPI after which utilize it to compromise the patient's health information.

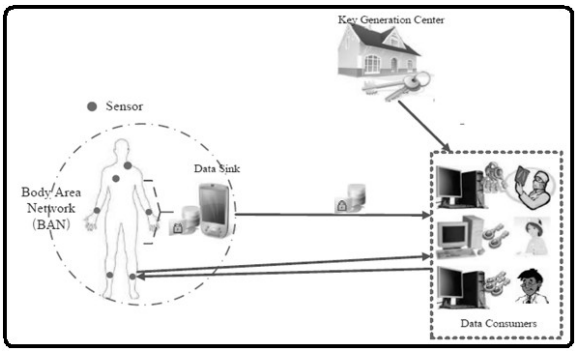


Fig.1.System architecture

3. PROPOSED SYSTEM:

We advise a singular file encryption and signature plan according to Clubpenguin ABE within this paper to deal with the secure communication problem and supply the needed security services pointed out above for BANs. A sensor can control the accessibility data it's created by constructing an access structure. For instance, by constructing the access structure (fGWU hospital AND fVascular Surgical Procedures or Cardiac Surgery), the information mandates that only doctors or experts in GWU hospital, Vascular Surgery Center or Cardiac Surgery Center might have the access right. Data are kept in ciphertext format in the data sink and also the trust we placed on the information sink has become drastically decreased because the data sink doesn't have the important thing to decrypt the stored ciphertext. However, the plan is one of the uneven file encryption family, which means a higher computational cost [4]. This issue is addressed using the plan to secure a session key and so the information is encrypted by symmetric file encryption in line with the session key. Benefits of suggested system: We advise a framework that allows approved doctors and experts to gain access to a patient's private medical information safely. Rather of utilizing software or any other mechanism to do access control, we use file encryption and signature method to supply a role-based encrypted access control. The sensor is able to control who can access its data by constructing an access structure for that data. We minimize the trust that individuals usually placed on the information

sink by storing the information in ciphertext. The compromise from the data stored in the data sink doesn't always indicate the information is compromised [5]. We assess the performance from the suggested plan when it comes to energy consumption and communication/computation overhead.

Methodology: Data ought to be transmitted inside a secure funnel, and everyone knows the difficulties in securing wireless communication channels. Node authentication is easily the most fundamental step perfectly into a BAN's initial trust establishment, key generation, and subsequent secure communications. Current advances have the ability to deploy battery-powered miniaturized IMDs on, in, or around the body for lengthy-term healthcare monitoring. The sensor really wants to distribute its collected data safely to approved doctors along with other experts. The only real factor the sensor must know would be that the physician or expert has got the privilege to gain access to its data. The understanding from the ciphertext necessitates the attributes based on the sender. For instance, within the Clubpenguin ABE plan, the access was based on an access tree connected using the ciphertext. Yu et al. created a distributed fine-grained access-control mechanism for wireless sensor systems. But it doesn't provide message authentication - another essential dependence on BAN security. For every attribute a person offers, a personal key must be generated, that you can use later to decrypt a ciphertext when the attributes fulfill the access tree from the original data [6]. Whenever a physician really wants to send instructions or instructions to some sensor inside a BAN, direct communications between your physician and also the sensor are essential. Thinking about the limitation in computation power and storage from the sensor, we'll leverage the information sink again by posting it an access token K1, that is encrypted by having an access tree per the sensor. In most cases, our protocol could be split into three phases: initialization phase, communication establishment phase, and communication phase. The Clubpenguin ABE provides uneven file encryption having a high computation cost. Thus we decide uneven file encryption to secure the session-key for creating symmetric file encryption. The tradeoff is apparent here: the shorter the time, the greater the regularity from the secret key updates, thus the greater the computation cost. There is some investigation on real-time key revocation, which mandates that when a user continues to be revoked, the update happens immediately. Observe that the sensor must send the brand new encrypted access token towards the data sink and also the data sink must switch the old one using the brand new one [7]. When a connection is made, the computation price is low. Nevertheless, you should observe that when both cost suffered by connection establishment which during communications are taken into account, our suggested plan could be more inviting compared to other schemes.

4. CONCLUSION:

Within this paper, we advise a framework which makes this secure by designing a protocol that facilitates role based encrypted access control and cuts down on the trust we put on the information sink. We advise a singular file encryption and signature plan according to Clubpenguin ABE within this paper to deal with the secure communication problem and supply the needed security services pointed out above for BANs. Within this paper, we advise algorithms to manage the access legal rights from the users in line with the attribute-based file encryption over Clubpenguin ABE. The performance of the design when it comes to energy consumption and communication/computation overhead is going to be extensively studied. The detailed way in which shows the way the data consumer can be towards the KGC he offers some attributes has run out of the scope of the paper.

REFERENCES:

[1] Chunqiang Hu, Student Member, IEEE, Hongjuan Li, Xiuzhen Cheng, Fellow, IEEE,

Xiaofeng Liao, Senior Member, IEEE, "Secure and Efficient data communication protocol for Wireless Body Area Networks", ieee transactions on multi-scale computing systems, 2016.

[2] H. B. Lim, D. Baumann, and E.-P. Li, "A human body model for efficient numerical characterization of uwb signal propagation in wireless body area networks." IEEE transactions on Biomedical Engineering, vol. 58, no. 3, pp. 689–697, 2011.

[3] J. Li, D. Wei, and H. Kou, "Secure monitoring scheme based on identity-based threshold signcryption for wireless sensor networks," in 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008, pp. 1–4.

[4] J. Akinyele, M. Pagano, M. Green, C. Lehmann, Z. Peterson, and A. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proceedings of the 1st ACM workshop on Security and privacy in smart phones and mobile devices. ACM, 2011, pp. 75–86.

[5] J. Zhou, Z. Cao, and X. Dong, "Bdk: secure and efficient biometric based deterministic key agreement in wireless body area networks," in Proceedings of the 8th International Conference on Body Area Networks. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013, pp. 488–494.

[6] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.

A SERVICE MIGRATION TO OPTIMIZE MONITOR COST CONTROLLER

Ch. Anusha[1]., G. Hari Priya[2]

1 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- chalamalasettianu@gmail.com)

2 Associate Professor, Department of H&S., Gates Information and Technology, Ooty, India

ABSTRACT: ***Moving OSN services toward geographically distributed clouds must reconcile the requirements from the 3 different factors. OSN services frequently possess a large users list and want to scale to satisfy demands of users worldwide, redistributed clouds that offer Infrastructure-as-a-Service can match this need seamlessly and supply tremendous resource and price efficiency advantages. Existing focus on OSN service provisioning either pursues least cost in one site with no QoS concern as with the geo-distribution situation. Within this paper, we read the problem of optimizing the financial price of the dynamic, multicolor-based OSN while making certain its QoS and knowledge availability. Social locality has multifold advantages: Given there are frequently a lot more reads than writes within an OSN service, it may thus save the great majority from the interclub traffic this plan also incurs a significantly lower storage consumption than full replication for the reason that the entire replication requires every cloud to keep an information replica for each user. The OSN provider ought to be enabled to determine whether or not to optimize the price for every billing period, based on her financial budget and expected profit, etc. When multiple role-swaps for any user can be found, we have to pick the one(s) meeting QoS needs. We investigate the way the costs suffer from the information availability requirement by the QoS requirement. We ensure social locality for those methods for fair comparison. The greedy method places every user's master on her behalf first most preferred cloud. We advise as our formula. By extensive evaluations with large-scale Twitter data, is verified to incur substantial cost reductions over existing, condition-of-the-art approaches.***

Keywords: Online social network, optimization models and methods, performance analysis and evaluation, cloud environment.

1. INTRODUCTION:

Within this paper, we read the problem of cost optimization for that dynamic OSN on multiple geo-distributed clouds over consecutive periods of time while meeting predefined QoS and knowledge availability needs. When compared with existing approaches, reduces cost considerably and finds a substantially good solution from the cost optimization problem, while guaranteeing all needs are satisfied. An OSN provider specifies the information availability requirement by indicating the minimum quantity of every user's slave replicas [1] [2]. We introduce the next notations to be able to formulate the issue. and therefore are binary decision variables. The previous equals to at least one if within the optimal placement user's master replica is positioned on cloud, and otherwise. We advise an optimization formula that iteratively swaps the roles of master and slave replicas on several clouds to achieve the perfect placement. Our formula follows a greedy approach in making use of role-swaps and requiring that each applied role-swap reduce cost. The greater cost reduction each role-swap has and also the more role-swaps are applied, the greater total price reduction we are able to achieve [3]. Whether just one role-swap or perhaps a double role-swap, three fundamental but nontrivial operations of are essential: figuring out whether it's achievable, calculating your buck reduction, and swapping the roles of involved replicas. Observe that applying one role-swap can alter the present QoS, and also the practicality from the next role-swap should be considered in line with the new QoS.

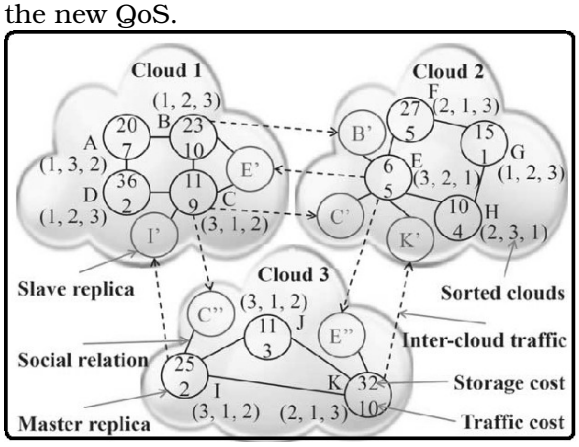


Fig.1.System architecture

2. IMPLEMENTATION:

Our QoS model links the QoS with OSN users' data locations among clouds. According to these models, then we formulate the price optimization problem that views QoS and knowledge availability needs. This issue is NP-hard. In comparison, the amount of the write operations done by a person on all replicas of hers and her buddies depends upon the amount and also the keeping the replicas. Within the new placement, whenever a slave must be produced on the cloud for social locality, we determine if it didn't exist around the cloud within the existing placement [4]. Each user only has one master replica and many slave replicas of her data, where each replica is located in a different cloud. When calculating the expense, we think that all clouds have a similar billing prices. The truth is resource use of clouds from various providers or at different locations might be billed at different prices. Individuals OSN service over multiple clouds, we start with identifying the kinds of costs associated with cloud resource utilization: the storage cost for storing users' data, the interclub traffic cost for synchronizing data replicas across clouds, the redistribution cost suffered by the price optimization mechanism itself, and a few underlying maintenance cost for accommodating OSN dynamics. We think that each cloud can offer “infinite” sources when needed for an OSN company, an assurance frequently supplied by a cloud provider to the customers [5]. Whenever a new user joins the OSN service, the service selects a cloud and places this user's data there. A while later following this initial placement with no after the finish of the present billing period, the OSN service must maintain social locality with this user and her neighbors, including creating new slave replicas on involved clouds when needed, incurring maintenance cost. Observe that, for that initial data placement, the OSN service could use various prespecified ways of select a cloud, for example selecting the main one using the cheapest access latency for that user. The price reduction only depends upon the storage and traffic price of user and her neighbors, and also the locations of the replicas within the new and old placements. If on user 's master cloud we store a slave replica of her neighbor to keep the social locality for , and when doesn't have other neighbors of her very own about this cloud, a job-swap between user 's master and her slave can make this slave replica of useless, which replica is thus an applicant for elimination. For METIS, there's a wide open-source implementation from the authors. We use its choice of minimizing the interpretation communication. We use each user's storage cost plus her traffic cost because the vertex size to produce its input. We operate on the previous to exhibit the “ideal” cost reduction, presuming we all know the precise costs of every user for every month at the outset of each month. We operate on the second, where replica locations are adjusted based on the believed costs of every user, to exhibit the potency of our estimation approach [6]. Thus, greedy can assign local users towards the same nearby cloud, and random has a tendency to straddle local social relations across clouds. SPAR has less cost than greedy and random but greater than METIS. We model the price of OSN data placement, evaluate the OSN service quality with this vector approach, and address OSN data availability by making certain the absolute minimum quantity of replicas for every user.

