IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Cloud Model - With TPA (Third Party Auditor)

Patel Himani Atulkumar [1], Patel Srushti Hasmukhbhai[2]

[1] Computer Engineering, G.T.U. P.G. School, Ahmedabad-380015, Gujarat, India

[2] Computer Engineering, R.G.P.V. P.G. School, Bhopal, India

Abstract

Cloud computing is a computing technique, where a large group of systems are connected to private or public networks, where data owner can store his data on remote systems and frees himself from storage burden and uses the data on-demand, anytime, everywhere. As, a Cloud data user does not possess direct control of his data, security is one of the few challenging issues which needs to be addressed. Security in Cloud computing can be addressed in many direction viz. authentication, confidentiality, integrity and many more. Data integrity or correctness is an issue where there may be some unauthorized alteration in the data without consent of the data owner.

General Terms:
Access Control mechanism, Authentication, data security et. al.

Keywords:
Trusted Third Party Auditor, Data Storage, Security, Cloud Computing

1. Introduction

Various issues related to Cloud computing includes Security of data from theft, Data Integrity on Cloud, Secure transmission of data to and from Cloud sever, Verifying files without much overhead/Computation , rights management, maintain security during sharing and many more. Data storage correctness or some time more generally referred as data integrity verification is one of chief Cloud security problems. Data can be altered by unauthorized entity without intimating to data owner. How would the data owner make sure that his data has not been modified by other intruders (or may be by the Cloud provider itself, accidently or intentionally). So detecting such kind of unlawful activities on data is an utmost priority issue. Data storage correctness schemes can be classified with TTP, based on who makes the verification. In case of TTP, an extra Third Party Auditor (TPA), some time in form of extra hardware or cryptographic coprocessor is used. This hardware scheme provides better performance due to dedicated hardware for the auditing process but has some drawbacks such as single TTP resulting into bottleneck in the system, mutually agreeing on a common TTP where there are thousands of users across the globe. Due to such kind of reasons, we prefer an approach where the functionalities of TPA are integrated in form of client application and the application can be downloaded by cloud user from cloud server. This client application provides all the cryptographic functionalities to achieve the goals of integrity, authentication and confidentiality. As this is a software approach, the performance of the overall system may not be comparable to dedicated hardware kind of TTP alternatives. To improve performance, we emphasize offline execution of computationally costly cryptographic algorithms. [22]

2. Achieving Integrity – With TPA

The cloud service provider is not completely trustworthy; it raises issues such as data security and privacy. One of the major security issues is achieving secure cloud data storage. Issue can be addressed into two directions first which makes use of trusted third party auditor (TTPA) and other which do not. Because of users convenient service provision it choose cloud storage. During the service process, users focus on the problem whether the data stored in the cloud is safe or not. But for the service provider, the main concern is the profits while providing convenient services. For both parties that focus on different aspects, the TPA operating as an independent and credible entity plays well in guaranteeing the trust relationship between the two parties. The TPA has professional authenticate knowledge and audit skills. Cloud storage service providers can also improve their services according to the audit report given by the TPA. The TPA mechanism refers to the comprehensive assessment of the phases of the cloud storage services including security management, configuration management, fault and abnormal management, data management, operation management and so on. Users may be unaware of the location of data while using cloud storage services due to the distributed characteristics of

cloud computing, which requires the TPA to be clear with the laws and regulations in the area where data have been stored. So this is the main consideration for the audit to service safety and configuration management. Agreement should specify the methods to process data, emergency measures to deal with failure and abnormal, continuous service providing and the consequences of SLA violation, and so on in detail for service providers. So this is the main consideration for the audit to fault and abnormal in service and data management. For providing storages and business access services externally, strict access control audit is particularly important. Access control audit to the system, network, and applications associated with cloud storage services can prevent viruses, network intrusion, data leakage and other security issues and also enhance management capacity of those services. [21], [9]

