CLOUD COMPUTING SECURITY FROM SINGLE CLOUD TO MULTI-CLOUDS

Arockia Panimalar.S[1], Priyadharshini.P[2], Abirami.P[3], Iniya.R[4]

[1] *Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*
[2,3,4] *III BCA 'A', Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*

---***---

Abstract - *Cloud computing provides many benefits in terms of low cost and accessibility of data. The use of cloud computing has increased rapidly in many organizations Security. One of the most important aspects refers to the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. A movement towards "multi-clouds", or in other words, "inter-clouds" or "cloud-of-clouds" has emerged recently. For example, the data stored in the cloud needs to be confidential, preserving integrity and available. The available multi-cloud proposals are unhandy or insecure. A solution can be seen in the recent research related to single and multi-cloud security. The level of customization can be can be achieved by providing and deciding security.*

Key Words: ***Cloud Computing, Single Cloud, Multi-Clouds, Cloud Storage, Data Storage.***

1. INTRODUCTION

The technology users can consume services at any time by their particular needs. The cloud computing, users has to buy individual or costly software, hardware resources become easy to get access to the services on demand over the network. The technology users can consume services at any time by their particular needs. It has to come up with a way to secure those files. Data stored in the cloud can be compromised or lost. It can encrypt them before storing in the cloud, in sorts out the disclosure aspects. It has store more than one cloud service and encrypt it before in send it off. A lot of research has been carried out for the same, and to a large extend has helped to strengthen cloud computing security. Each of them will have the same file Also, cloud computing offers highly efficient data retrieval and availability. The migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data. Cloud providers are taking the responsibility of resource optimization [1].

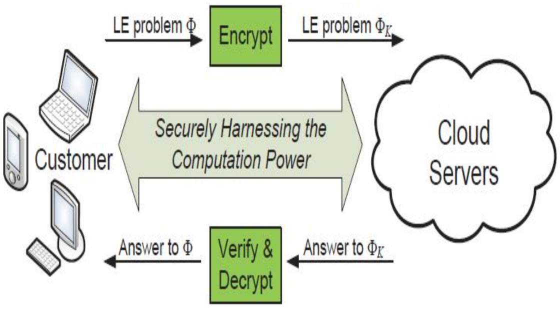


Figure1: System Architecture

2. DATA INTEGRITY

Computation integrity means that program execution should be as expected and be kept from malware, an insider, or a malicious user that could change the program execution and render an incorrect result. Data that is stored in the cloud could suffer from the damage on transmitting to/from cloud data storage. Data integrity could help in getting lost data or notifying if there is data manipulation. Integrity should be checked at the data level and computation level. Data integrity Means data should be kept from unauthorized modification. The data integrity should be maintained and checked constantly in order to prove that data and computation are intact. Any modification to the data should be detected.

The following examples explain how data integrity could be violated.

2.1 Data Loss or Manipulation

Users have a huge number of user files. Therefore, cloud providers provide Storage as Service. Those files can be accessed every day or sometimes rarely. Therefore, there is a strong need to keep them correct. The cloud is untrustworthy; the data might be lost or modified by unauthorized users. In many cases, data could be altered intentional or accidentally. Also, there are many administrative errors that could cause losing data such as getting or restoring incorrect backups. The attacker could utilize the user's outsourced data since they have lost the control over it.

2.2 Untrusted Remote Server Performing Computation on Behave of User

Cloud computing is not just about storage. The cloud provider is not security boundary or transparent to the owner of the tasks no one will prove whether the computation integrity is intact. Also, there are some intensive computations that need cloud processing power in order to perform their tasks. Therefore users outsource their computations [2].

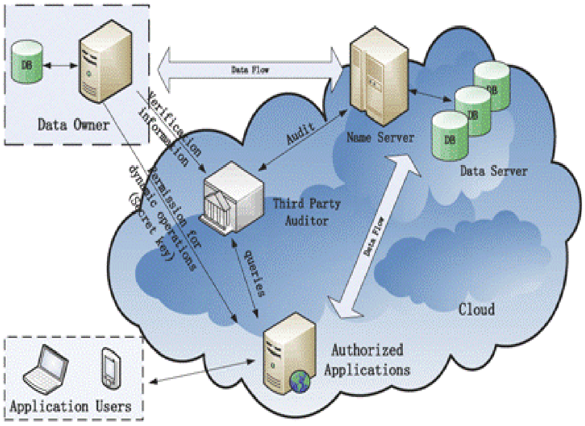


Figure 2: Audit System Architecture for Cloud Computing

3. DATA INTRUSION

The importance of data intrusion detection systems in a cloud computing environment. 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 services. The find out how intrusion detection is performed on Software as a Service and Platform as a Service and Infrastructure as Service offerings, along with the available host, network and hypervisor based intrusion detection options. Detecting and responding to those attacks the norm and considered when it comes to security .An Amazon account password, they will be able to get access to all the account's instances and resources [3].

