

Volume : 4, Issue: 1
January - June 2014

ISSN : 2229 - 3515

International Journal of
**ADVANCES IN
SOFT COMPUTING
TECHNOLOGY**

Editor-in-Chief
Dr. Vaka Murali Mohan



Published by

BHAVANA RESEARCH CENTER

An Overview of Security Concerns In Cloud Computing

Zubear Ahammed, K^{1*}, Yadaiah, V² and Dr. C. S. Kumar³

1. Dept of CSE, TRR College of Engineering, Inole (V), Patancheru (M), Medak (Dt), A.P
2. Associate Professor, Dept of CSE, Vignan Institute of Technology & Sciences, Hyderabad, AP
3. Professor & Head, Dept of CSE, Vignan Institute of Technology & Sciences, Hyderabad, AP

KEYWORDS

Cloud Computing;

Multi Cloud;

Single Cloud;

Cloud service provider;

Security;

Abstract: Cloud is kind of centralized database where numerous clients accumulate their data, recover data and possibly adjust data and it is a representation where user is made available services by Cloud Service Provider on the basis of pay per use. The applications that are distributed as services over the internet and the servers in the centres of data providing the services refer to the cloud computing technology and are accessing resources essential to carry out functions by means of energetically changing requirements. The advantages of cloud computing include on-demand self-service, ubiquitous network admission, location autonomous resource pooling, fast resource elasticity, usage-based charge, transmission of risk. Due to service availability breakdown, dealing with single cloud providers is becoming less accepted with customers. In the recent times there has been a move towards multi-clouds and the likelihood for relocation to a multi cloud situation is inspected and the issues related to the protection in multi-clouds were reviewed in the related research. The most important purpose of moving to inter clouds is to get better what was obtainable in single clouds by means of allocating consistency, trust, and protection among multiple cloud providers.

1. INTRODUCTION

For the past few years, the technology that has the extreme growth sections in the field of infrastructure is cloud computing that permits the consumers to make usage of applications devoid of installation and by means of internet access the personal files. By means of concentrating memory, bandwidth and processing cloud computing permits for additional resourceful computing and to preserve the data the internet was used by the technology [4]. The advantages of cloud computing include on-demand self-service, ubiquitous network admission, location autonomous resource pooling, fast resource elasticity, usage-based charge, transmission of risk. The applications that are distributed as services over the

internet and the servers in the centres of data providing the services refer to the technology and are accessing resources essential to carry out functions by means of energetically changing requirements. Single cloud providers' usage is becoming less accepted by means of customers because of the service availability breakdown and the chances that there are malevolent insiders in the solitary cloud [8]. To decrease safety risks that affect the cloud computing user we support the relocation to multi-clouds due to its capability in the modern times. As the data is mutual by means of a third party, the users of the cloud computing keeps away from an untrusted cloud provider. The previous methods do not assurance that the server will reply a query without knowing the query type and the data accuracy stored in the server, even though they allow consumers to make sure the reliability of their information that has been returned through servers [1]. The essential issues concerning to the security risks of cloud computing is the data integrity maintaining where the data may possibly

*** Mr. ZUBEAR AHAMMED, K**

Department of Computer Science & Engg.
TRR College of Engineering
Patancheru, Medak (Dt), A.P, India
Ph. No: 91-8897391842
E- Mail: zubearnxt@gmail.com

suffer from damage during modification operations to the cloud storage provider. The concept of multi-clouds propose that cloud computing must not finish by means of a particular cloud. The purpose of moving to inter clouds is to get better what was obtainable in solitary clouds by allocating consistency, trust, and protection among multiple cloud providers. The protection of the data regarding the customers should be made sure by the cloud service providers and should be accountable if any security risk affects their customers' service infrastructure [11]. Due to the intolerable insiders in the cloud, customers do not want to lose their confidential information and more over the loss of service availability for many customers, has caused several problems recently. There has been a move towards multi-clouds and the likelihood for relocation from single to a multi-cloud atmosphere is inspected and the concerns related to the protection in multi-clouds were reviewed in the related research. Much research has been done to make sure about the safety of the single cloud, whereas regarding the issues related to security, multi clouds have received less attention.