3.OPTIMIZATION OF REPLICA PLACEMENT:

Our results reveal that, while always making certain the QoS and also the data availability as needed can help to eliminate a lot more one-time cost compared to condition-of-the-art methods, also it can also considerably lessen the accumulative cost. The charging for read operations is thus from the scope in our optimization of replica placement. In comparison, the amount of the write operations done by a person on all replicas of hers and her buddies depends upon the amount and also the keeping the replicas. Within the new placement, whenever a slave must be produced on the cloud for social locality,

4. CONCLUSION:

We determine if it didn't exist around the cloud within the existing placement. If that's the case, the price of creating this slave is put into the redistribution cost suffered by this role-swap. When we cannot remove a slave because of the data availability reason, this user shouldn't be considered when calculating cost decrease in a job-swap which involves this user, and also the slave can also be not touched when conducting the function-swap. The graph partitioning problem divides a weighted graph right into a given quantity of partitions to be able to minimize either the weights of edges that straddle partitions or even the interpretation communication volume while balancing the weights of vertices in every partition.

REFERENCES:

[1] F. Pellegrini and J. Roman, "Scotch: A software package for static mapping by dual recursive bipartitioning of process and architecture graphs," in Proc. HPCN Europe, 1996, pp. 493–498.

[2] K. Schloegel, G. Karypis, and V. Kumar, "Wavefront diffusion and LMSR: Algorithms for dynamic repartitioning of adaptive meshes," IEEE Trans. Parallel Distrib. Syst., vol. 12, no. 5, pp. 451–466, May 2001.

[3] Y. Wu, C. Wu, B. Li, L. Zhang, Z. Li, and F. C. M. Lau, "Scaling social media applications into geo-distributed clouds," in Proc. IEEE INFOCOM, 2012, pp. 684–692.

[4] L. Backstrom, D. Huttenlocher, J. Kleinberg, and X. Lan, "Group formation in large social networks: membership, growth, and evolution," in Proc. SIGKDD, 2006, pp. 44–54.

[5] A. Khanafer, M. Kodialam, and K. PN Puttaswamy, "The constrained ski-rental problem and its application to online cloud cost optimization," in Proc. IEEE INFOCOM, 2013, pp. 1492–1500.

[6] F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida, "Characterizing user behavior in online social networks," in Proc. IMC, 2009, pp. 49–62.

NETWORK LINK-BASED ENERGY CONSUMPTION WITH QOS REQUIREMENTS

V. Saroja[1]., B. Haritha[2]

1 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (:- donsaroja007@gmail.com)

2 Associate Professor, Department of H&S., Santhi Ram Engineering College., Nandhyala, AP., India.

ABSTRACT: ***Ternary content addressable memory is broadly accustomed to implement packet classification due to its parallel search capacity and constant processing speed. Besides, there frequently exists redundancy among rules. For instance, R2 is really unnecessary and could be securely taken off the classifier, since it is completely included in R3. Both of these problems result in inefficiency in TCAM use. Because TCAMs are costly and power-hungry, it is crucial to lessen the amount of TCAM records needed to represent a classifier. Whenever a packet comes for query, correspondingly, we have to use the same permutations towards the header from the packet, the preprocessing step. We are able to judge the direction of the block through the positions from the wildcards within the Boolean representation. If two blocks have wildcards appearing exactly within the same items of their Boolean representations, we are saying both of these blocks have been in exactly the same direction. Within the direct logic optimization phase, we directly apply logic optimization around the original classifier to group adjacent rule elements. This really is to lessen the amount of rules that'll be active in the permutation phase and, hence, lessen the computation complexity. The best way to estimate the amount of rules reduced for any given set of assistant blocks is as simple as checking all possible rule pairs in the present classifier to find out if them could be a target block set of the given assistant blocks. On a single hands, the BP formula can offer sub-optimal results; However, we limit the run-time complexity from the BP formula. The suggested BP is really a new technique for the reason that it looks for nonequivalent classifiers instead of equivalent ones, as previous schemes did. Our experiments were according to one real-existence firewall classifier and many artificial classifiers generated by utilizing Class-Bench. To judge the performance, we compared the BP technique with McGeer's formula.***

Keywords: ***ternary content-addressable memory (TCAM), classifier minimization, field-programmable gate array (FPGA), logic optimization, packet classification***

1. INTRODUCTION:

The first is the well-known range expansion problem for packet classifiers to become kept in TCAM records. Dong et al. in suggested four simple heuristic algorithms to locate equivalent classifiers consuming less TCAM records [1]. Dong's algorithms will also be special installments of logic optimization and also the first-matching property. Bit Weaving may be the first all-field optimization plan trying to break the limitations of fields. It may find and merge two rules with one bit different; regardless of by which field the part is situated. Throughout the mapping, the overlapping part of rules is connected with the act of the greatest-priority rule. Much like McGeer's plan, the BP technique is another bit-level solution, with the exception that BP swaps blocks (or points) to develop a nonequivalent classifier and therefore needs preprocessing on incoming packets. While BP can help to eliminate the TCAM size, the preprocessing does introduce overhead. However the overhead could be much smaller sized than the TCAM resource saved. The machine throughput is made the decision through the slower of preprocessing and TCAM searching. To make sure high end, the preprocessing must be implemented by hardware. Because of its architectures, an SRAM-based FPGA is usually more power efficient than the usual TCAM with similar gate count. After applying BP, when the total gate count of FPGA and TCAM is smaller sized compared to original gate count of TCAM, we are able to think power is saved. To obtain the optimal solution for that BP problem, one way possible is brute pressure. This type of solution, however, is impractical. Let's consider a brute pressure method. As you may know, block permutations just have to change rule distribution and don't add or delete any rule elements. One technique is to lessen parameters like and, however this may sacrifice the compression performance. So, a great tradeoff between run-some time and compression is required in tangible applications. When becomes bigger, due to the

large coefficients, the rum-time can always grow rapidly [2]. For hardware cost, we used the idea of "Equivalent Gate Count" to estimate the particular hardware resource saved using the BP technique.

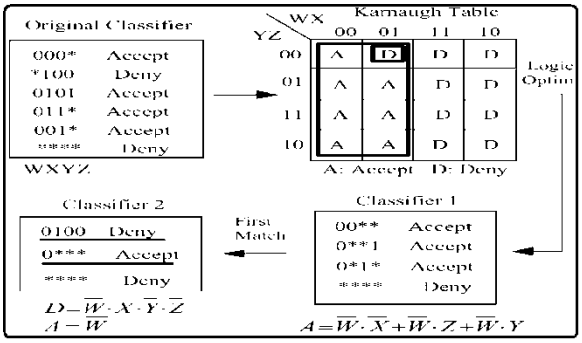


Fig.1.Proposed framework

2. METHODOLOGY:

Within this paper, we advise a brand new technique known as Block Permutation (BP) to lessen the amount of TCAM records needed to represent a classifier. Within this paper, we advise a singular technique known as Block Permutation (BP) to compress the packet classification rules kept in TCAMs. A TCAM has a vast selection of records, by which every bit could be symbolized as '0', '1', or '*'. Normally, the very best compression of the range-field optimization plan would be to reduce an expanded classifier towards the size before expansion [3]. Within this category, The most popular a part of each one of these schemes would be to first expand all ranges to prefixes, obtaining a new classifier without any range fields, after which convert the non-range classifier to some semantically equivalent one which consumes less TCAM records. To judge the performance, we compared the BP technique with McGeer's formula, the first bit-level plan. A packet must traverse stages having a delay of clock cycles before entering the TCAM for that classification. Because each stage is straightforward enough, the pipeline can run in a high clock rate and therefore give a high throughput. You should explain that swapping small blocks causes more overhead than swapping big blocks, because small blocks have less wildcards within the Boolean representations, hence involving more non-wildcard bits in to the permutations. Within the permutation phase, we recursively find and perform permutations around the classifier. We make use of the parameter to manage the amount of iteration models. The FPGA overhead from the ACL classifiers is comparatively high in comparison to the TCAM saved. It is because the compressions are achieved by swapping relatively small permutations of blocks. To enhance throughput, normally, we are able to use more stages. Within the ACL classifiers, we always discover that block permutation contributes a lot more compression than direct logic optimization does, a well known fact that we are able to judge the ACL classifiers also fall under "sparse" rule distributions. Since the overall throughput of the pipeline is dependent upon the slowest stage(s), it's possible that some extremely complicated permutations would slow lower the pipeline. Based on the original concept of block permutation, we anticipate finding and execute just one permutation in every round of iteration [4]. Only when a set of rules meets each one of these three constraints don't let see it as a set of target blocks. These constraints can largely reduce the amount of target block pairs that should be considered in every round of iteration, hence lowering the computational complexity. Its primary idea would be to deduce the Boolean representations of assistant blocks in the Boolean representations from the given target blocks [5]. Thinking about that BP compression and FPGA synthesis take some time, we ought to begin a new complete BP process earlier, before scratch TCAM becomes full. The advance is achieved by performing a number of permutations to alter the distribution of rule elements in Boolean Space from sparse to dense, thus allowing more rules to become merged into each TCAM entry. There's two

situations that we have to consider when swapping a set of assistant blocks inside a permutation. After partitioning, while run-time is reduced, we are able to obtain a better compression. It is because when we keep your same around the original classifier for those parts, in every round, we are able to really consider more target block pairs as a whole [6].

3. FIELD-PROGRAMMABLE GATE ARRAY (FPGA):

We've developed a competent heuristic method of find permutations for compression and also have designed its hardware implementation using a field-programmable gate array (FPGA) to preprocess incoming packets. In BP, the incoming packets have to be preprocessed prior to being compared from the compressed classifier in TCAM. Circuit size and throughput performance would be the two major performance metrics we must consider when applying the permutations.

4. CONCLUSION:

This preprocessing could be implemented by FPGA. Within this paper, we advise a competent heuristic formula to locate permutations and offer an FPGA implementation methodology. Based on the conditions, there must be one target block included in among the two assistant blocks and moved throughout the swapping, as the other target block remains fixed. This operation of swapping assistant blocks can help to eliminate the space between two target blocks to 1, to enable them to be merged. Our experiments were according to one real-existence firewall classifier and many artificial classifiers generated by utilizing Class-Bench. To judge the performance, we compared the BP technique with McGeer's formula.

REFERENCES:

[1] P. McGeer, J. Sanghavi, R. Brayton, and A. Sangiovanni-Vincentelli, "Espresso-signature: A new exact minimizer for logic functions," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 1, no. 4, pp. 432–440, Dec. 1993.

[2] M. Karnaugh, "The map method for synthesis of combinational logic circuits," Trans. Am. Inst. Electr. Eng., vol. 72, no. 9, pt. I, pp. 593–599, 1953.

[3] C. Meiners, A. X. Liu, and E. Torng, "Bit weaving: A non-prefix approach to compressing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2009, pp. 93–102.

[4] O. Rottenstreich et al., "Compressing forwarding tables for datacenter scalability," IEEE J. Sel. Areas Commun., Switching and Routing for Scalable and Energy-Efficient Datacenter Networks, vol. 32, no. 1, pp. 138 – 151, Jan. 2014.

[5] C. Meiners, A. X. Liu, and E. Torng, "TCAM Razor: A systematic approach towards minimizing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2007, pp. 266–275.

[6] Y. Xu, Z. Liu, Z. Zhang, and H. J. Chao, "An ultra high throughput and memory efficient pipeline architecture for multi-match packet classification without TCAMs," in Proc. ACM/IEEE ANCS, 2009, pp. 189–198.

PIEZOELECTRIC MATERIAL FOR MICRO ENERGY HARVESTING FROM VIBARATION, MECHANICAL STRESS AND HUMAN BODY MOTION

A. Anil Kumar[1]., P. Suresh [2].,

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women.,

Maisammaguda., Medchal., TS, India (: anumula86@gmail.com)

2 Assistant Professor, Department of H & S., Anurag College of Engineering.,

Ghatkesar., Uppal., TS, India.

