ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Security Modelling in Cloud.

Thanusha[1], Ashwini Kolhe[2], and Venkatesan M[3].

[1]School Of Computer Science and Engineering, VIT University, Vellore - Tamil Nadu-632014.
[2]School Of Computer Science and Engineering, VIT University, Vellore - Tamil Nadu-632014.
[3]Associate Professor, School Of Computer Science and Engineering, VIT University, Vellore - Tamil Nadu-632014.

ABSTRACT

Cloud computing has formed the conceptual an infrastructural basis for tomorrows computing. It is well-known that cloud computing has many enterprise applications potential advantages and data are emigrating to public or hybrid cloud. Cloud Computing has been e visualized as the next-generation architecture of IT Enterprise. Users can use cloud storage to store the data and get the data on-demand quality applications and services provide by different computing resources. TPA is a third party auditor used for checking the data integrity. Its doesn't bother to the storage of data and maintaining the data. To certainly introduce an effective TPA , the auditing processes under process should not bring new to system. The integrity of data is checked by the doing the public auditing. For this the third party auditor (TPA) is used. This process relives all burden from the cloud user. In this paper, the secure cloud system is built which supports security of the user data. This can be happen by integrating the Homomorphic linear authenticator and MAC-protocol. After this we performs audits for the many number of users simultaneously and more accurately, this will give the highly accurate and secured cloud model.

Keywords: TPA, security, cloud, data integrity, HLA, MAC-protocol.

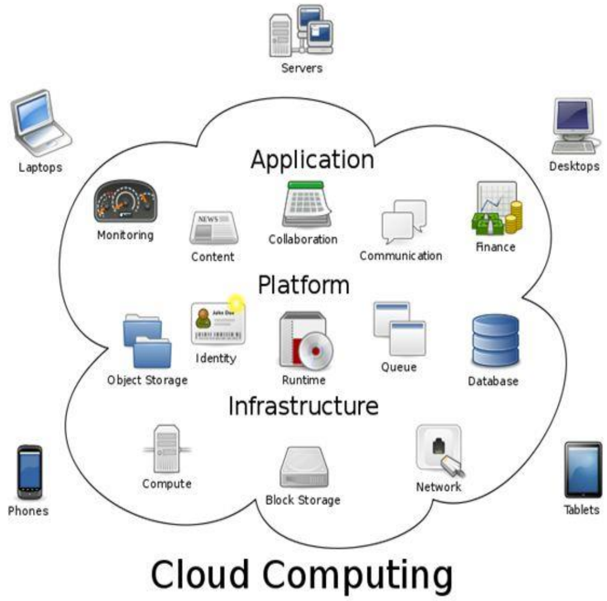
Corresponding author

INTRODUCTION

Cloud computing is architecture offers a computing service on demand and by minimal per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically having them. Cloud computing is an emerging computing technology that uses the internet and central remote servers to maintain data and application. Cloud computing is internet based technology that enables small business and organizations to use highly sophisticated computer applications.

Different models of cloud computing:

Cloud services is divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Software as a Service, describes any cloud service where consumers are able to access software applications over the internet. The applications are hosted in "the cloud" and can be used for a wide range of tasks for both individuals and organizations. Twitter, Google, Facebook and Flickr are all examples of SaaS, with users able to access the services via any internet enabled device. PaaS, is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser. Nowadays, information is one of the most valuable possessions of companies, organizations and individuals. From the beginning of time, people try to secure information saved on various kinds of storages. Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers. As a recent phenomenon, Cloud computing is perceived as a virtual cloud with unlimited possibilities of providing service in a field of information technology. The Organization of National Institute of Standards and Technology (NIST) defines cloud computing as a service model which enables instant, simple and on request available network access to shared offer of configurable computing resources (networks, servers, applications, service and data).



In case of need, they can be provided or loosened for minimal administrative expenses and it also provides coordination needs of the service providers. The deployment models include public, private, hybrid, and community clouds, and Virtual Private Clouds (VPCs), while the service delivery models. Although, the new benefits bring potential and privacy problems as well. User acceptance of cloud-based services can be significantly hindered due to security and privacy issues resulting from the illegal and unethical use of information. Recent surveys support the observation that customers are prevented by security and privacy concerns from adopting cloud computing services and platforms.

This project solves the security issues in cloud which mainly includes use of cloud request processors and database servers and also includes security of the data. The main objectives of the study are listed below:

- To provide security in cloud database servers.
- To provide data integrity
- Provide data Hosting services i.e. upload and download.

The main issues of the cloud based system is as follows :

- Data redundancy
- Computational overhead
- No perfect integrity verification process
- Takes more time to recover the file
- No security

LITERATURE SURVEY

[1] “HLA Based Third Party Auditing For Secure Cloud Storage” in this paper, it is explained that how the security is provided by the by using HLA algorithm. All the work is based on TPA audition of the data. They have got successful results for securing the user data and further its is extended for robust system. which will cope up with the large amount of data and thus encourages the users to use more cloud based services.