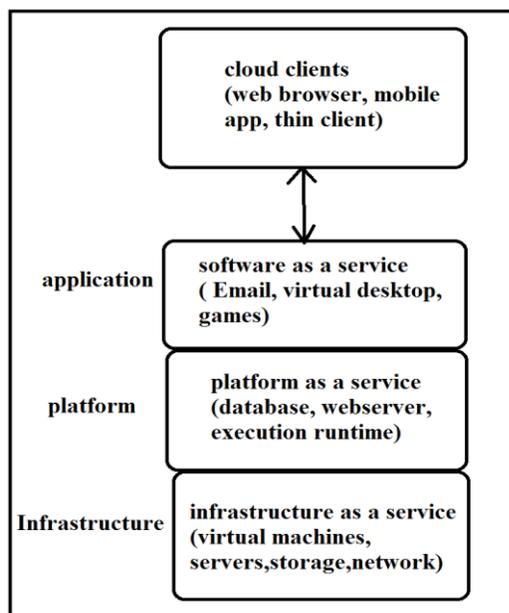


Fig1: An overview of cloud infrastructure

2. METHODOLOGY:

Cloud provider put forward numerous services that can possibly profit its customers, such as quick access to their data, scalability, pay-for-use, data storage, data recovery and defend against various hackers. From the

networking organization services, information storage and computing services, the operator can obtain benefit in infrastructure as a service and it is the circulation of computer organization as a provision. Software-as-a-Service: The online deliverance of competence and functionality of the software without requirement for running the software locally is observed in the system of software as a service [9]. It is the initial service and has the benefit of prevalent implementation shown in fig1. To access and influence the information wherever was allowed by the users and contain an association of data which is an imperative contemplation in humankind. Minimum ability to customize the function intended for particular needs of the business is the drawback. As practicable substitute for conventional software that inhabits on an individual computer is the solution of the SaaS acceptable by the huge enterprises. An extensive selection of complicated applications such as management of supply chain and other vertical functions were delivered by the SaaS providers of the level of enterprise [7]. Reducing of the outlay of the software licencing and outlay of the hardware, Dialed up or down of the stretchy IT resources are the advantages of the direct SaaS. By means of the service provider's resources, the user runs tradition requests in platform as a service Infrastructure-as-a-Service: The delivery scheme that makes available the infrastructure as a service is IaaS and to a great extent diminishes the requirement for enormous early investments in computing servers and devices of networking. IaaS is a solitary layer of tenant cloud computing where the vendors of the committed resources are allocated simply with the clients of the contract based at a payment of pay per use [2]. The significant usage of cloud computing necessitates the resources of the computing for data hosting and application running. The Cloud deployment representing the third layer in the environment of cloud computing comprises the clouds such as private, public, hybrid and community clouds [5]. A cloud atmosphere that is made obtainable intended for multi-tenants and is available to the community is called a public cloud; private cloud is accessible for a specific

group, whereas a community cloud is altered for an exact group of clients.

3. DATA STORAGE SECURITY IN THE CLOUD:

The concept of multi-clouds put forward that cloud computing ought not to finish by means of a solitary cloud. Moving from single clouds to multi-clouds is rational and significant for many reasons. To store data on numerous cloud servers, the usage of Byzantine fault-tolerant replication, as a result if one of the cloud providers is injured, they are still able to get back data accurately. To address the difficulty of the loss of privacy, Data encryption is measured the solution. The DepSky system accumulates the cryptographic keys in the cloud by means of the secret sharing algorithm, as the data will be accessed by dispersed functions to conceal the assessment of the keys from a malevolent insider. The most important purpose of moving to inter clouds is to get better what was presented in solitary clouds through allocating consistency, trust, and protection among multiple cloud providers [6]. To guard the stored information within the cloud, customers can make use of cryptographic methods in order to reduce the threat in cloud storage. Keeping a short hash in local memory by means of a hash function for data reliability is a good solution. By means of recalculating the hash of the received data, the verification of the server responses is done in this way, which is evaluated with the local stored data.

4. MINIMIZE LOSS OF CONTROL:

Cloud consumer needs situational awareness for critical applications, When underlying components fail, what is the effect of the failure to the mission logic What recovery measures can be taken (by provider and consumer), Requires an application-specific run-time monitoring and management tool for the consumer, The cloud consumer and cloud provider have different views of the system, Enable both the provider and tenants to monitor the components in the cloud that are under their control.