Abstract*— There is renewed interest in the increasing energy consumption of portable electronic devices and the concept of renewable energy harvesting in the human environment. This project focuses on one of these advanced methods of energy recovery using a piezoelectric material. The process of capturing the energy that surrounds a system and converting it into usable electrical energy is known as ENERGY CAPTURING. Mechanical energy is one of the most ubiquitous energies that can be reused in our environment. Mechanical residual energies can generally be used by converting vibrations into electricity. This project describes the use of PIEZOELECTRIC DEVICES to collect the energy of mechanical vibrations, the energy of mechanical stresses and strains, of the human body, which can generate electricity at milliwatt or microwatt level. Piezoelectric materials are excellent power generating devices in which an electric field is generated when a piezoelectric material is filtered; therefore, the piezoelectric material can convert environmental vibrations into electrical energy. Piezoelectric materials are widely used in real areas. .

Keywords*— Piezoelectric, Power generation, Vibration, Mechanical stress, Human body motion.

1. INTRODUCTION

In recent years, low power consumption electronic devices have grown rapidly. As the power consumption of these portable electronic devices increases, we are seeing renewed interest in the concept of using alternative renewable energies. Therefore, new power generation technologies are required for new generation devices, as they can couple mechanical and electrical properties [1].

This project describes the use of piezoelectric materials to recover energy from mechanical vibrations, mechanical stress and strain energy, the movement of the human body that can generate electricity at milliwatt or microwatt level. The concept of capturing the wasted energy surrounding a system from sources of vibration in the area is ubiquitous and accessible and can be found in places like car engines, rotating equipment, and the human body, which in all cases converts the vibration into electrical energy the deformation of an engine. Piezoelectric material. Harvesting this energy is one of the most promising techniques because of its high energy density. Piezoelectric materials have a crystalline structure that offers a unique ability to convert an applied voltage into electrical current and vice versa [2]. Piezoelectric materials are excellent power generating devices in which, when a piezo is loaded, an electric field is created; therefore, the piezoelectric material can convert environmental vibrations into electrical energy. Piezoelectric materials are widely used in real areas. Some of the newer apps are mentioned below.

2. PIEZOELECTRIC EFFECT

A unique property of the material that can convert mechanical energy into electrical energy, that is, vibrations into electricity. This effect occurs naturally in quartz, but in comparison, the energy recovery in lead zirconate titanate (PZT) is more beneficial. This effect makes them excellent energy producers.

This mechanism for generating electricity from this piezoelectric material is called the piezoelectric effect.

There are two piezoelectric effects:

1.direct effect

2. Reverse effect.

DIRECT EFFECT: The direct effect (called generator) is identified with the phenomenon

by which an electrical charge (polarization) is generated from mechanical stress. It is the property of the material to develop an electrical charge in the material when a mechanical stress is exerted on the material.

Example: In gas lighters, PE sensors such as acceleration sensors, pressure sensors.

REVERSE EFFECT - The reverse effect (called a motor) is associated with mechanical movement created by the application of an electric field. It is the property of the material to develop mechanical stress when an electrical charge is induced.

Example: buzzers, PE actuators used for micropositioning are also based on the reverse piezoelectric effect.

Therefore, piezoelectric energy recovery consists of using the direct effect (generator) [3-4].

3. BLOCK DIAGRAM OF PROPOSED SYSTEM

When stressed, a piezoelectric material generates electricity, ie mechanical vibrations, whereby the pressure exerted on the material is converted into electricity. Therefore, these crystals are connected in series to increase the voltage and they are connected in parallel to increase the current to achieve the required power generation.

The piezo output is alternating current which is converted to direct current using a bridge rectifier and then stored in a storage capacitor. The storage capacitor is connected to the battery via the charging switch relay. The charge regulator prevents overcharging and also protects against voltage peaks. The controller stops charging the battery when it exceeds a set high voltage limit, i.e. H. 14.2V, and activates charging again when the battery voltage drops back to 11.2V. To overcharge the battery to avoid the relay is used for high battery lock. A low-cut relay is also used to prevent the battery from discharging deeply. A relay driver circuit (ULN2003) that acts as a current amplifier is used to operate this relay.

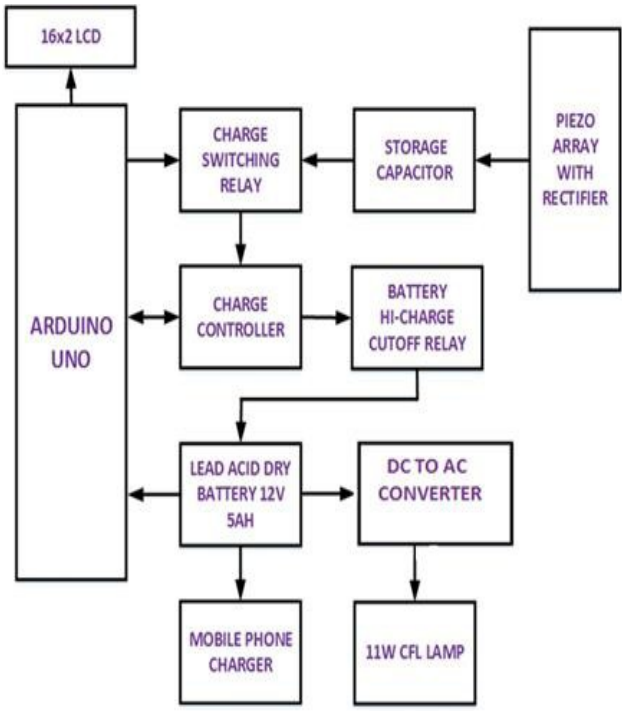


Fig-1: Function diagram

The relay control circuit stores the output voltage in two series-connected 6 V and 5 Ah lead-acid batteries. This is used because it is cheaper, easily disposable, durable, and maintenance free. The voltage stored in the battery is used to power the AC and DC loads. The DC load used here is the mobile charger.

To power an AC load from a 3-13 W light bulb, the 12 V DC voltage is converted to 12 V AC and a frequency of 50 Hz is generated over the RLC network. Now this 12 V AC is increased to 220 V AC using a step-up transformer and the waves are filtered out.

The power supply of the Arduino card is the power generated by the piezo matrix itself, and this input voltage for the Arduino card is 5 V. To supply this 5 V, a voltage divider circuit is used that is designed in a ratio of 1:10 and supplies a voltage of 5 V to the Arduino. The 7805 voltage regulator also supplies a constant voltage of 5 V to the LCD display.

To monitor the voltage level of the piezo matrix and the condition of the battery, a program is written using sketch language in which the LCD screen shows the voltage levels of the battery and the piezo matrix.

Two of these piezoelectric matrix banks are produced and connected in parallel, as a result of which a voltage of 12.5 volts and 120 milliA current is generated, as shown in FIG. 6, via these two banks connected in parallel, intermediate storage and from there the battery is charged.

Fig. 2: Two banks connected in parallel

4. PROVEN RESULTS AND PRODUCTION

We used 30 Piezo on a 370mm * 200mm mat. The voltage developed by piezo, which varies with the pressure applied, the minimum and maximum voltages obtained are as follows.

Generate a voltage of 13.56 V in a time interval. Minimum developed voltage = 1.1 V per step.

Maximum voltage developed = 2.8 V per step.

We take an average print weight of 60 kg from a person, the developed output voltage is as shown in the following calculation.

Table 1: Tested results for various load values

Load	11KΩ	22KΩ	44KΩ
Voltage in V	13.6	13.6	13.6
Charging time in sec	10.46	9.42	13
Discharging time in sec	4.88	7.95	13.95
No of steps	12	12	15

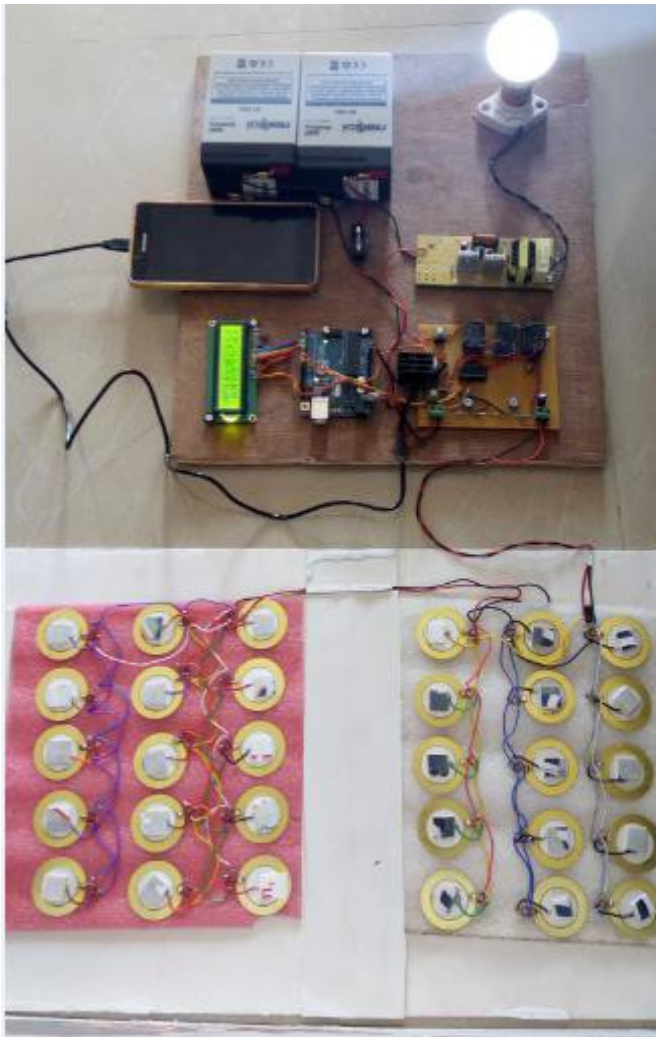


Fig. 3: Complete project configuration

Benefits

1. This is an environmentally friendly solution for generating electricity.
2. The piezoelectric material can be made in any one desired shape and shape.
3. It has no moving parts, so it has a long lifespan.
4. Very quiet.
5. Easy replacement of equipment.
6. Profitable.

5. CONCLUSION

In this article, a model of an energy recovery system using piezoelectric materials was presented. Piezoelectrics are intelligent materials that can be used to generate energy from dynamic vibration sources. It is clear that the harnessing of energy by piezoelectric

materials offers a cleaner way to power lighting systems and other devices or to store them for later use. This is a new approach to leading the world in implementing greener technologies to protect the environment. Piezoelectric energy recovery systems are a one-time installation and require very little maintenance, making them inexpensive. It is necessary to continue experimenting in order to carry out the implementation on a larger scale with an efficient interface circuit at a low cost in the universities. Research is currently underway to improve current piezoelectric materials and develop new materials.

REFERENCES

1. An Inductorless Self-Controlled Rectifier for Piezoelectric Energy Harvesting by Shaohua Lu and FaridBoussaid from University of Western Australia 2015.
2. V.J. Lauardini, Heat Transfer in Cold Climates (Van Nostrand, New York).
3. T.R. Goodman, The heat balance integral and its application in problems involving a change. J. Sol. Energy Eng. Trans.
4. Damjanovic, Dragan (1998). "Ferroelectric, dielectric and piezoelectric Properties of ferroelectric thin films and ceramics"

ANALYSIS OF BLIND AND TRAINING-BASED COMPENSATION ALGORITHMS FOR QUADRATURE AMPLITUDE MODULATION

L.Prashanth[1]., D.Raj Kumar[2]

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (: prashanthlukkalpr@gmail.com)

2 Assistant Professor, Department of H & S., CMR Institute of Technology., Kandlakoya., Medchal., TS, India

Abstract— This article demonstrated an in-depth analysis of blind and training-based compensation algorithms. Performance analysis and simulation results have been added to make them more general and specific. All simulation results were performed in quadrature amplitude modulation (QAM). The comparative demonstration was represented by graphics and simulation results

Keywords— Equalization, Training Equalization Algorithm, Blind Equalization Algorithm, LMS, RLS, MMA, SCA.

