Cloud Security Issues - A Survey

V.Nirmala
Full Time Research Scholar
Dept of CSE, Government College of Technology
Coimbatore

R. Shanmuga Lakshmi, Ph.D.
Associate Professor
Dept of CSE, Government College of Technology
Coimbatore

ABSTRACT
Cloud computing is the one which offers infrastructure to the client on a pay as you use model by leveraging on the Internet technology. As this model depicts the electricity billing it is often termed as utility computing. It offers various services to the client based on the need. The need of the resources can be scaled up or down on the basis of the requirement. The IT sectors started using cloud service models. As the use of cloud increases day by day the concerns of cloud also gets increased. There are number of data breaches that are happening day by day that affect the cloud growth. The major concern in adapting cloud is its security. The companies have lot of data that gets increased each day enlarges the complication of data privacy and security. The data that we talk can be classified as either stagnant data i.e., for simple storage as offered by Amazon's Simple Storage Service (S3) or it can be vibrant that changes often. The solution available to protect the stagnant data will be to simply encrypt the data before it gets stored in the server. In order to solve the issues of vibrant data the techniques are being proposed to work out on the encrypted. This paper is a survey of different security issues that affects the cloud environment and related work that are carried out in the area of integrity.

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords
Cloud computing, cloud security, Integrity .

1. INTRODUCTION
Cloud computing is a term for anything that involves delivering services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was stimulated by the cloud symbol that's used to represent the Internet in network diagrams. Cloud as a whole is not a new technology that has emerged, but it has used all other boomed technologies in recent years to provide the best of all services.

Cloud came into reality using a method called Virtualization. Virtualization is nothing but an abstract of the resources that are available .The Infrastructure-as-a-Service (IaaS) provider like Amazon Web Services provides virtual server instances with unique IP addresses and provides blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed, it's also referred to as utility computing. Infrastructure as services that is physical assets as services is being provided by vendors like IBM Blue house, VMWare, Amazon EC2, Microsoft Azure Platform and more.

Currently the secured data storage mechanism in cloud is still in evaluation stage and it is not very popular across companies and individual users. Primary reasons of low usage are data security and internet availability. Some of the security issues are very critical and are to be handled in an efficient way.

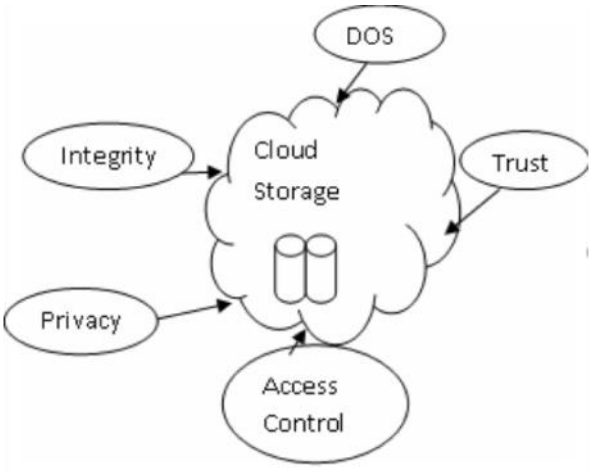

Fig 1: Security issues in cloud

The Fig 1 shows the various security issues of Cloud. The major security concerns are Privacy, data integrity and confidentiality. The solutions that are available in network security cannot be used as such for cloud. So, there is a need for new approaches to work on the security features to enhance cloud storage.

The data's that we place in cloud can classified in to either stagnant or vibrant. The stagnant data's are the one which will never change during the entire storage. Amazon's simple storage service (Amazon S3) offers such type of service. The security solution for stagnant data is to simply encrypt the data and store safely in the cloud. Whenever there is a need of data bring the data to the client site, decrypt and use the data. The vibrant data's are the one which changes

