International Journal of Scientific Research in Computer Science and Engineering
Vol.5, Issue.1, pp.45-48, Feb (2017)

Research Paper

E-ISSN: 2320-7639

A Security Key Management Model for Cloud Environment

Nitesh Jain[1*] and Pradeep Sharma[2]

[1] Dept. of Computer Science, Govt. (Model, Autonomous) Holkar Science College, Indore, INDIA
[2] Dept. of Computer Science, Govt. (Model, Autonomous) Holkar Science College, Indore, INDIA

Corresponding Author: jain2014.nj@gmail.com

Available online at: www.isroset.org

Received 22nd Jan 2017, Revised 05th Feb 2017, Accepted 15th Feb 2017, Online 28th Feb 2017

Abstract: - Security is the most important factor in cloud computing for ensuring client data is placed on secure mode in the cloud. For any organization, Data is very valuable assets but as number of users and quantity of data is increasing day by day, which cause the need of data security on cloud. For cloud computing there should be various security and privacy measures like identity management, physical personal security, availability, application processing authentication, atomic transaction etc. Security is mostly broken when any one doesn't follow certain security measure or not being attentive for threat and vulnerabilities. Dealing with "One Cloud" providers is predicted to become minor popular with customers due to risks of service availability failure and the possibility of malicious insiders in the one cloud. In this research paper we have also dealing with a security key management model for cloud environment or cloud of cloud.

Keywords: - Cloud Computing, Security Model, Data Security, Cloud Environment

I. INTRODUCTION

Cloud computing is the concept of suing remote service through network using resources. Cloud Computing is formed by two words cloud + Computing. If we separately see the words than here cloud is used as a metaphor for the internet, which is based on the drawing just as telephone network. Here all the resources are shared by the company, as to secure their cost. And computing means "to Count". So the cloud computing means to share the internet resources, servers, software's required by computer and other devices. That is the cloud computing is the new technology by which we utilize on-demand computing, storages, data and services anywhere from the world.

Cloud Computing is a term used to describe both a platform and different application. As a platform is supplies, configures and reconfigures servers, while the servers can be physical system or virtual system. In other word, Cloud Computing describes application that is extended to be accessible through the internet and for this purpose large data Centers and powerful servers are used to host the web applications and web services. [1,2,3,4,5,6,7,8,910]

Cloud computing is generally divided in to three segments are "Application", "Storage" and "Connectivity" and each segment is used to service as a different service for a different purpose to use in different business [2]. The concept of cloud computing is linked closely with those of service model [6,7,8,9,10,11,12]:

IaaS (Infrastructure as-a-services): It basically deals by providers to provide feature on demand utility.

PaaS(Platform as-a-services): It is used by developer for creating new application.

SaaS(Software as-a-services): It is provide application as a service on internet.

II. TYPE OF CLOUD

In Cloud computing is categorized in four categories.

Private Cloud: In private cloud data is managed properly within organization only without the limit of network bandwidth. It is some time called internal cloud eg. S3 (simple storage service), EC2 (Elastic Cloud Computing).

Public Cloud: This is only one of which cloud service is being available to user via a service provider over the internet it provides service on a pay-per-usage model eg. Google Apps Engine, Blue cloud by IBM.

Community Cloud: This type of cloud is basically managed by group of organization that have common objective eg. Security polices etc.

Hybrid Cloud: Hybrid cloud is a combination of private and public cloud means a vendor has a private cloud and forms a partnership with a public cloud provider.

III. NEED FOR CLOUD SECURITY

In [3], in their paper have depicted a complete survey on the issues related to cloud computing environment security. Cloud computing environment is both promising and scary. Despite of the attractive economic and technological advantages it has, businesses still think of the potential security threat before entrusting their data and information. Security is the most crucial aspect of everyday computing; this is very well applicable to cloud computing environment itself. There are many security concerns in cloud computing environment security; a few can be listed as follow:

Malicious Attacker
Hackers these days can breach the strongest security provisions and hijack confidential data. Malicious attacker can inject viruses or worms into the database system (Back End), and destroy or corrupt the data that is of important and valuable to the company.