1. INTRODUCTION

Today, the wireless communication mode has taken over the wired communication mode. As the world moves from 3G to 4G to 5G there is a growing need for bandwidth, i. H. Data Rates. In high-bandwidth digital transmission, the formation of a receiver requires a start-up process. This configuration involves three steps to configure automatic gain control, get the time, and converge the adaptive filters. For many applications, certain sets of predefined bits are periodically sent to the receiver, which are referred to as a training sequence and which the receiver can use as an ideal reference since it is already known on the receiver side.

In the learning-based data-assisted equalization technique, a data element called the pilot / training signal is fed into the receiver, which helps the receiver to learn the channel values and then use this data for ISI channel estimation and cancellation. The training-based EQ method has a fast conversion rate, better efficiency and is easy to use. This method works best in environments where fast fading with high Doppler scattering and low coherence time is required. The disadvantage of this equalizer; however, is that they need pilot signals all the time. The constant streaming of the training sequence consumes a lot of bandwidth, which is a major disadvantage. In GSM, around 18% of the bandwidth is used by the learning sequences that are periodically sent to the receiver [5]. There are several learning algorithms that can be used in an adaptive learning-based equalizer, e.g. B. LMS [6] and RLS [7]. The EQ just needs to know the signal mapping technique and then estimate the channel effects accordingly. There are different algorithms, including CMA, MMA and SCA.

1.1 LMS compensation

LMS [6] is the most common form of adaptive equalization. The LMS uses a stochastic gradient descent to update the equalizer weights during operation. The complex version of the LMS-EQ is used for every complex channel gain and is given by

$$z(k)=\omega^{T}(k)x(k) \qquad (1)$$

z (k) represents the output of the given adaptive equalizer and is equal to the product of the received signal and the weight of the given equalizer.

$$e(k) = s(k) - z(k) \qquad (2)$$

The estimate of the error is shown in the equation. 2 times e (k) while s (k) shows the desired signal. Subtracting the equalizer gain z (k) from the desired signal s (k) would give us the estimate of the system error. The update of the system weight can be calculated as follows

1.2 Recursive Least Squares

The RLS (Recursive Least Squares) algorithm is a different type of adaptive algorithm that is more computationally complex than its LMS counterpart. The performance of an RLS equalizer can be calculated using the following formula

While the two equations 4 and 5 are used together to compute K (k) the gain vector. The

λ, which represents the forgetting factor, has a value close to 1. λ, the weighting factor, gives the old samples less weight than the new ones and ignores the previous ones.

2. PROPOSED SYSTEM DESIGN

2.1 Multi-module algorithm

The Multiple Modulus Algorithm (MMA) [12] [18] is the advanced form of the older CMA algorithm. In the old CMA, the real and imaginary parts of the output of an equalizer had to be separated. In MMA, too, the real and imaginary parts are separated in order to obtain the cost function, which can be represented mathematically as

$$J_{MMA}=E\{(|z_{kr}|^p-R_{MMA^p})^2+(|z_{ki}|^p-R_{MMA^p})^2\}$$

In equation 10, E denotes the expectation operator, *zkr* denotes the real part and *zki* denotes the imaginary part of the output of the equalizer for the k-th value. "P" mentioned in the equation indicates an integer required for calculation.

$$R_{MMA^p}=E\,|\,s_{kr}\,|^{2p}/E\,\{|\,s_{kr}\,|^p\}=E\,|\,s_{ki}\,|^{2p}/E\,|\,ski\,|^p$$

$$e_k=z_{kr}\,|\,z_{kr}\,|^{p-2}(|\,z_{kr}\,|^p-R_{MMA^p})+jz_{ki}\,|\,z_{ki}\,|^{p-2}(|\,z_{ki}\,|^p-R_{MMA^p})$$

RMMAp is known as the statistical Goddard constant. While Skr is the real part of the equation, Ski is the imaginary part of the equation. In a complex constellation, the equalizer offset is visible to the MMS Cost Function (RMMA ± ± jRMMA) to 4 pints and can as a sum of two cost functions expressed are. We can increase the performance of the MMA equalizer by increasing the pa value at the expense of increasing complexity. For simplicity and convenience, we choose 2 as the p-value.

3. RESULTS AND COMPLETION OF THE SIMULATION

3.1 Constellation diagrams for different algorithms

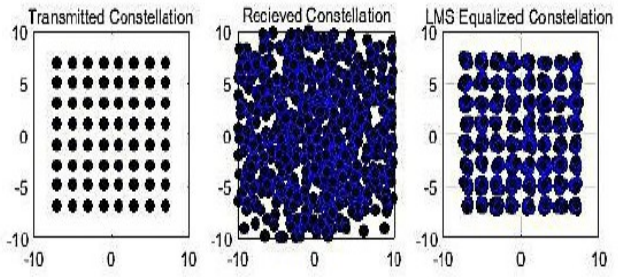


Fig. 1: LMS equalization algorithm in the 64-QAM constellation

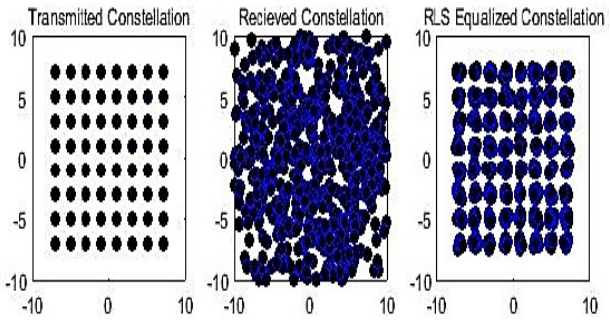


Fig. 2: RLS equalization algorithm in the 64-QAM constellation

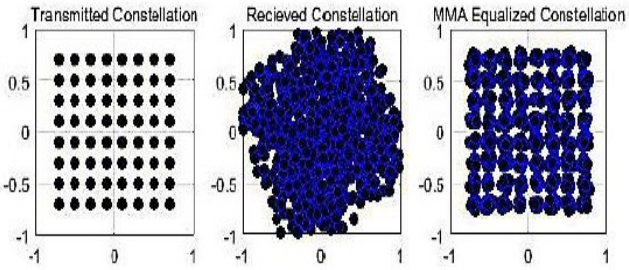


Fig.3: MMA equalization algorithm in the 64 QAM constellation

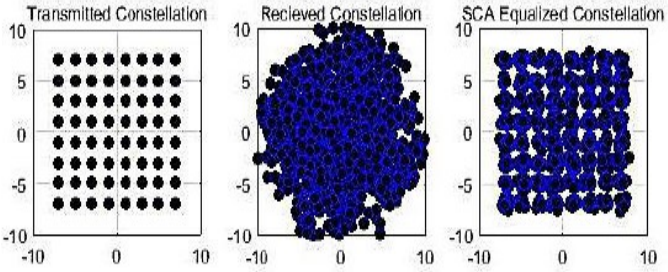


Fig. 4: SCA equalization algorithm in the 64 QAM constellation

In the graphics above, the left side represents the original signal transmitted to the receiver, the figure in the middle represents the distorted and phase-shifted signal due to the channel values and AWGN in the middle. This leads to a distorted and shifted signal at the ISI receiver. Now to extract the original signal we apply each of the algorithms and the figure on the right in each of the graphs is the balanced signal.

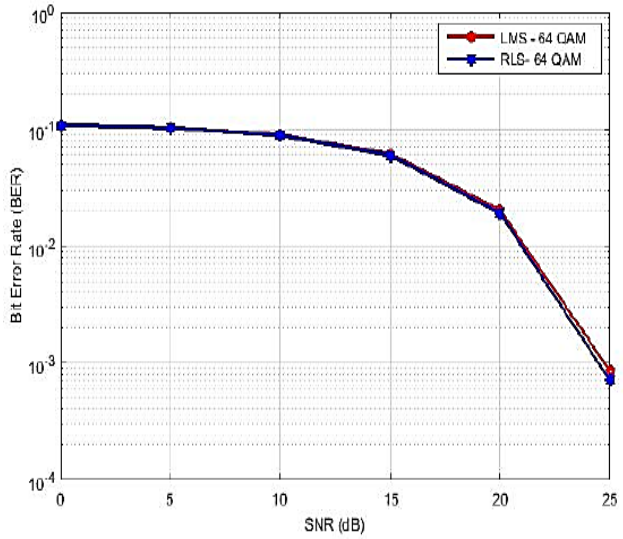


Fig. 5: BER comparison of the LMS and RLS algorithms for a 64 QAM constellation

To compare the BER of the LMS and RLS for the 64-QAM constellation, we need to compare the two graphs. We can see that the values remain almost the same up to 20 dB, above which the RLS shows a slight improvement in the BER, while the BER drops significantly by around 25 dB.

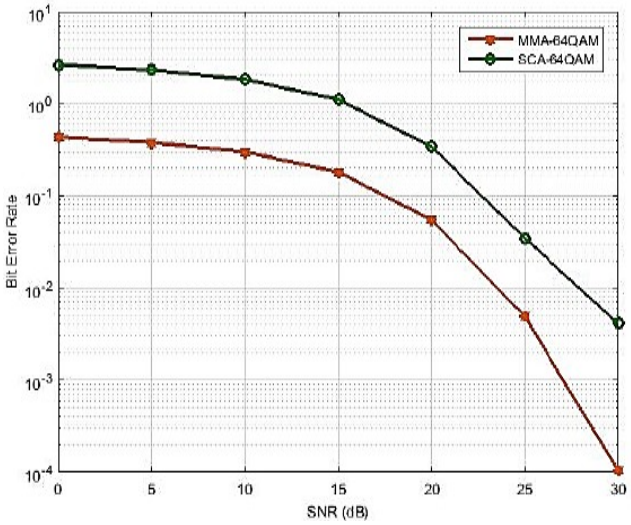


Fig. 6: BER comparison of MMA and SCA algorithms for a 64-QAM constellation

The above graph shows the comparison of MMA and SCA for the 64-QAM constellation, and we can see the very significant difference in the performance of the two blind equalization algorithms.

3.2 ISI residual comparison of LMS and RLS for 64-QAM

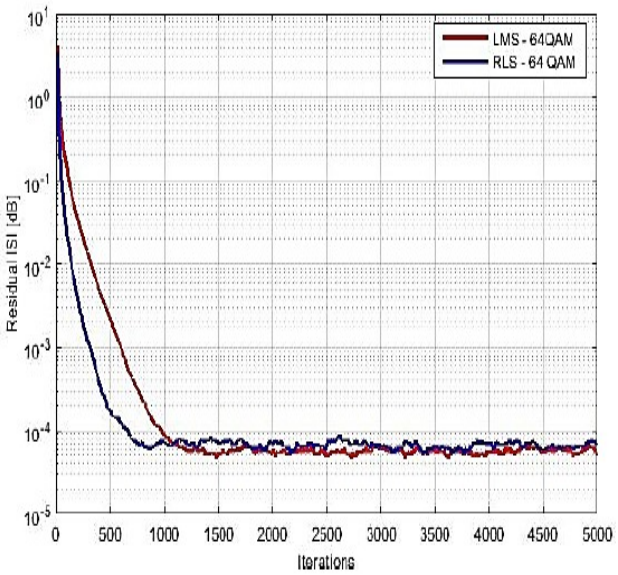


Fig. 7: ISI residual comparison of LMS and RLS algorithms for a 64-QAM constellation

In the graphic above we can see the remaining ISI comparison of the two learning algorithms for 64 QAM constellations. The RLS in the graph above has a better rate of convergence than the LMS and about 700 iterations. The SPI can be seen as stabilizing. While the LMS takes a long time to converge and requires around 1000 iterations to stabilize.