Provide mechanisms that enable the provider to act on attacks he can handle. infrastructure remapping (create new or move existing fault domains) shutting down offending components or targets (and assisting tenants with porting if necessary Repairs, Provide mechanisms that enable the consumer to act on attacks that he can handle (application-level monitoring). RAdAC (Risk-adaptable Access Control), VM porting with remote attestation of target physical host, Provide ability to move the user's application to another cloud.

The concept of 'Don't put all your eggs in one basket' Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture, Propose a multi-cloud or intra-cloud architecture in which consumers Spread the risk, Increase redundancy (per-task or per-application), Increase chance of mission completion for critical applications.

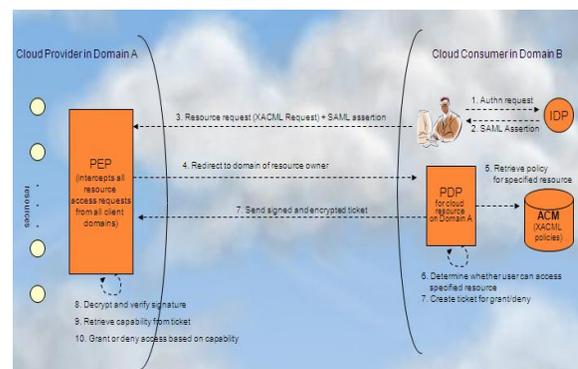


Fig. 2: Minimize Loss of Control: Access Control

Possible issues to consider: Policy incompatibility (combined, what is the overarching policy?). Data dependency between clouds, Differing data semantics across clouds, Knowing when to utilize the redundancy feature (monitoring technology) Is it worth it to spread your sensitive data across multiple clouds?, Redundancy could increase risk of exposure

5. CONCLUSION:

The most important purpose of moving to inter clouds is to get improved what was obtainable in solitary clouds by means of sharing out consistency, trust, and protection among multiple cloud providers. Much research has been done to make sure about the safety of the single

cloud, whereas regarding the issues related to security, multi clouds have received less attention. To decrease safety risks that affect the cloud computing user we support the relocation to multi-clouds due to its capability. By means of a multi-share technique replicating the data into multi-clouds may possibly decrease the threat of data intrusion and augment data integrity. To supply a protected cloud database that promises preventing security risks facing the cloud computing community, we aim to make framework available for future work and this structure will make use of multi-clouds and the algorithm of secret sharing to decrease the data intrusion risk and the failure of service accessibility and ensuring data reliability. To deal out the data into three different cloud providers in relation to data interference and data reliability, the undisclosed sharing algorithm was applied on the stored information.

6. REFERENCES:

- [1] H.MeI, J. Dawei, "Supporting Data base Applications as a Service", ICDE'09: Proc. 25th Intl.Conf. on Data Engg., 2009, pp. 832-843.
- [2] A. Juels and B.S. Kaliski Jr, "PORs: Proofs of retrievability for large files", CCS '07: Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 584-597.
- [3] R. Perez, R. Sailer "virtualizing the trusted platform module", Proc. 15th Conf. on USENIX Security Symposium, 2006, pp. 305-320.
- [4] M. Van Dijk., A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing", HotSec'10: Proc. 5thUSENIX Conf. on Hot topics in security, 2010, pp.1-8.
- [5] G.R. Goodson, J., G.Ganger M.K. Reiter, "Efficient Byzantine-tolerant erasure-coded storage", DSN'04: Proc. Intl. Conf. on Dependable Systems and Networks, 2004, pp.1-22.
- [6] P.A. Loscocco, S.D. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner and J.F. Farrell, "The inevitability of failure: The flawed assumption of security in modern computing environments", Citeseer, 1998, pp. 303-314.
- [7] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.
- [8] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky and D. Shaket, "Venus: Verification for untrusted cloud storage", CCSW'10: Proc. ACM workshop on Cloud computing security workshop, 2010, pp. 19-30
- [9] F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc. 1stIntl. Workshop of Dependability of Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.