Service Hijacking
Service hijacking is nothing but gaining unauthorized services. It includes various techniques like fraud, phishing and software exploitation. This is considered to be one of the top most threats.

SQL Injection Attack
A SQL code is inserted into the model code. By doing this the invader can gain access to a database and to other unauthorized information. SQL cross scripting is a well-known tool for hackers, wherein on use of special characters the hacker can modify rows and columns.

Confidentiality
Confidentiality is preventing the improper disclosure of information. Preserving confidentiality is one of the major issues faced by cloud systems, since the information is stored at a remote location that the Service Provider has full access to. Therefore, there has been some method of preserving the confidentiality of data stored in the cloud. The main method used to preserve data confidentiality is data encryption; however encryption brings about its own issues, some of which are discussed later.

IV. THE MULTI-CLOUDS STRATEGY

Multi-cloud strategy is the use of two or more cloud to minimize the risk of service availability failure, Loss and corruption of data, loss of privacy, vender lock-in and the possibility of malicious insiders in the single cloud. The service unavailability can occur due to breakdown of hardware, software or system infrastructure. A multi-cloud strategy can also improve overall enterprise performance by avoiding "vendor lock-in" and using different infrastructures to meet the needs of diverse partners and customers. The cost of using multiple clouds will be higher than that of single clouds. Thus unless and until there is a design which can make use of multi-clouds without increasing cost, the implementation will be highly impractical [4].

V. PROBLEM FORMULATION

Due to constantly increase in the popularity of cloud computing security of cloud become main top issue of cloud computing such kind of issue become more significant when user want to move critical application and sensitive data to public cloud and shared cloud environment generally security refer to confidentiality integrity and availability confidentiality refer who is owner of encryption key. Integrity refers that no common policy exists for approved data exchange the industry has various protocol use to push different jobs. The most problematic issue is data availability some time data is not available on demand of client in that case we can say that security becomes mandatory field in this area.

VI. METHODS

In cloud computing security can provide in two ways which are:

- Security is provided by service provider [1].
- Security is provided by the client [1].

That specifies in cloud computing we can implement security by using two ends either at client end or service provider end total depend on client latest requirement. In this research paper we have also dealing with a security key management model for cloud environment or cloud of cloud. The storage security and data security is must to store, manage, share, analyze and utilize the substantial amount of data residing on cloud should be secure.

VII. PROPOSED MODEL

A. EXISTING SYSTEM
Cloud providers should address privacy and security issues and a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

B. DISADVANTAGES OF EXISTING SYSTEM

- Cloud providers should address privacy and security issues and a matter of high and urgent priority.
- Service availability failure and the possibility that there are malicious insiders in the single cloud.

C. PROPOSED SYSTEM

- This project focuses on the issued related to the data security aspect of cloud computing
- Moving towards "Cloud of Cloud" or Cloud Environment technique which improves.
  - Better read performance
  - Reduces Data Corruptions
  - Reduces intrusion ……etc

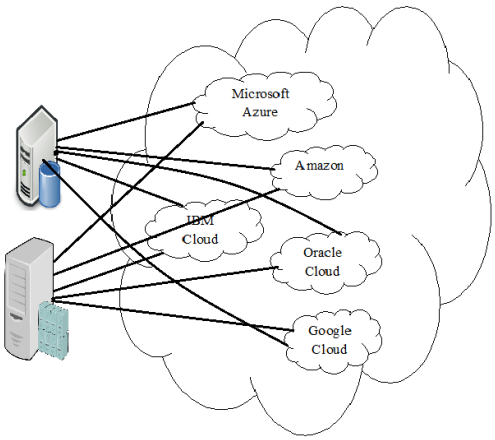

Fig 1

D. ADVANTAGES OF PROPOSED SYSTEM

- Data Integrity
- Service Availability
- The user runs custom applications using the service provider's resources.
- Cloud service providers should ensure the security of their customer's data and should be responsible if any security risk affects their customer's service.