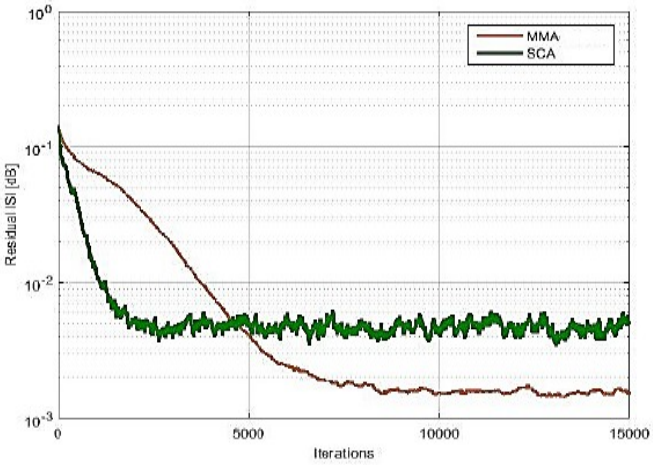


Fig. 8: Residual ISI comparison of the MMA and SCA algorithms for a 64 QAM constellation

4. CONCLUSION

The graphic above shows the blind algorithm comparison of MMA and SCA for a constellation of 64 QAM. However, the rate of convergence of MMA is very high than that of SCA; The performance of SCA on MSE is

much better than that of MMA. It takes about 200 iterations for MSE to stabilize while SCA takes about 8,000 iterations to stabilize. Therefore, for a static system with 64 QAM, SCA should be the first priority. However, the RLS offers the best performance in terms of BER, MSE and residual ISI. Because of its complexity and slow rate of convergence, the EPIRB may be preferred for wireless systems with relatively static nodes. In the blind equalization algorithm, however, the general MMA is better than the SCA. Like RLS, SCA requires complex calculations and sometimes gives better ISI results, but is more expensive. In summary, a balancing algorithm should be used on a case-by-case basis or a dynamic wireless communication system that can quickly switch between these algorithms depending on the environment to ensure a smooth flow of communication.

REFERENCES

1. Kavitha, Veeraruna, and Vinod Sharma. "Comparison of training, blind and semi blind equalizers in MIMO fading systems using capacity as measure." In Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP'05). IEEE International Conference on, vol. 3, pp. iii-589. IEEE, 2005.
2. Sharma, Prachi, Piush Gupta, and Pradeep Kumar Singh. "Performance Comparison of ZF, LMS and RLS Algorithms for Linear Adaptive Equalizer." International Journal of Advanced Computer Science and Applications 2, no. 3 (2016).
3. J.R. Treichler, M.G. Larimore and J.C. Harp, “Practical Blind Demodulators for High- order QAM signals", Proceedings of the IEEE special issue on Blind System Identification and Estimation, vol. 86, pp. 1907-1926, Oct. 1998.
4. Zhang, Haijun, Yang Shi, and A. Saadat Mehr. "Robust equalisation for inter symbol interference communication channels." Signal Processing, IET 6, no. 2 (2012): 73-78.
5. Chung, G. C., S. S. Thwin, and Mohamad Yusoff Alias. "Statistical distribution of UWB signals in the presence of inter-symbol interference." InSustainable Utilization and Development in Engineering and Technology (CSUDET), 2013 IEEE Conference on, pp. 60-62. IEEE, 2013.
6. Wang, Yuanquan, Rongling Li, Yiguang Wang, and Ziran Zhang. "3.25-Gbps visible light communication system based on single carrier frequency domain equalization utilizing an RGB LED." In Optical Fiber Communication Conference, pp. Th1F-1. Optical Society of America, 2014.
7. Wei si yuan,”Blind Equalization for Qam signal based on the dual mode algorithm,science direct,pp34-37.
8. Shafayat Abrar and Roy A. Axford Jr.,”Sliced Multi Modulus Algorithm” ETRI Journal, Volume 27, Number 3, June 2005.
9. Jalali, Sammuel. "Wireless Channel Equalization in Digital Communication Systems." (2012).

GENETIC ALGORITHM FOR VLC BASED ON MIMO-OFDM WITH LOW SIGNAL-TO-NOISE RATIO AND IMPROVED FITNESS FACTOR OF MULTI-USER

R.Mounika[1]., Y. Saritha Kumari[2].,

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (: mounikarayaram001@gmail.com)

2 Assistant Professor, Department of H & S., Malla Reddy College of Engineering., Maisammaguda Medchal., TS, India.

Abstract— The three parameters transmission range, transmission speed and reliability are used to characterize the quality of service of a wireless communication system. In conventional OFDM configurations, one of the above parameters can add to the cost of the degradation of two other parameters. However, by consolidating MIMO with OFDM systems, all of these parameters can be improved at the same time. The two most important functions of the MIMO OFDM system are symbol recognition and channel estimation. These functions can be performed by various algorithms, such as B. the maximum likelihood (ML) detector, the least squares (LS) detector, etc. The complexity of these algorithms is very high in the system with a large number of transmitters and receivers and with a large cluster size. We propose a genetic algorithm for VLC based on MIMO-OFDM and examine its signal-to-noise ratio (SNR) for many LED configurations. Rectangular LED framing provides better signal-to-noise ratio than linear framing for higher order modulation schemes

Keywords— MIMO-OFDM, GA, VLC, LEDs, SNR.

1. INTRODUCTION

Due to its high spectral efficiency, its high signal-to-noise ratio (SNR) and, in contrast to ISI, orthogonal frequency division multiplexing (OFDM) is a suitable technique for handling higher data transmission rates in VLC [1]. With MIMO indoor multi-input multi-output (VLC) technology, an improved data rate (Rb) can be achieved without the need for additional bandwidth expansion, while at the same time improving the channel strength. Implement a VLC based on MIMO images to combat distortion caused by multipath and increase data transfer rates. In this article, a MIMO-OFDM-VLC system with a genetic algorithm is investigated in order to meet the requirements of real and non-negatively transmitted signals in the optical domain. The ray tracing algorithm [2] is used to to evaluate the characteristics of the MIMO multipath channel and also the impulse response - to evaluate parameters of the channel, to obtain the channel gain matrix. We examine rectangular and linear LED frames in a room environment and analyze the BER distribution in the receiver level. We show that with the proposed system a data transfer rate Rb of 1.2 Gbit / s couldachieved [3].

II.PROPOSED SYSTEM MODEL

The block diagram of the VLC system module can be given as shown in the figure: 1. The concept of the VLC depends on the intensity modulation (IM) and the forward detection (DD) so the information bits are displayed as a symbol which then modulates the intensity of the visible light generated by the LED driver circuit through the LED array. Photo detectors (PD) are used at the receiver to identify signals transmitted over optical channels. An optical concentrator and an optical filter are used in front of the photo detector. When the opto-electrical (optical to electrical) conversion is performed, the data is received by the photo detector, it is demodulated, and then the original information bits are restored after amplification.

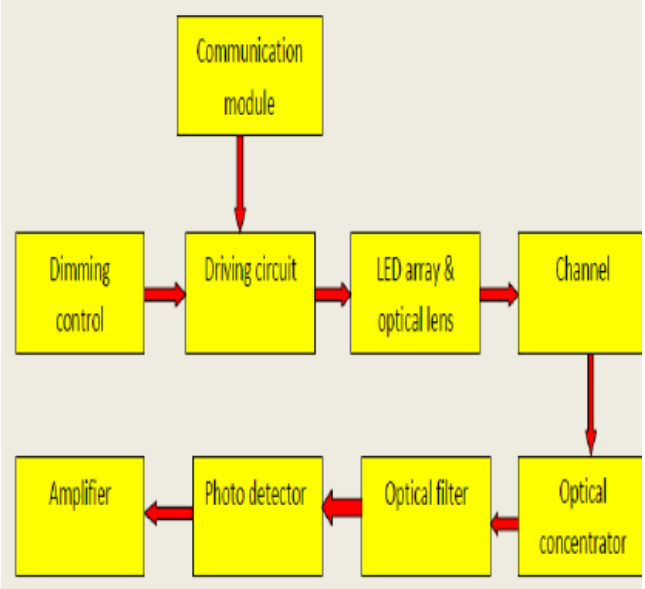


Figure 1: Function diagram of the VLC system module [4]

The source information bits are named adaptively to the profile signal. The profiled signal from each subcarrier in the system is then multiplied by its matrix of interdependent channels, after which an inverse fast Fourier transform (IFFT) is performed in parallel with the serial conversion (P / S) and prefix insertion. Cyclic (CP) to restore the signal in the time domain [9]. For channel estimation on the receiver side, pilot symbols are also inserted into the signal. Second order Butterworth filters are used as the LPF (Figure 2). The DC bias voltage controls the LED after the digital-to-analog conversion.

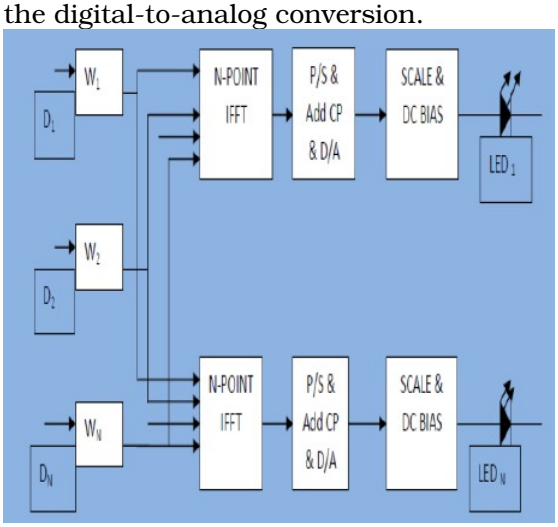


Figure 2: MU-MIMO-VLC-SYSTEM

The nonlinear behavior of the LED is mandatory for the optical OFDM due to its sensitivity to the resulting distortion, so we consider the nonlinear behavior of the LED in this approach. The non-linearity of property IV of the LED is also suggested by the scheme under consideration. The IV curve, which is created using the data specifications in the LED data sheet (OSRAM LUW W5AM), is shown in Figure 3.

III.RESEARCH METHODOLOGY

Channel estimation checks the capacity of the transmission channel to analyze the amount of data that can be transmitted through it. Since the system bandwidth is fixed, a check is also made to see if there is another option that can increase the capacity of the channel. The bandwidth plays a fundamental role in the choice of the transmission speed in the network. It is decided to avoid the collision between two signals. There are different channel estimation schemes such as LS (Least Square), MMSE (Least Mean Square Error), DFT (Discrete Fourier Transform) etc.

The main aim of this research work is to improve the above schemes by using the genetic algorithm (GA). The results of the algorithm are compared to the subcarrier matrix based on the signal-to-noise ratio parameters to calculate the percentage improvement. The research framework is illustrated in Figure 4, which outlines the steps required to complete the proposed work.

Proposed genetic algorithm

The genetic algorithm presents the process of natural selection in a specific method to generate solutions to research and optimization problems, regardless of whether these are limited or not. The basic principle of the genetic algorithm is the feasibility of the population of coded solutions to various time-consuming optimization problems. It is a class of transformation algorithms with which optimal solutions can be achieved using methods that have been intrigued by natural evolution, such as inheritance, mutation and crossing [16]. The genetic algorithm uses three basic principles to generate the next generation from the current population, as shown in Figure 3.

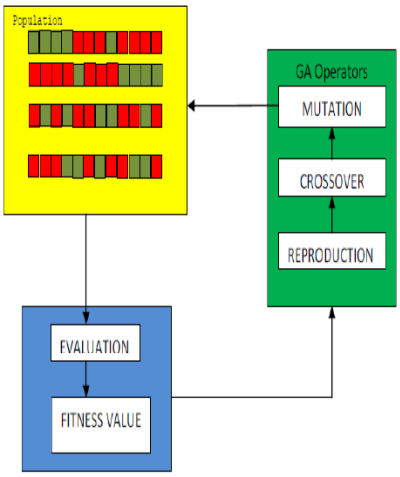


Figure 3: Evolution flow of the genetic algorithm

The final step in applying the genetic algorithm is to select the best genotypes, which have a very important key role in selecting the group of individuals known as genesis that will contribute to the next generation of the population. They bring their genes, the inputs into their vectors, into their next generations. These individuals are selected using the method based on physical condition, generally choosing the most appropriate or best solution.

IV. RESULT ANALYSIS

The spectral efficiency of each subcarrier in the configuration with an average optical transmit power P = 1 watt (0 dBW) is managed in the case of MIMO OFDM with the minimum DC bias for each transmitter, as shown in Figure 5, symmetry is applied in the system, there is only Subcarriers from 1st to 31st that contain effective information. It is analyzed that as the subcarrier index increases, the spectral efficiency improves completely if the minimum IF-MMSE DC polarization is used.