3. Proposed Model

The Fig. 1 represents the sequence of operation performed. Overall function is divided into 6 different steps. Details of steps are given below.
Step 1:- Client / TPA Generate Key pair
Client and Third party auditor (TPA) generate a key pair during step1 using a public key encryption in singe step which is used for encrypt data during transmission.
Step 1.1:- To get id from TPA and Client send registration request to TPA.
Step 1.2:- TPA Generate ID store key and ID, and send ID back to client.
Step 2:- Data Storage
Aim of step 2 is store the data generated by the client.
Step 2.1:- Client encrypt the file using symmetric key which is generated by different available encryption algorithm (AES,DES). Client send data file to Cloud Server Provider (CSP). CSP generate file id in this step.
Step 2.2:- Hash code calculate from encrypted file which is produce in step 2.1 and store in Data base. Also message digest has been done in this step. Client Easily access file from TPA with the Help of file id which is generated in step 2.1. Client again encrypt file using its private key and the newly encrypted file with some other information sent to TPA.
Step 2.3:- TPA send conformation regarding storing of data file to CSP.
Step 2.4:- CSP stores data.
Step 3:- Offline File Verification
Aim of this step is to check integrity of User's data on Cloud Server Provider.
Step 3.1:- TPA send its id, and based on id Cloud Server Provider reply with list of files which is owned by Client. TPA selects a file from list and selected file name send to CSP.
Step 3.2:- After some authentication CSP calculate hash code and send hash back to TPA. TPA Compares hash locally after decrypting.
Step 4:- Data Verification Client send request for rights. Clients send the id of file to the TPA from whom it wants file access. Cloud server generate file list from id and send file list back to TPA. User select file from list and send selection with request rights (i.e. altered or modified) on TPA.
Step 5:- Data Retrieval
TPA grants or denies the request and status sends to CSP who makes changes in database accordingly. User send a symmetric key for the file to TPA in case of granting the rights.
Step 6:- Data Update
User rights for file modification are checked by csp before overwriting the file on csp. The user sends hash code to user and after some verification user update hash in its local database.

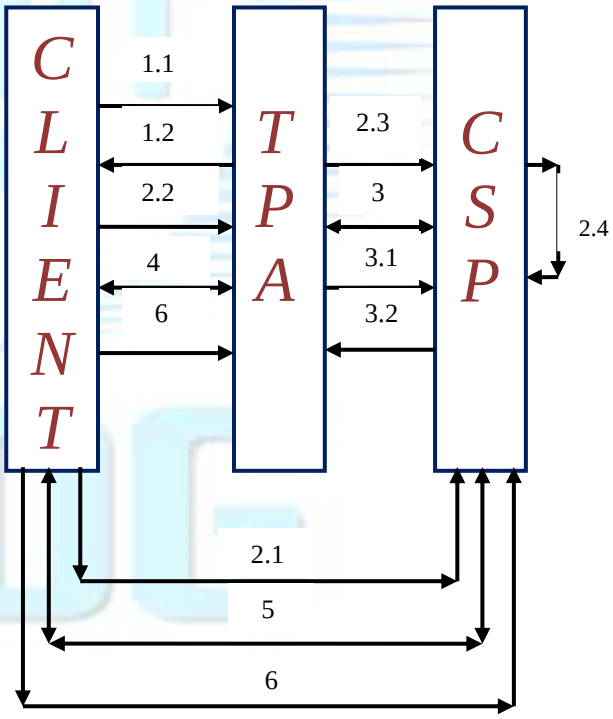

Fig. 1 Sequence of Operation.

4. Conclusions

Cloud computing security issues have brought us with great opportunities and challenges. Security in cloud

computing can be addressed with TPA and without TPA. In the cloud computing by using the TTPA mechanism we can increase the data security which is essentially a distributed storage system. To ensure each data access in control and reduce the complexity of cloud computing by help of Advance Encryption Technique (AES). Cryptographic techniques are used to provide secure communication between the client and the cloud. The system ensures that the client's data is stored only on trusted storage servers and it cannot be transferred by malicious system administrators to some corrupt node. Symmetric key sharing is handled with public key cryptography, to achieve faster performance and low computational overhead. The system achieves confidentiality and integrity of the client's data stored in the cloud. Also secure and efficient data dynamic operations such as update delete and append on the data blocks stored in the cloud. Our future goal is to design a secure cloud storage system with TPA which addresses the issues mentioned.

Acknowledgments

We would like to sincerely thank Prof. H. B. Patel for his advice and guidance at the start of this article. His guidance has also been essential during some steps of this article and his quick invaluable insights have always been very helpful. His hard working and passion for research also has set an example that we would like to follow. We really appreciate his interest and enthusiasm during this article.