[2]”A Novel Data Security Model for Cloud Computing” in this paper, they have shown the security is biggest issue the cloud has facing to remedy to it the architecture they have proposed. Three layers of cloud security model to provide security has explained.

[3] “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” iintgis paper this paper studies the data integrity problem and ensures the data integrity. It included TPA to reduce the burden on the cloud user. It reduces the more involvement of end user. On the behalf of the end user this TPA will work. To support the data handling, data is decided into the blocks and further this block is proceed.

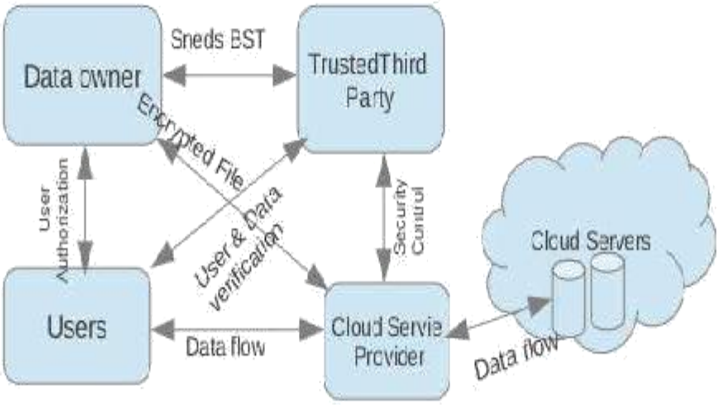
[4] “Security and Privacy in Cloud Computing” in this paper they have identified some security attribute listed as privacy-preservability, accountability, availability, integrity, accountability, confidentiality. They have explained each attribute in detailed. The security and privacy issues are discussed in detail.

[5] “Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation” in this paper they have proposed that a novel public auditing scheme for the integrity of shared data with efficient and collusion-resistant user revocation utilizing the concept of Shamir secret sharing. Besides, our scheme also supports secure and efficient public auditing due to our improved polynomial-based authentication tags.

PROBLEM STATEMENT

The system and thread model:

There are three different parts of architecture of the cloud based system as shown .The cloud user, who is willing to store the large amount of data on the cloud; Cloud service provider manages. The cloud server to ensure data storage service in reliable way. The third party auditor (TPA), is allowed to take a charge of cloud storage on the behalf of user. End user will be depends on cloud server. To decrease the computational and resource maintenance at the cloud server, cloud end user ensures the security , storage integrity and its outsourced .



The architecture of cloud data storage service

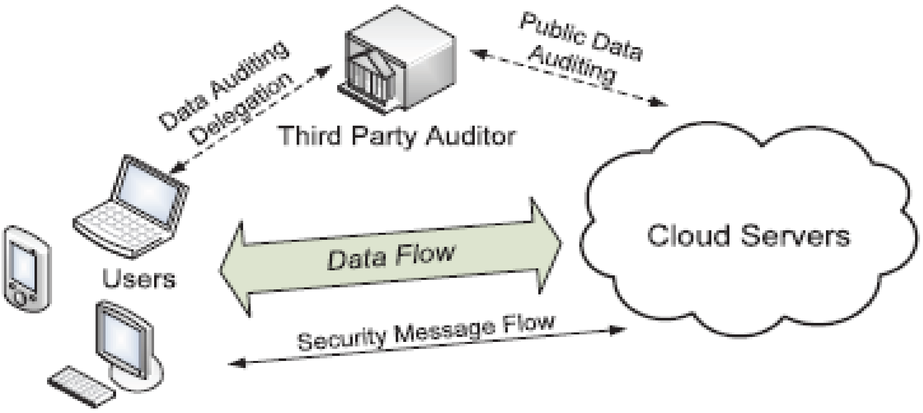
Design Goals

To ensure the data security and data integrity for cloud based model our model design should achieve the following tactics.

- TPA: TPA is allowed to to check the accuracy of cloud. Correctness of the
- storage : while storing one users data it should be unharmful to the other pieces of the files.
- Preserving the Privacy : the TPA is not allowed to read the data while collecting is collection during the auditing process.
- Auditing of batch : to process the request of multiple users at a same time TPA should enabled with secure mode.
- Lightweight : while doing the auditing The TPA is allowed to do it with low computation overheads and minimum communication with other entity of the system.

THE PROPOSED SCHEME

This section presents our actual auditing process for the cloud servers to provide data security and also verifies the data integrity of the data which stored at cloud based server. This model consists of different algorithms like keyGen, SigGen, GenProof, VerifyProof, HLA, MAC protocol etc. User runs keyGenalgothims for creating verification metadata which is consist of MAC. the remaining information will be used for auditing the data. The cloud server runs the GenProof to get the proof of data has stored successfully and keeps the track of data when last time it has modified and at what day. TPA runs the VerifyProof to audit the proof from cloud server.