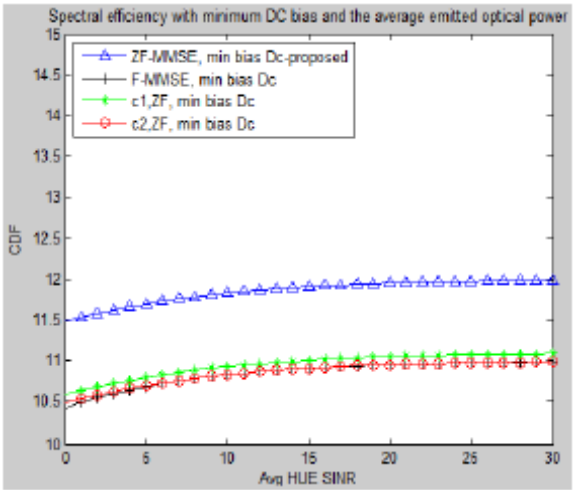


Figure 4: Spectral efficiency with minimal asymmetry and average emitted optical power

The result shows that the channel capacity of the MIMO OFDM system improves when the solution to mitigate spectral efficiency is implemented in order to maximize the capacity used to allocate different power levels to the devices. For the DFT correlated with the GA algorithm in the MIMO channel, the MIMO capacity is for fixed values of the tuning length compared to the increase in the number of transmitting and receiving antennas.

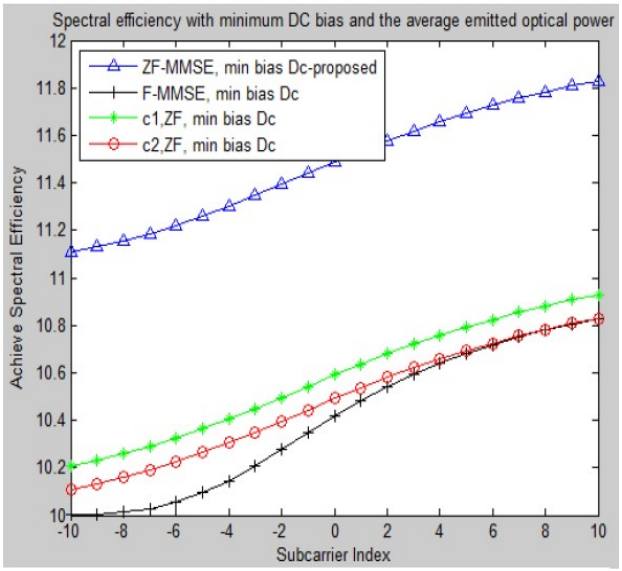


Figure 5: Spectral efficiency with minimal DC polarization and average emitted optical power.

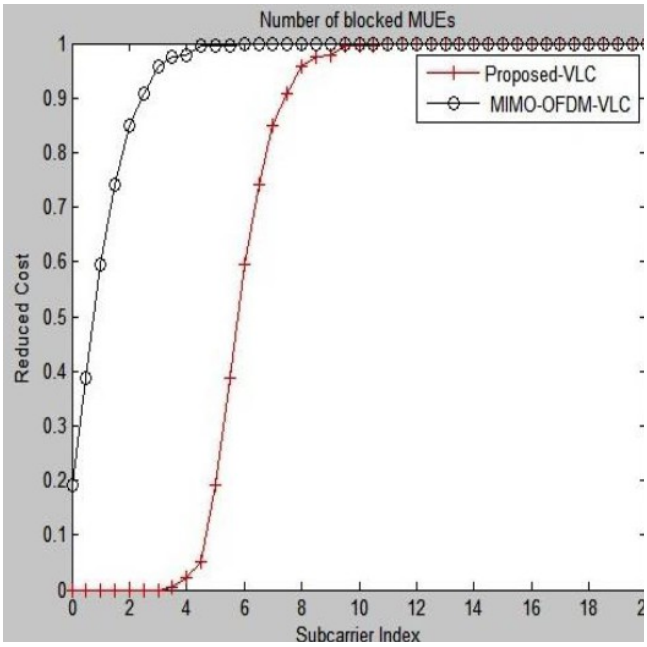


Figure 6: Proposal for reducing costs for MIMO-OFDM-VCO and VLC

V. CONCLUSION

The aim of this document was to provide an inexpensive and more efficient communication system for visible light. The idea was to design and implement a visible light communication system that multiplexed orthogonal frequency division inputs with multiple outputs and multiple outputs associated with a generic algorithm to provide a low cost system with an improved physical form factor. The combination of MIMO and OFDM has become a promising solution for future high-speed wireless communication systems. The configuration was designed to use software defined radios, which allowed for quick and easy implementation, as well as tremendous capabilities for changing communication link parameters. SDR appliances have also enabled the use of open source software, which allows for an inexpensive implementation. The deployment platform chosen was a good choice, but it took many man hours to install all of the software and learn how to use it properly. After working with the software, future use of the software will be very easy. This document is intended to help and clarify future work.

REFERENCES

1. A.H. Azhar, Tuan-Ann Tran and D. O'Brien, "Demonstration Of High-speed Data Transmission Using MIMO-OFDM Visible Light Communications" GLOBECOM Workshops, 2010 IEEE, pp.1052-1056.
2. Rajbir Kaur, Charanjit Kaur, "Investigation on Channel Estimation techniques for MIMO- OFDM System for QAM/QPSK Modulation", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, Sep 2012, pp. 1419-1424.
3. A.Burton, H. Le Minh, Z.Ghassemlooy, E. Bentley and C. Botella, "Experimental Demonstration Of 50-Mb/S Visible Light Communication using 4◇4 MIMO," IEEE Photonics Technology Letters, Vol. 26, May 2014, pp.945-948.
4. Naveen Kumar, N. Lorenco,Spiez.M , AguiasRL, "Visible Light Communication & VIDAS," IETE Technical Review, Vol 25, issue 6 , Dec 2008, pp 359-367.
5. H. Elgala, R. Mesleh, and H. Haas, "An LED Model For Intensity Modulated Optical Communication Systems," IEEE Photonics Tech. Letter, vol. 22, No. 11, June 2010, pp. 835–837.
6. Yang Hong, Tesi Wu and Lian-Kuan Chen, "On the Performance of Adaptive MIMO-OFDM Indoor Visible Light Communications" IEEE, 2015, pp. 1-4.
7. Y. Zhao and A. Huang, "A Novel Channel Estimation Method For OFDM Mobile Communication Systems Based On Pilot Signals And Transform-Domain Processing", IEEE 1997, pp 2089-2093.

8. H. Minn and V.K. Bhargava, “An Investigation into Time-domain Approach for OFDM Channel Estimation”, IEEE Transactions on Broadcasting, Vol 46, Issue 4, Dec 2000, pp 240–248.
9. Q. Gao, C. Gong, S. Li, and Z. Xu, “DC-Informative Modulation For Visible Light Communications Under Lighting Constraints,” IEEE Wireless Communication, vol. 22, No. 2, Apr. 2015, pp. 54–60.
10. Abhinav Johri, Farooq Husain, Ekta Agarwal "A Review: Visible Light Communication using MU-MIMO-OFDM", SSRG International Journal of Electronics and Communication Engineering (SSRG - IJECE), V4 (4), 16-20 April 2017.

DESIGN OF VOLTAGE LEVEL SHIFTER FOR HIGH SPEED DUAL SUPPLY CIRCUITS WITH POWER OPTIMIZATION

M.Uppa Mahesh[1]., V. Narasimha[2].,

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: maheshuppa18may@gmail.com)

2 Assistant Professor, Department of H & S., Swamy Ramanadatheerda Institute of Engineering and Technology., Nalgonda., TS, India.

Abstract— Reducing energy consumption has always been the primary goal of digital energy harvesting devices. An effective way to use different voltages in the low power design depends on their speed. However, this enables the use of an interface block called a level converter or level shifter. This article contains a modified structure of the level shifter for a low power implementation. The results of the simulation of the proposed structure in 0.18 µm CMOS technology show that the level shifter has a propagation delay of 12.5 n and a power dissipation of at a low input supply voltage of 0.4 V and a high supply voltage of 1.8 V 87.7 nW for an input signal of 1 MHz. These level changers are used to compare the product of power delay, speed and power

Keywords CMOS, level converter, subthreshold operation, Dual supply circuits, power delay product.

1. INTRODUCTION

Energy efficiency and speed are an important performance factor in all digital circuits. Various techniques have been used to reduce dynamic and static performance. On the other hand, lowering the supply voltage increases the propagation delay of the circuits [2]. To avoid these problems, a dual-power architecture is introduced in which a low voltage (VddL) is supplied to the blocks on the non-critical paths, while a high supply voltage (VddH) is applied to the analog and digital blocks. Speed. Some of the most commonly used techniques are dynamic voltage scales, which operate close to threshold voltage levels and support multiple voltage ranges. For this reason, a level shift circuit is needed to provide the precise voltage level of the circuit. A voltage level shifter is one of the main components of a digital system. Level shifters are used to provide the correct voltage level for each component in digital circuitry.

The voltage level conversion is necessary if two devices have different supply voltage nodes. There are two possible conditions. A higher voltage device may be required to drive a lower voltage device. A low voltage device may be required to control a high voltage device.

Fig-1: Operation of the voltage level changer

2. IMPLEMENTATION OF THE EXISTING LEVEL CHANGE

This section briefly explains the circuit configuration and advantages of the two-stage converters described recently. The operation of the circuit shown in Fig. 2 is as follows. When the input signal goes high, transistor Mn1 turns on and nmos transistor Mn4 turns on because the overdrive voltage of Mp3 is higher than Mn3. Therefore, the transient current Mp1, Mn1 and Mn4 flows, and this current is mirrored in Mp2 against and attempts to move the output node upwards. Eventually the output will go high and transistor Mp3 will turn off, so nmos transistor Mn4 will be lowered by nmos transistor Mn3 which means there will be no static current flowing through Mp1, Mn1 and Mn4.

When the input is low and INB is high, the nmos transistor Mn2 conducts and lowers the output node at the same time, the nmos transistor Mn1 turns off and no static current flows. This means that the current of Mp2 is not completely close to the existence of a weak limit of zero. Another reduction in current value is being used by another Mp4 device.

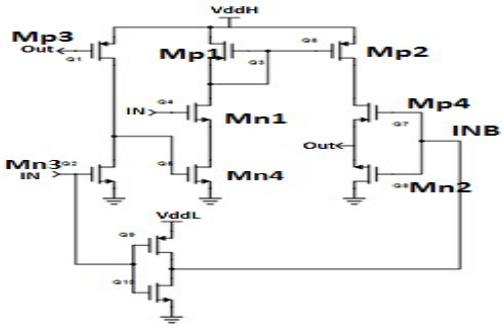


Fig-2: Schematic representation of the voltage level changer [1]

2.1 Extension Of The Step Changer With Additional Circuit

To further reduce power and delay, a voltage level changer extension with auxiliary circuit is used (see Figure 2). The auxiliary circuit only changes the high-low transition of the input signal and increases node Qc to a value greater than VddL. Transistors Mn6, Mn7, and Mp6 turn on and nmos transistor Mn5 turns off so the transient current flowing through Mn6, Mn7, Mp6 are mirrors of Mp7 and raise the QC node.

3. PROPOSED SYSTEM OF VOLTAGE EXCHANGE CIRCUIT

A new voltage level changer with power optimization is presented. This is where the power activation technology is implemented to optimize the performance.

Power gating is the most widely used circuit design technique in industrial products. It means connecting the suspension transistor to a combination of pull-up-pull-down network to reduce the leakage current below the threshold. A suspension transistor separates the pull-up network from Vdd and the pull-down network from Vss.

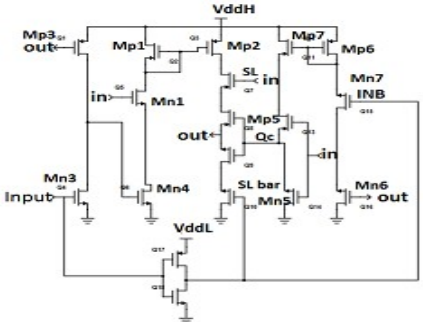


Fig. 3: Proposed voltage level variator

The sleep transistor SL disconnects the mp transistor from Vdd and the bar SL disconnects the nmos transistor Mn5 from Vss. During the active mode SL = 0, the dormant transistor turns on and provides a low resistance in the conduction path. Circuit in standby mode SL = 1 disconnected from the power supply by a power switch.