Figure 3: Data Intrusion

4. SERVICE AVAILABILITY

Service availability is most significant in the cloud computing security. Amazon previously mentions in its authorizing agreement that it is possible that the service might be unavailable from time to time. The user's web service may conclude for any reason at any time any user's files break the cloud storage policy. Companies seeking to protect services from such failure such as backups or use of multiple clouds [4].

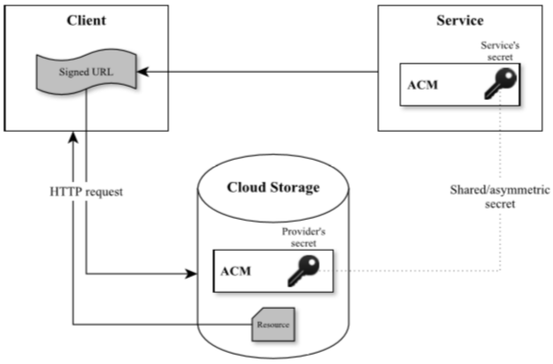


Figure 4: The service implements its own ACM which manages permission of end users.

5. DATA CONFIDENTIALITY ISSUES

Usually the data is encrypted before it is outsourced. The service provider gets encrypted data. Therefore, it is considered not useful or meaningless. However, the client is responsible for handling the access control policy, encrypting the data, decrypting it and managing the cryptographic keys. Even this would cause a burden to the user; sharing it with others exposes it to risks. When the data is shared among many users, there has to be more flexibility in the encryption process to handle users of the group, manage the keys between users, and enforce the access control policy in order to protect the data confidentiality. Sharing the data among a group of users adds more burden on the owner of the outsourced data. In the authors describe a cryptosystem in which the data owner encrypts the data by using his public Key aggregate cryptosystem for sharing data identifiers called a class on the encryption process. Also, the owner has a master key to create others secret keys for one, some classes of data, or all classes of ciphertext. It is an aggregate key where each part of it can decrypt part of the ciphertext. The whole key can decrypt the whole ciphertext. Therefore, this cryptosystem helps in sharing data among a group of users with fine grain access control and without giving them a key that can decrypt all that data. This figure shows the general view of this system [5].

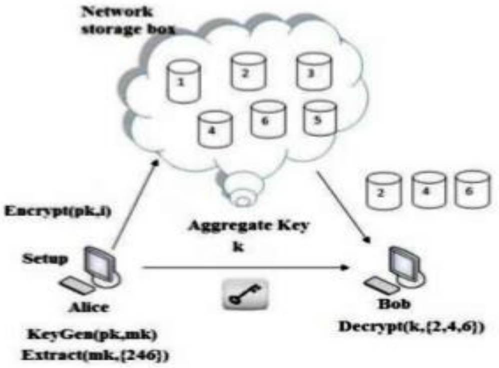


Figure 5: Data Issues

6. THE MULTI-CLOUDS STRATEGY

The service unavailability can occur due to breakdown of hardware, software or system infrastructure. The unless and until there is a design which can make use of multi-clouds without increasing cost, the implementation will be highly impractical 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 cost of using multiple clouds will be higher than that of single clouds [6].

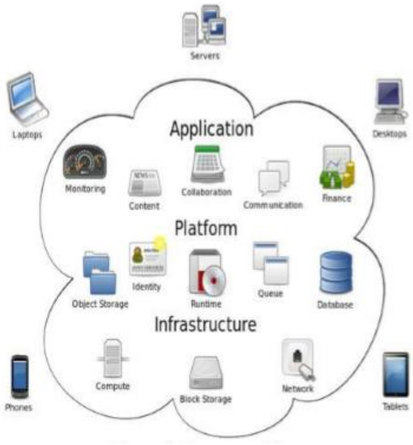


Figure 6: Multi-Cloud Strategy

7. TYPES OF CLOUD COMPUTING

The cloud computing is classified as

7.1 Public Cloud

In public cloud the computing infrastructure is hosted by the cloud vendor at the vendor's premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared among various any organizations.