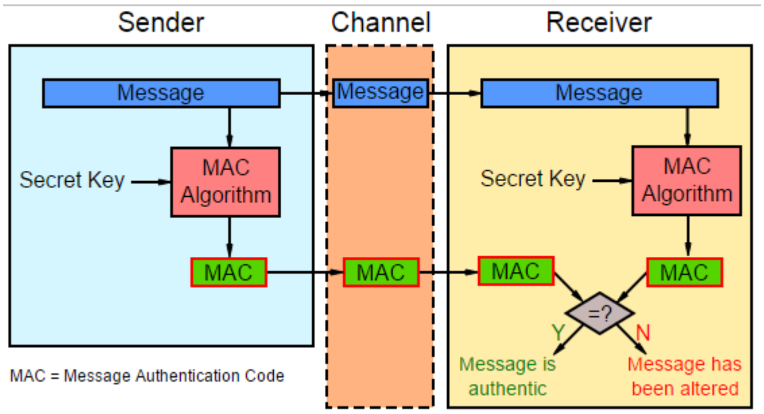
To execute this model we need to cover two phase which listed as follows:

- Setup: by executing the KeyGen the public and secret attributes initialized by user. File F is processed by the
- SigGen which creates the verification metadata. Upload this copy to the server and delete the local copy.
- Audit : to check the that whether cloud server has got the data file F properly or not at the time of the auditing The TPA will generate the audit message be assured. Then GenProof will get executed which automatically generates the verification metadata.

The basic schemes before showing the final output, we focused on the two parts of this scheme. One is MAC-based and another one is Homomorphic Linear Authenticator i.e. HLA-based.

MAC based Solution :

The authentication of data is done by using a message authentication protocol (MAC) . It accepts the secrete key as input and some message to be authenticated. After processing input it gives the MAC output. The data integrity and the authenticity of message is protected by this MAC value. Sometimes it is also called as Hash function. Secrete key both generates and verifies the Mac value. Before initializing a message transfer both sender and receiver agrees on same secrete key. By using two ways we can Authentic the data. One is by just uploading the data blocks with their MAC values. Then after TPA retrieve data and checks the correctness by using secret key.



When sender's and receiver's secrete key matches after successful execution of the MAC algorithm the only message transfer will triggered as shown

HLA-based :

Homomorphic encryption allow the complex mathematical operations to be performed on secret data without interfering the secrete message. In mathematics, homomorphic describes the change of one data set into another while preserving relationships between elements in both set. To effectively support public auditability without having to retrieve the data blocks themselves, the HLA technique can be used. HLAs, like MACs, are also some unforgettable verification metadata that authenticate the integrity of a data block. The difference is that HLAs can be aggregated. It is possible to compute an aggregated HLA which authenticates a linear combination of the individual data blocks.

CONCLUSION

In this paper, we have proposed the secured cloud based system for storing data at the cloud server. We integrated the HLA and MAC algorithm to get the required results. The TPA performs the auditing process which relives the unnecessary work of the user. This system makes the user free from their fear of outsourced data files. This long analysis shows that our layouts are provably secure and highly efficient.

REFERENCES

[1] Sh. Ajoudanian and M. R. Ahmadi ”A Novel Data Security Model for Cloud Computing” IACSIT International Journal of Engineering and Technology, Vol. 4, No. 3, June 2012.

[2] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Jin Li “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.

[3] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE “Security and Privacy in Cloud Computing” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.

[4] ChandineeSaraswathy K. , Keerthi D. , Padma G. “HLA Based Third Party Auditing For Secure Cloud Storage”ChandineeSaraswathy K. et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1526-1532.

[5] Yuchuan Luo†, Ming Xu†, Shaojing Fu†‡, Dongsheng Wang†, Junquan Deng† “Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation” 2015 IEEE Trustcom/BigDataSE/ISPA.

[6] Deyan Chen1, Hong Zhao “Data Security and Privacy Protection Issues in Cloud Computing” 2012 International Conference on Computer Science and Electronics Engineering.

[7] Kan Yang, Student Member, IEEE, and XiaohuaJia, Fellow, IEEE “An Efficient and Secure Dynamic Auditing

Protocol for Data Storage in Cloud Computing” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013.

[8] Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE “Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud” IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 1, JANUARY/FEBRUARY 2015.

[9] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation” IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 8, AUGUST 2016.

[10] ZoltánBalogh, Milan Turčáni “Modeling of Data Security in Cloud Computing” 978-1-4673-9519-9/16/$31.00 ©2016 IEEE.