4. SIMULATION RESULTS

The voltage level shifter design in Figure 1 was implemented at 180 nm using virtuous cadence software. Then the transient analysis as in FIG. 5 is obtained.

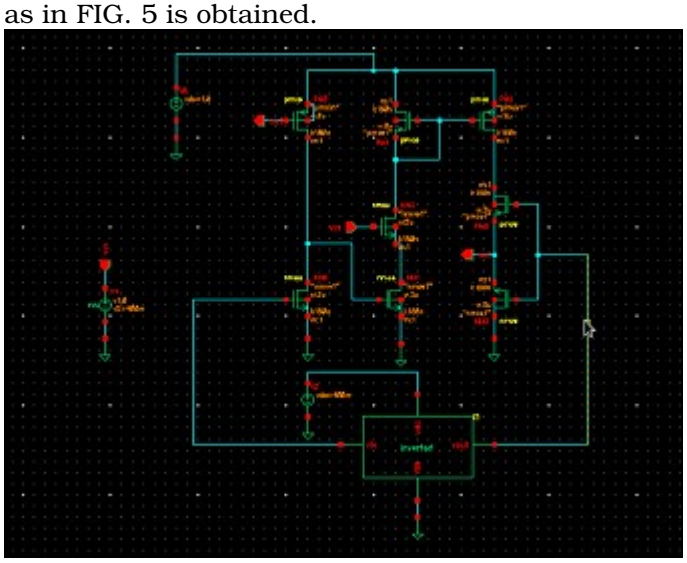


Fig-4: Implementation of the voltage level changer

The power consumption of the voltage level changer can be divided into two areas: static power consumption and dynamic power consumption. Static power dissipation due to leakage current in integrated CMOS circuits. The leakage capacity is only minimized in standby mode. This is less than the dynamic power dissipation that occurs due to the charging and discharging of the charging capacity. A total power consumption of the voltage level changer of 172.9 nW was determined for the 180 nm technology. The voltage level changer delay was 62.1 ns.

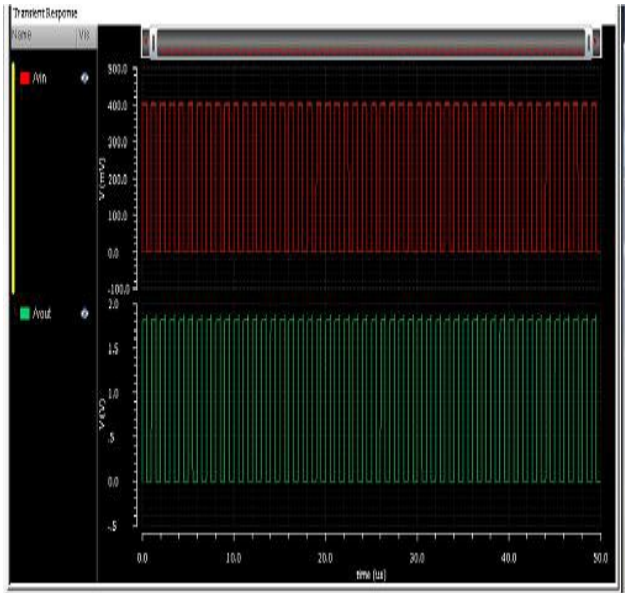


Fig. 5: Transient analysis of the voltage level changer

To further reduce power and delay, the voltage level changer is expanded to include the auxiliary circuit [1]. In Fig. 6 a level changer with auxiliary circuit has been implemented and the power and the delay have been calculated.

The proposed new optimized supply voltage level changer has been implemented in Figure 6. The average power consumption was 87.57 nW. The performance is reduced to 50% compared to other level change designs. The leakage power has been compressed by the current activation technology.

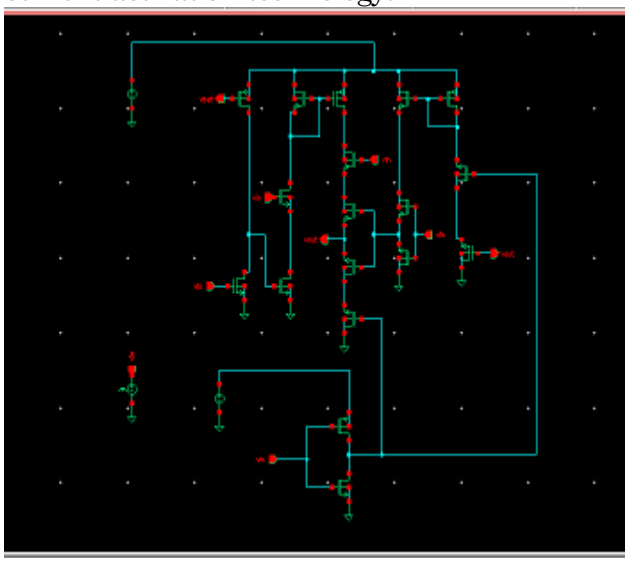


FIG-6: Implementation of the proposed voltage level changer

The simulation results were compared in the table: 1.

Table 1: Comparative results of voltage level changers

Designs(180nm)	Average power(nW)	Delay(ns)	Power Delay Product (nW.ns)
Existing voltage level Shifter	172.9nW	62.1ns	10737.09
Level Shifter with Auxiliary circuit	166.01nW	12.1ns	2008.721
Proposed Voltage Level Shifter	87.57nW	12.5ns	1094.625

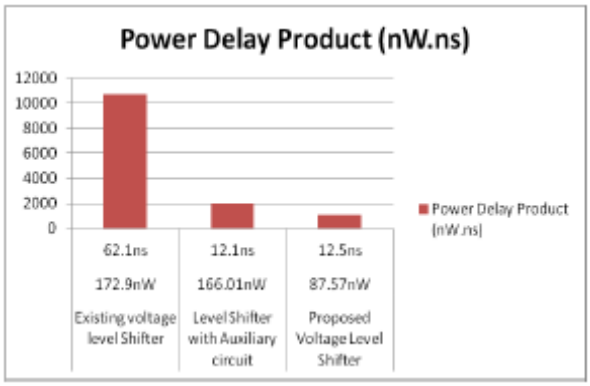


Fig 7: Histogram representation of the simulation result

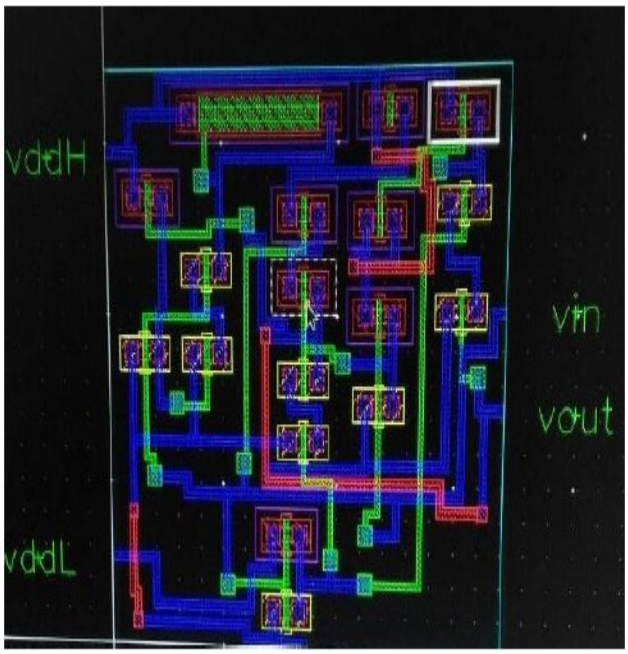


Fig. 8: Implementation of the proposed constraint design

5. CONCLUSION

In this specification, a design has been proposed for a fast and low change in supply voltage level that can convert extremely low

values of input voltages . The existing and proposed designs were simulated using virtuous cadence tools. The average power dissipation of the proposed design has been halved compared to the existing voltage level changer. The average power loss was 87.5nW. The PDP of both designs is measured and for the proposed design as a minimally found.

REFERENCES

1. S. Lütkemeier and U. Rückert, "A subthreshold to above-threshold level shifter comprising a Wilson current mirror," IEEE Trans. Circuits Syst. II, vol. 57, no. 9, pp. 721–724, Sep. 2010.
2. K. Usami et al., "Automated low-power technique exploiting multiple supply voltages applied to a media processor," IEEE J. Solid-State Circuits, vol. 33, no. 3, pp. 463–472, Mar. 1998.
3. A.Wang and A. P. Chandrakasan, "A 180-mV subthreshold FFT processor using a minimum energy design methodology," IEEE J. Solid-State Circuits, vol. 40, no. 1, pp. 310–319, Jan. 2005.
4. M. Lanuzza, P. Corsonello, and S. Perri, "Fast and wide range voltage conversion in multisupply voltage designs," IEEE Trans. Very Large scale Integr. (VLSI) Syst., vol. 23, no. 2, pp. 388–391, Feb. 2015.
5. Y. Osaki, T. Hirose, N. Kuroki, and M. Numa, "A low-power level shifter with logic error correction for extremely low-voltage digital CMOS LSIs," IEEE J. Solid-State Circuits, vol. 47, no. 7, pp. 1776–1783,Jul. 2012.
6. Seyed Rasool Hosseini, Mehdi Saberi, and Reza Lotfi A High-Speed and Power-Efficient Voltage Level Shifter for Dual-Supply Applications Oct. 2016.
7. S. Rasool Hosseini, Mehdi Saberi and Reza Lotfi, "A Low-Power Subthreshold to Above-Threshold Voltage Level Shifter", IEEE Trans. Circuits Syst. II, vol. 61, no. 10, pp. 753–757, Oct. 2014.

CNT FET BASED SHIFT REGISTER DESIGN IN HSPICE. BASED ON PULSED LATCH SENSE AMPLIFIER

A.Anil Kumar[1]., L. Prashanth[2]

1 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: anumula86@gmail.com)

2 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: prashanthlukkalpr@gmail.com)

Abstract— Power consumption and area reduction in the past few days are the main concerns in circuit design. The change log is a fundamental component of storage devices. This design reduces the performance of the shift register by using pulse latches instead of flip-flops. Because flip-flops based on a shift register use more energy. Pulsed bars developed with Carbon Nano Tube technology. CNTFET technology is one of the best replacement products for CMOS technology due to its excellent properties such as high thermal conductivity, small atomic diameter of carbon and high tensile strength. Here the shift register is based on pulse locks using CMOS technology and the CNTFET technology has been compared. This shift register was implemented in the 32 nm CNTFET technology in HSPICE.

Keywords— Pulsed latch, Shift register, Flip-flop, CNTFET memory devices.

1. INTRODUCTION

In the past, VLSI designers have focused on speed and cost. The consideration of power is the second in question. Today, power supply will someday be the primary concern due to the remarkable growth and success in the field of battery operated devices such as laptops, cell phones, tablets, etc. The motives for reducing energy consumption vary from application to application.

Various techniques are available for minimizing energy. There are three components responsible for power loss in a circuit: short-circuit power, dynamic power and static power. Dynamic power is the main power consumed in charging and discharging capacitors.

Pdynamic = CL VDD2 α f … (1)

Shift registers are a sequential logic circuit. It is used to change binary information and can also save that binary information. Therefore, only shift registers are basic building blocks in storage devices.