References

[1] "Karumanchi, Sushama, "A Trusted Storage System for the Cloud" (2010). University of Kentucky Master's Theses. Paper 22 http://uknowledge.uky.edu/gradschool_theses/22

[2] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V 3.1, Nov 2011.

[3] W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", December 2011, NIST Special Publication 800-144.

[4] Ziyuan Wang "Security and privacy issues within the CloudComputing"http://ieeexplore.ieee.org/iel5/6085643/6086119/06086163.pdf2011 International Conference on Computational and Information Sciences

[5] SameeraAbdulrahmanAlmulla, Chan YeobYeun "Cloud Computing Security Management"http://ieeexplore.ieee.org/iel5/5523174/5542651/05542654.pdf

[6] Jiyi WU1, 2, Lingdi PING1, Xiaoping GE3,Ya Wang4, Jianqing FU1 "Cloud Storage as the Infrastructure of Cloud Computing" 2010 International Conference on Intelligent Computing and Cognitive Informatics.

[7] KrešimirPopović, ŽeljkoHocenski "Cloud computing security issuesand challenges" ieeexplore.ieee.org › MIPRO, 2010

[8] MarinelaMircea "Addressing Data Security in the Cloud" World Academy of Science, Engineering and Technology 66 2012 [PDF]https://www.waset.org/journals/waset/v66/v66-99.pdf

[9] Amala. U "Dynamic Audit Services for Achieving Data Integrity in Clouds" International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012 www.ijarcce.com/upload/.../20-Dynamic%20Audit%20Services.pdf

[10] Ling Li Lin Xu Jing Li Changchun Zhang "Study on the Third-party Audit in Cloud Storage Service" ieeexplore.ieee.org/iel5/6132470/6138497/06138525.pdf

[11] Shuai Han, Jianchuan Xing "ensuring Data Storage security Through A Novel Third Party Auditor Scheme in Cloud Computing" Proceedings of IEEE CCIS 2011

[12] Balakrishnan.s, saranya.G, Shobana.S, Karthikeyan.S "Introducing Effective Third Party Auditing (TPA) for Data storage security in Cloud" IJCST Vol.2, Issue 2, June 2011

[13] WassimItani, Aymankayssi, Ali Chehab "Privacy as a service: Privacy-Aware Data Storage and Processing in Cloud Computing architectures" 2009 Eighth IEEE International Conference on dependable, Autonomic and Secure computing.

[14] Ling Li, Lin Xu, Jing Li, Changchun Zhang "Study on the Third-party Audit in Cloud storage Service" International conference on cloud and Service Computing 2011.

[15] JunfengTian, Zhijie Wu "A Trusted Control Model of Cloud Storage" International conference on computer Distributed control and intelligent environmental Monitoring 2012.

[16] PrimožCigoj "Security Aspects of OpenStack" kt.ijs.si/markodebeljak/Lectures/Seminar%20I_Primoz_Cigoj.pdf

[17] Tuan Viet – DINH "Cloud Data Management ftp://ftp.irisa.fr/local/caps/DEPOTS/.../Dinh_Viet-Tuan.pdf

[18] SushamaKarumanchi "A TRUSTED STORAGE SYSTEM FOR THE CLOUD" http://uknowledge.uky.edu/gradschool_theses/22

[19] [19] Isaac Agudo , David Nuñez, Gabriele Giammatteo, PanagiotisRizomiliotis , Costas Lambrinoudakis " Cryptography goes to the Cloud"

[20] LepakshiGoud "Achieving Availability, Elasticity and Reliability of the Data Access in Cloud Computing" International Journal of Advanced Engineering Sciences And Technologies Vol No. 5, Issue No. 2,

[21] Hiren B. Patel, Dhiren Patel, "Achieving Secure cloud Storage without using of Trusted Third Party Auditor: a Review" International Journal of computer Applications (0975- 8887) Volume 57-No. 6, November 2012

[22] Krunal Suthar, Pramalik Kumar, Hitesh Gupta " SMDS: Secure Model for Cloud Data Storage" International Journal of computer applications(0975-8887) Volume 56-No.3, October 2012