E. DEPSKY SYSTEM

DepSky is one such architecture design that overcomes all the limitations of multi-clouds by eliminating the requirement of code execution in the servers (i.e., storage clouds). It is still efficient as it requires only two communication round-trips for each operation. Also, it deals with data confidentiality and reduces the amount of data stored in each cloud. It uses an efficient set of Byzantine quorum system protocols, cryptography, secret sharing, erasure codes and the diversity that comes from using several clouds. Several areas of cloud computing that will benefit from DepSky are discussed in [5].

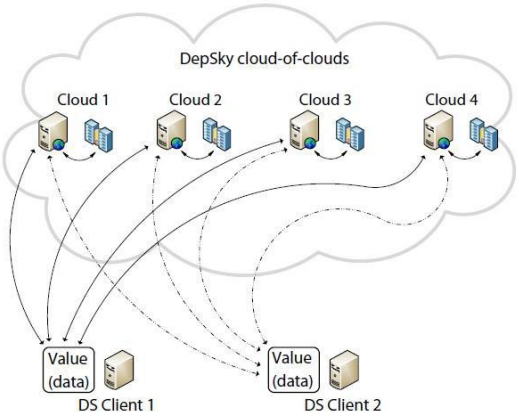

Fig 2. DepSky Architecture

The DepSky System model contains three parts: readers, writer, and four cloud storage provider, where readers and writers are the client's tasks. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas writers only fail by crashing.

VIII. IMPLEMENTATION

- Data integrity
- Data Intrusion
- Service Availability

Data Integrity

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider.

Data Intrusion

- Another Security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion.
- If someone gains access to an Amazon account password they will be able to access all of the account's instances and resources.
- Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its service. Furthermore, there is a possibility for the user's email to be hacked, and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

Service Availability

- Another major concern in cloud services is service availability.
- Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time.
- The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.

IX. CONCLUSION

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

X. FUTURE WORK

For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk ofdata intrusion and the loss of service availability in the cloud and ensure data integrity. In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder.

XI. ACKNOWLEDGMENT

I would like to thank all the people who showered their kind support needed for the entire research. I am gratified towards our project guide Dr. Pradeep Sharma, our project Coordinator Mr. Shivlal Mewada and the entire faculty of our institution; they have always been encouraging and inspirational. Lastly my family and friends how are always there through thick and thin.

REFERENCES

[1]. S.L. Mewada, U.K. Singh, P. Sharma, "Security Enhancement in Cloud Computing (CC)", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.31-37, 2013.

[2]. R. Piplode, P. Sharma and U.K. Singh, "*Study of Threats, Risk and Challenges in Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.26-30, 2013.

[3]. S. Ayyub, D. Roy, "*Cloud Computing Characteristics and Security Issues*", International Journal of Computer Sciences and Engineering, Vol.1, Issue.4, pp.18-22, 2013.

[4]. G.Malini and A.Immaculate Mercy , "*Evaluating Synchronized Determination Assembly in Multi-Cloud Atmosphere*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.9, pp.277-281, 2015.

[5]. S.Sujitha and S. J. Mohana, "*Secure Data Storage and Retrieval Using Adaptive Integrity Protocol Model in Cloud Environment*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.9, pp.181-184, 2015.

[6]. Md Kausar Alam, Sharmila Banu K, "*An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds*", *International Journal of Scientific and Research Publications*, vol. 3, issue 4, pp.23-28, 2013.

[7]. A. Juels, 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.

[8]. C. Cachin, I. Keidar, A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[9]. H. Abu-Libdeh, L. Princehouse, H. Weatherspoon, "RACS: a case for cloud storage diversity", *SoCC'10: Proc. 1st*

[10]. Rakesh Prasad Sarang and Rajesh Kumar Bunkar, "*Study of Services and Privacy Usage in Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.6, pp.7-12, 2013.

[11] R. Sood, R. Sharma, "*Cloud Security Threats and Issues-A Review*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.4, pp.115-119, 2017.

[12]. 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, China, pp.129-134, 2011.