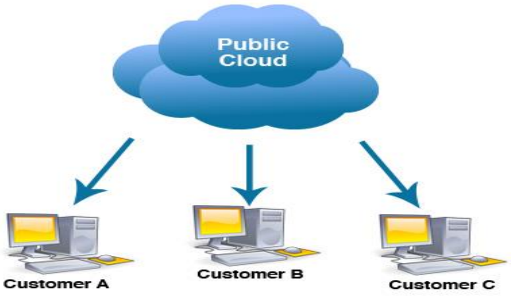


Figure 7: Public Cloud

7.2 Private Cloud

Some experts consider that private clouds are not real examples of cloud computing. The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Private clouds are more expensive and more secure when compared it to public clouds. Private clouds are of two types: On-premise private clouds and externally hosted private clouds.

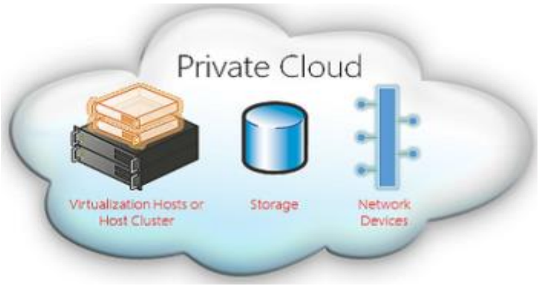


Figure 8: Private Cloud

7.3 Hybrid Cloud

The usage of both private and public clouds together is called hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization use their own computing infrastructure for normal usage, Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The access the cloud for high/peak load requirements.

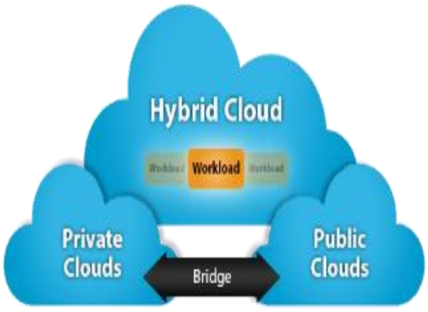


Figure 9: Hybrid Cloud

7.4 Community Cloud

A community cloud in computing is an effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally [4].

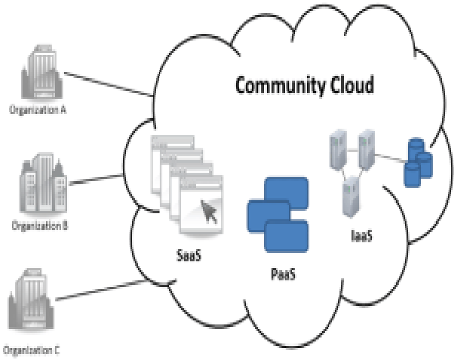
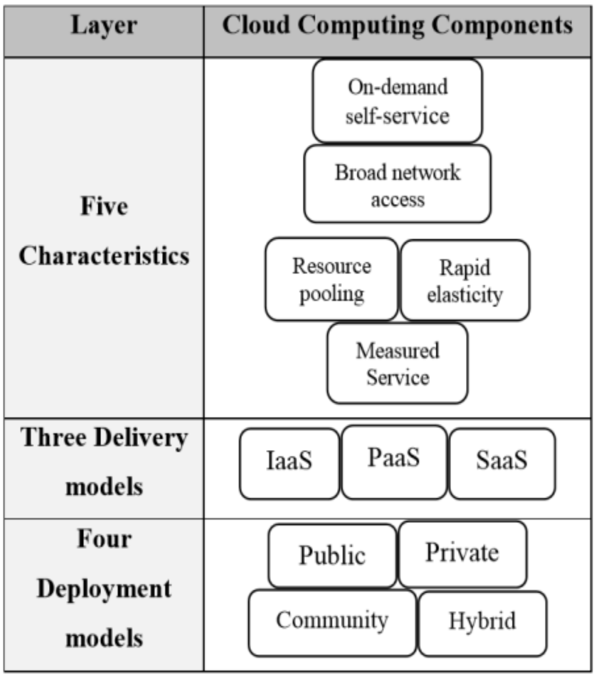


Figure 10: Community Cloud

8. LAYER MODELS OF CLOUD



Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

Figure 11: Layer Models of Cloud

9. DEPSKY ARCHITECTURE

The DepSky system model contains three types readers, writers, and four cloud storage providers, where readers and writers are the clients tasks Bessani et al. explain readers can fail arbitrarily for example, they can fail by crashing, they can fail from time to time and then display any behaviour it writers only fail by crashing.