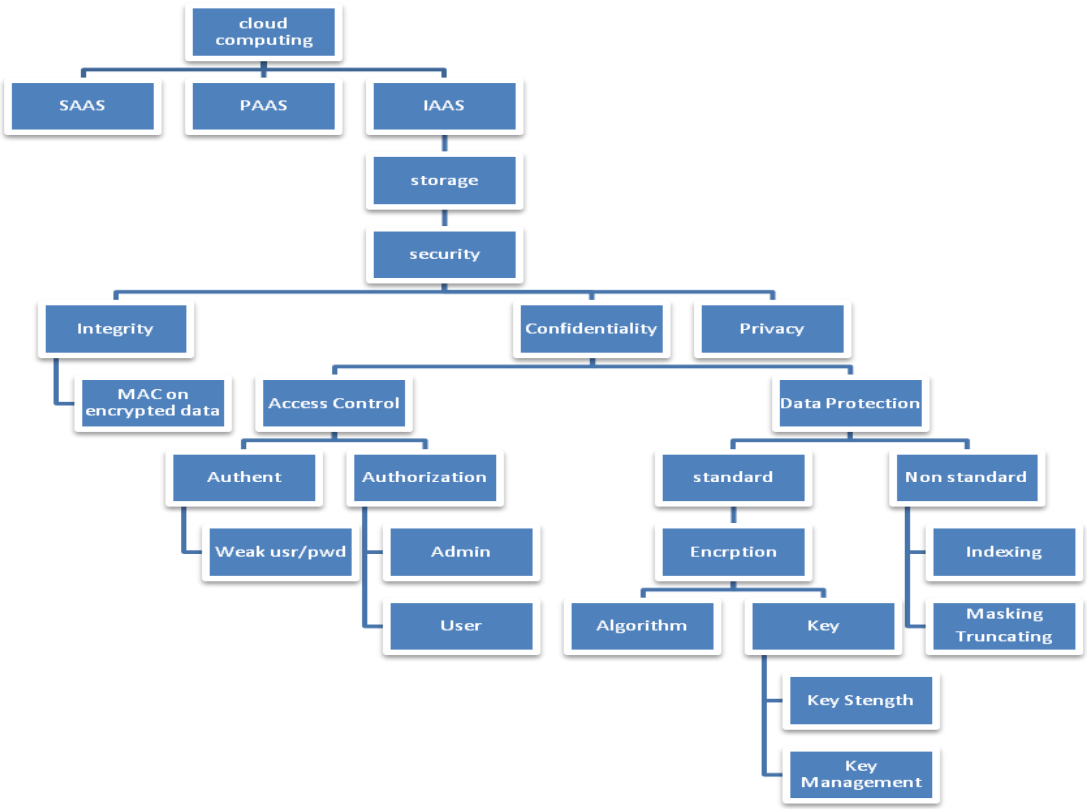

Fig 2: Cloud Security Framework

often are to be handled in specific manner. As in the case of stagnant data we cannot work on the vibrant data. So there is a need special treatment for those types of data. The security given for the storage is not up to the standard to suit the cloud. The major security issues are grouped under three different classes such as Integrity, Access Control and Privacy. The Fig 2 list down the various security issues that may affect the IAAS Service.

2. RELATED WORK

Integrity is the measure of checking the data soundness. The data's are classified as either stagnant or vibrant. In the case of static data, the encrypted data can be placed in the cloud. Once there is a need of data it can be brought as such to the client site and can be decrypted. So there will be less security break through. There are number of research works going on in the case of vibrant data where the data's get often updated and added. The following works have been attempted already in order to work on encrypted data. Although, the solutions provided have some margins.

PROVABLE DATA POSSESSION (PDP)[1]

This model uses the RSA based Homomorphic verifiable tag technique to ensure the data in the cloud. It introduces the public auditability scheme to check the integrity if data by trusted third party. It works well for the static data.

PROOF OF RETREIVABILITY (POR):[2]

The "proof of retrievability" (PoR) model uses error-correcting codes to ensure the correctness of data in the server. It introduces the sentinels in the middle of the block to check the integrity. It supports vibrant data but the number of check is limited.

PUBLIC AUDITABILITY AND DATA DYNAMICS [4]

It considers vibrant data storage and helps to find the errors and data check in a distributed manner. It supports only less number of data operations.

PUBLIC VERIFIABILITY AND DATA DYNAMICS [3]

This is based on Merkle Hash Tree construction for block tag authentication on Proof of retrievability model. It is seamlessly connects both dynamic data update and efficient verification technique to verify the data at the server.

POR SCHEME WITH FULL PROOF SECURITY [4]

The security model uses publicly verifiable homomorphic authenticators technique. It is constructed from BLS signatures.

DYNAMIC PDP MODEL: [5]

It is an extension of the PDP model constructed using provable data possession. It computes the tag and authenticates tag before verifying using rank based authentication.

SPACE-EFFICIENT BLOCK STORAGE INTEGRITY[1]

It uses tweakable enciphering technique and second preimage resistant hash function mechanism to provide the integrity of data at the server.