2. LITERATURE SURVEY

Elio Consoli, et al. (2012) [1] present Flip-Flops (FF) are key elements in the design of energy-efficient high-speed microprocessors because their data on output delay (DQ) and power dissipation have a strong influence on the processor clock period and overall performance. Over the past several years, the Transmission Gate Pulse Latch (TGPL) [3] has proven to be the most energy efficient FF in much of the design field, from high speed product designs to EDs. Minimum (power delay), while the master-slave FFs (TGFF and ACFF) are the most energy efficient in the ED space area with low power consumption. TGPL also has the lowest DQ delay with STFF. However, the latter therefore has a considerably poorer energy efficiency; The TGPL is the best reference for comparison. Seongmoo Heo, et al. (2007) [2] introduced new techniques for evaluating the performance and delay of latch and latch designs and showed that no existing design performs well in the wide range of operating states present in the systems. We offer the use of a selection of latch and toggle models, each tailored to different trigger models and speed requirements. We demonstrate our technique on a channeled MIPS processor data path on which SPECint95 performance tests are run. In doing so, we reduce the entire switchover and latch performance by over 60% without extending the cycle time. Bai Sun Kong et al. (2001) [4] presented a family of novel low-power flip-flops, collectively referred to as conditional capture flip-flops (CCFF). They enable statistical performance reduction by

eliminating redundant junctions from internal nodes. These flip-flops also have a negative settling time and therefore provide small data for the output latency and the soft edge attribute to overcome the cycle time loss associated with clock drift. The simulation comparison shows that the proposed differential flip-flop offers an energy saving of up to 61% without affecting the latency, while the asymmetrical structure offers a maximum energy saving of about 67% compared to conventional flip-flops. Borivoje Nikolic et al. (2000) [5] presented an experimental setup and evaluation of a new type of flip-flop (SAFF) based on sense amplifiers. The main speed bottleneck in existing SAFFs has been found to be the coupled setpoint reset interlock (SR) on the output stage. The new flip-flop uses a new locking topology on the output stage which drastically reduces delay and improves maneuverability. The performance of this flip-flop is verified by measurements on a test chip implemented by CMOS with an effective channel length of 0.18 µm. Umiing KO et al. (1996) [8] presented the performance, performance and energy efficiency of various CMOS master-slave D-flip-flops (DFF). To improve performance and energy efficiency, push-pull DFF and push-pull isolation DFF are offered. Of the five DFFs compared, the proposed push-pull isolation circuit is the fastest with the best energy efficiency.

3. EXISTING SYSTEM

Important shift register parameters such as area, power and delay can be reduced with the latch. Pulsed lock means the combination of a lock and a pulsed clock generator. Figure 3 shows the latch circuit depressed. The pulsed flip-flop has a small number of transistors compared to the flip-flop. Therefore, the shift register area is reduced. The pulse lock is a lock that can capture data for the specified time defined by the width of the clock waveform. Pulse locking uses a narrow clock pulse so that important low power properties such as: B. Cycle performance are low.

4. PROPOSED SYSTEM DESIGN

Pulse clock signal generated in a pulse clock generator consisting of delay and AND gate circuits. The clock pulse width in the conventional pulse clock generator is greater than the sum of the rise and fall times. However, the delayed pulse clock generator generates a pulse width that is smaller than the sum of the rise and fall times.

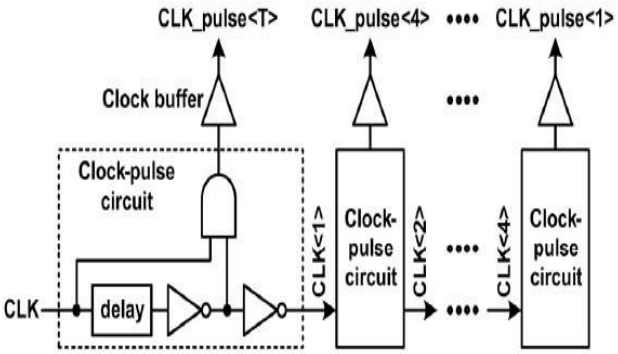


Fig. 1: Pulsed clock generator.

Because each shape has pulsed clock signals generated by the AND gate and two delay signals. Therefore, only this delayed pulse clock generator is suitable for generating a narrow clock pulse.

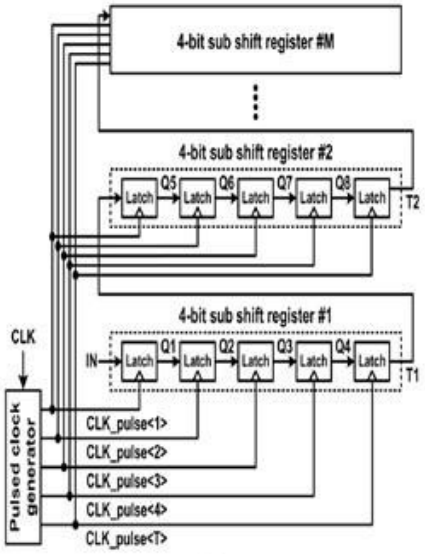


Fig. 2: Shift register using SSASPL.

The 4-bit shift register is considered here. Usually the shift register is divided into four types as follows: Serial In Serial Out (SISO), Serial In Parallel Out (SISO), Parallel In Serial Out (PISO), Parallel in Parallel Output (PIPO). The following figure shows the proposed shift

register based pulse latch using a CNTFET. It has three connections for data transfer operations. The proposed change registers contain five locks in series. The data is blocked. The exit of this lock is connected to the next lock. The extra latch in the shift register is output to temporarily store the data and then sent to the next latch in the next shift register. The first type is the Serial Serial Output Shift Register (SISO), which accepts serial data and outputs data to the serial output. The following diagram shows the serial output shift register with CNTFET.

5. SIMULATION AND RESULTS

This section contains the simulation of the shift register using a toggle switch. Shift register with PPCFF simulation as in Fig.

Pulse locking on the sense amplifier is used in the shift register. Requires a pulsed clock signal and two differential inputs. 17 transistors are required in which the M1-M10 transistors are used to generate the pulsed clock signal. The remaining transistors M11-M17 represent the pulse locking operations of the sense amplifier.

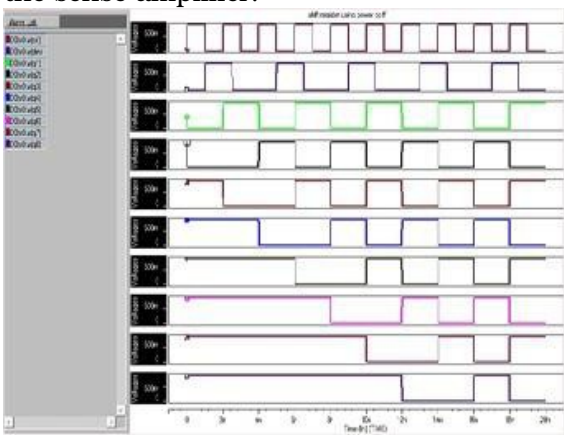


Fig. 3: Change log with PPCFF.

Simulation of the pulse clock generator as in Fig. The clock input is passed to the inverter, followed by the AND gate and the buffer. The buffer is used to temporarily store data and then send it to SSASPL in the shift register.

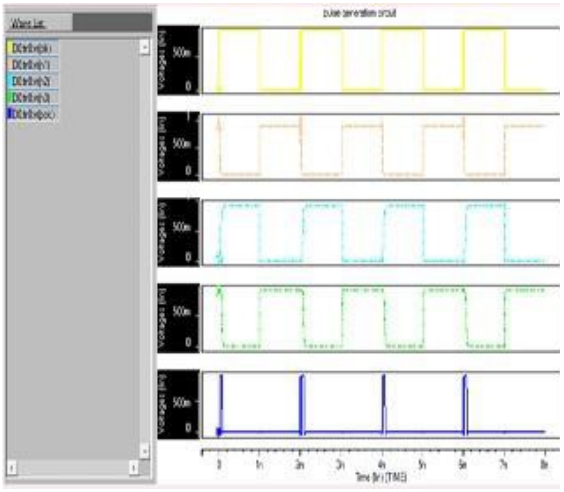


Fig. 4: Waveform of the pulse clock generator.

The output of the pulsed clock generator is sent to the input of the NMOS transistor in SSASPL. The waveform of the SSASPL is shown in Fig. 2.

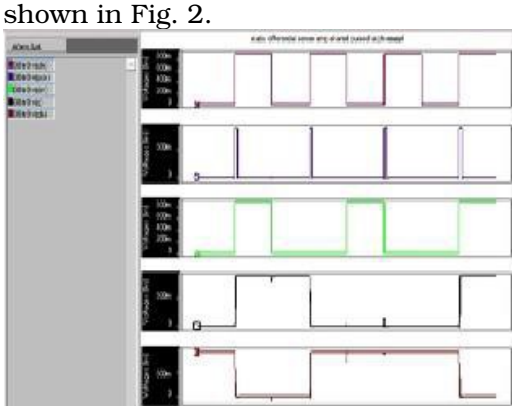


Fig. 5: SSASPL waveform.

Finally, the output of the shift register based pulse locking using CNTFET technology is as shown in FIG.

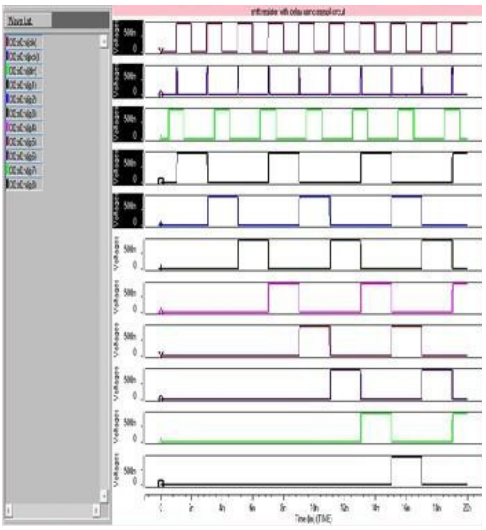


Fig. 6: Pulsed blocking waveform based on the shift register using a CNTFET.

Also compare the performance delay product of shift registers based on PPCFF and SSASPL.

C hart-1: comparison of delay, power and power delay product (PDP) of two shift registers.

6. CONCLUSION

In this article, the pulse-latch based shift register with low power sense amplifier using CNTFET technology has been proposed. From the discussion we can conclude that CNTFET is the best MOSFET replacement because of its power dissipation and delay.

REFERENCES

1. B.-S. Kong, S.-S. Kim, and Y.-H. Jun, "Conditional- capture flip-flop for statistical power reduction," IEEE J. Solid-State Circuits, vol. 36, pp. 1263–1271, Aug. 2001.
2. Cho, "A 10-bit column-driver IC with parasitic- insensitive iterative charge-sharing based capacitor-string interpolation for mobile active- matrix LCDs,"IEEE J. Solid-State Circuits, vol., no. 3, pp. 766–782, Mar. 2014.
3. Sanjeet kumar Sinha and Saruabh chadhury,"Comparative study of leakage power in CNTFET over MOSFET device," Journal of semiconductors, vol.35, No.11, November 2014.
4. J. Montanaro et al., "A 160-MHz, 32-b, 0.5-W CMOS RISC microprocessor," IEEE J. Solid-State Circuits, vol. 31, no. 11, pp. 1703–1714, Nov. 1996.
5. C. K. Teh, T. Fujita, H. Hara, and M. Hamada, "A 77% energy-saving 22-transistor single-phase-clocking D-flip-flop with adaptive-coupling configuration in 40 nm CMOS," in IEEE Int. Solid-State circuits Conf. (ISSCC) Dig. Tech. Papers, Feb. 2011, pp. 338–339.
6. U. KO and P. T. Balsara, "High Performance,Energy Efficient, Master-Slave Flip-flop Circuits," Proceedings of the 1995 IEEE Symposium on Low Power Electronics, pp. 16- 17, October 1995.
7. Stojanovicand V. Oklobdzija, "Comparative analysis of master slave latches and flip-flops for high-performance and low-power systems," IEEEJ. Solid- State Circuits, vol. 34, no. 4, pp. 536–548, Apr. 1999.
8. H. Partovi et al., "Flow-through latch and edge- triggered flip-flop hybrid elements," IEEE Int. Solid- State circuits Conf. (ISSCC) Dig. Tech. Papers, pp. 138–139, Feb. 1996.
9. Byung-Do Yang," Low Power and Area Efficient Shift Register Using Pulsed Latchs", IEEETransactionson circuits and systems I; regular paper, vol.62, no.6, June 2015.
10. E. Consoli, M. Alioto, G. Palumbo, and J. Rabaey, "Conditional push-pull pulsed latch with 726 fJops energy delay product in 65 nm CMOS," in IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Paper Feb. 2012, pp. 482–483.