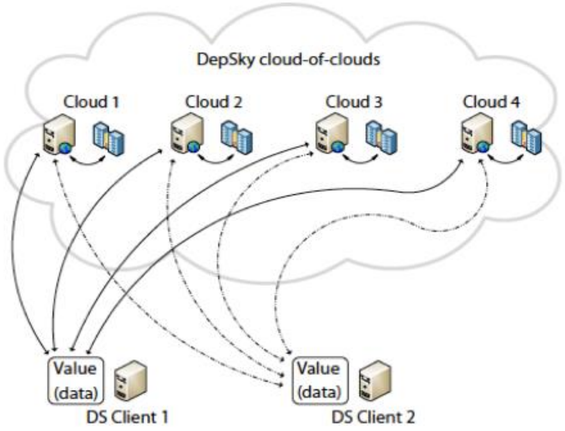


Figure 12: DepSky Architecture

10. IMPLEMENTATION

The context is a service-oriented client-server architecture with special focus on data confidentiality, availability, and service transparency and their types.

Figure 13: Cloud Processing

10.1 Secured Cost Effective Multi-Cloud Storage

The physical possession of their data and it's have an easy of implementing better data security policies. It cryptographic schemes applied distributed data storage, for enabling the data privacy. It has been proposed for hiding the data from the storage provider and hence preserving data privacy. The authors proposed a scheme in which, the user's identity is also detached from the data, and claim to provide public auditing of data. It concentrates on one single cloud service provider, which can easily become a bottleneck for such services. The authors studied and proved that sole cryptographic measures are insufficient for ensuring data privacy in cloud computing. The data is stored on an autonomous business party, that provides data storage as a subscription service the user might not be availing the storage services from that service provider, it will have no clue of such a passive attack. The users have to trust the cloud service provider (SP) with security of their data. The better the cryptographic scheme, the more complex will be its implementation and hence the service provider will ask for higher cost. This could also lead to a monopoly over cloud services in the market. Therefore, the conventional single service provider based cryptographic techniques does not seem too much promising. It aims to remove the centralized distribution of cloud data.

Figure 14: Secured Cost Effective Multi-Cloud Storage

10.2 Requirements

The requirements emerge from operations which client applications need to carry out. In cloud storage systems, these are typically file upload, download, update, and deletion. Today's de facto standard for basic file operations on cloud storage is a Rest-full API based on the HTTP protocol.

10.3 Permission Transfer in Clouds

On the cloud end of an access broker, APIs for permission transfer are required. In Section III we discovered the following technologies to pass permissions on cloud resources to other parties: Public access is always possible but contradicts with the principle of data confidentiality. Hence, it is not an option in most scenarios.

Figure 15: Transfer in Cloud

10.4 Signed URLs

Signed URLs, a form of query string authentication, is an access control feature used by most cloud storage services though with differences in name and implementation [4].

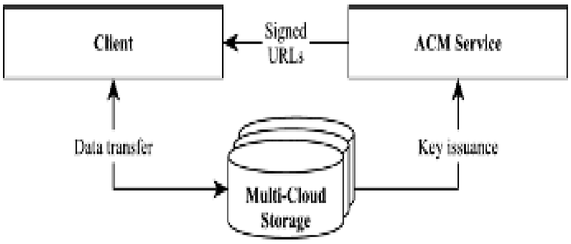


Figure 16: Cloud Transfer

11. CONCLUSION

It is clear that the use of cloud computing is increased rapidly; cloud computing security is still considered the major issue in the cloud computing environment. User does not want to lose their private information as a result of malicious insiders in the cloud. Protection is reduced. If one cloud provider fails, we can still access our data live in other cloud providers. The migration to multi-clouds because of its capacity to diminish security risk that influence the cloud computing user. The information is shared by the third party and Server users need to keep away from the untrusted cloud provider [5].

12. FUTURE WORK

The framework and give to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. Each Signed URL expires after a specific, predefined timeout. Hereby, each URL should only be valid for one request. If it fails, the client has to contact the ACM component again to retry. An important aspect of cloud storage is availability. Regarding service availability risk or loss of data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud provider fails, we can still access our data live in other cloud providers [6].

13. REFERENCES

[1] G. Sidharth1, D. Baswaraj2 1 MTech (CSE), CMR Institute of Technology, Hyderabad, India Head of the Department (CSE), CMR Institute of Technology, Hyderabad, India

[2] Shaik.Aafreen Naaz1, Pothireddygari. Ramya2, P. Vishunu Vardhan Reddy3 Department of IT, G. Pullaiah College Of Engineering and Technology

[3]Monjur Ahmed1 and Mohammad Ashraf Hossain, Daffodil Institute of IT, Dhaka, Bangladesh. Dhaka, Bangladesh.

International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[4] Rabi Prasad Padhy1 Senior Software Engineer Associate Professor HOD Bangalore, India IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011

[5] Latifur Khan, The University of Texas at Dallas, USA Bhavani Thuraisingham, The University of Texas at Dallas, USA International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 39

[6] Priyanka Pareek, Latifur Khan, The University of Texas at Dallas, US Bhavani Thuraisingham, The University of Texas at Dallas.