Table 1. Comparison of different integrity check techniques

Data Integrity Models	Technique used	Type of data	Dynamic Operations	Supports Public Auditability
PDP [1]	Homomorphic Verifiable tag	stagnant data	Not allowed	NO
POR[2]	Sentinels	stagnant data	Not allowed	NO
Public Auditability[4]	Merkle Hash trees and Bilinear aggregation function	Vibrant data	Allowed	YES
Public Verifiability[3]	Merkle Hash Tree	Vibrant data	Allowed	YES
POR scheme with full proof mechanism[3]	Homomorphic authentication technique with BLS signature	Vibrant data	Allowed	YES
Dynamic PDP model[5]	Rank based authentication	Vibrant data	Allowed but partially	YES
Space efficient block storage integrity[1]	Hash function	Vibrant data	Allowed	YES

3. CLOUD SECURITY ISSUES

3.1 Security Issues

These security issues are because of the vibrant nature of the cloud. They are

- **Elasticity** – Different users uses same machine to run their application using virtualization technique. This may lead to data breach.
- **Network insecurity** – The amount of traffic and uncontrolled nature of network may lead to data loss or replay of data.
- **Location** – As the Cloud clients are not sure of the location of their data raises the insecurity of the data.
- **Load burst** – As the nature of the cloud changes similarly the load of the cloud also changes accordingly.
- **Virtualization** – The cloud computing runs on the technique of virtualization where same system is allocated for multiple users at the same time there are possibilities that lead to unsafe of data.
- **IP address** – The use of same IP addresses to different users at times may lead to access of different resources of other users.

3.2 Research Issues

The cloud practical approach is very complex and changing. The vast traffic and load in the server increases the cloud architecture and its use. The virtualization techniques help in great deal to reduce the need of more physical resources which reduces the complexity. The primary issues that makes the cloud to readily acceptable is its security feature and chance of migrating from one cloud to another. The various works that have to be contributed to the cloud society to meet out the security needs are as follows.

1) **Service Provider Security**: The data has to be protected before getting stored in the cloud which may lead to data unsafe in the server side.
2) **Dangerous Neighbor**: The virtualization technique allows more than a user to work on a single machine which may lead to the requirement of protected data.
3) **Access Control**: There is a need of proper access control mechanism provided by the cloud service provider for the safe of client's data.
4) **Identity Management**: There should be way to properly identify the valid user simply not depending on the weak username password technique.
5) **Honest Cloud Service Provider**: Some untrue client may act as if they have sent the data actually without sending the data. So, Proper mechanism is a must to handle those clients.
6) **Log based Systems**: In order for billing proper log should be maintained by the service provider.
7) **Disaster Recovery**: There should be solutions to handle natural disaster so as to protect the data.
8) **Fraud Control**: While sharing of data to the shares there may be false sharer while pretending to be original.

The above are the major research areas which are to be concentrated to provide safe and sound cloud to the society.

4. CONCLUSION

Cloud computing uses various techniques to optimize and secure performance in an efficient manner. The cloud depends on network, virtualization environment and hypervisors which sit on operating system to control the virtual plays. The growth of cloud depends on both safe and cost effective nature to make the organizations and individuals to adopt the cloud.

In this paper mainly we discussed about the cloud security issues and the research issues in the security level. A secure cloud is impossible without satisfying all those research issues starting from protecting data from cloud service provider till virtualization environment because of the complex and changing nature of the cloud computing. So a new security solution should be provided to secure the data from different types of attack posed by different people at different places.

Our research is focusing on providing solutions to all these issues and develops a model to give secure cloud infrastructure that helps to adopt the cloud as and when required.

5. ACKNOWLEDGMENTS

Authors wish to extend their thanks to the Government College of Technology, Coimbatore for providing needed infrastructure to carry out the work.

6. REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, Kissner, Z. Peterson,and D. Song, "Provable data possession at untrusted stores,"in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609.

[2] A. Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in Proc. of CCS'07. New York, NY, USA: ACM, 2007,pp. 584–597

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09. Saint Malo, France: Springer-Verlag, 2009, pp. 355–370

[4] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public Auditability and data dynamics for storage security in cloud computing," in Proc. Of ESORICS'09.

[5] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS'09. Chicago, IL, USA:ACM, 2009.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, Charleston, South Carolina, USA, 2009.

[7] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP:Multiple-Replica Provable Data Possession," in ICDCS '08: Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems,(Washington, DC, USA), pp. 411–420, IEEE Computer Society, 2008.

[8] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT '08: Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, (Berlin, Heidelberg), pp. 90–107, Springer-Verlag, 2008.

[9] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS XI.,Usenix, 2007.