IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013
ISSN: 2320 - 8791
www.ijreat.org

A Review of Addressing Storage Correctness in Cloud Computing With Trusted Third Party Auditor

Patel Himani Atulkumar [1], Patel Ameeben Atulkumar[2]

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

[2] Computer Engineering, S.P. College of Engineering, Visnagar-384315, Gujarat, India

Abstract

Cloud computing has become a significant new style of computing technology trend in recent years. A cloud computing is a dynamically scalable infrastructure in which virtualized resources are provided as services over the Internet. As data is stored on remote locations of cloud service provider and users do not have direct control over their data. Data security in cloud is very significant issue. Many researchers have proposed solutions of this problem in various directions. Broadly, we categorize the proposals in two group's viz. first, which make use of trusted third party auditor (TTPA) and second which do not make use of the same. Both the directions have their own strength and weaknesses. In this paper we discuss cloud computing, its service models, cloud security Issues & Challenges. We further analyze various solutions with TTPA and study their benefits in terms of data integrity, access control mechanism, data confidentiality etc.

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

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

1. Introduction

Cloud computing is a model for enabling ubiquitous & convenient on demand network access for share pool of configurable compute deploying resources(e.g. network, server, storage, applications and services).[6] In cloud computing there are mainly two broad classifications of models viz. service model and deployment model. Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS) are the three commonly known service models. Deployment models include public, private, community and hybrid types. The accessibility of Public cloud is almost anywhere. Anyone having Internet connectivity and required credentials can use the Public cloud from anywhere, anytime. Private cloud is use and managed by the single organization or third party and it is located on-premise or off-premise. Private clouds are used for safety reasons where organization does not want its resourced to be accessed by anyone except its own employees within the four walls. For the sharing purpose in different organization or specific sharing community we can use Community cloud. Hybrid cloud is a combination of a one or more public, private and community cloud. Irrespective of the service model and deployment type, a common problem in cloud adaptation is security, as the data owner loses her control over data. There has not been any universally adopted security model for cloud computing which is trusted by cloud users.

Cloud has centralized management of resources so it can reduce the unnecessary cost to system which is operating by the users. Cloud storage is built on the network computing environment. There are many benefits to move data into the cloud. For example, users do not have to worry about the complexities of direct hardware management. But since users store their data in the cloud, they lose its control data. Security becomes a significant issue to be addressed. Data security is always an important aspect of quality of service and it is also a key issue in cloud computing.

Traditional cryptographic primitives for data security cannot be directly adopted the environment of cloud [3].In cloud environment when there is service failure or system intrusion, authenticated and authorized access control mechanism is required to prevent stealing data. Security issues in cloud are divided into regulatory compliance, privileged user access, data location & data segregation, recovery and long term viability [8]. In this paper we discuss about trusted third party auditor which provides trustful data security. It is also claimed to reduce response

time and bandwidth during the communication between third party auditor and cloud service provider.

2. Review of Related Problem

In this section we review of proposed data storage security approach through TTPA. By using this approach to make an assurance of trustfully and reliable to make the system. Shuai han [1] efficiently protect data flow with the third party auditor function move into cloud service provider and achieve security trustful and independent with use of advanced cryptographic technique RSA to encrypt all data flow between servers in the advance cloud service provider. And bilinear Diffie-Hellman helps to insure the security while exchanging long keys which is use of up-to-date implementations. Third party auditor has expertise and capabilities that users do not have and it is trusted to access and expose risk of cloud storage services on behalf of the users upon request. Also TTPA is invariably online and makes every data access be in control. Design a message header and series of mechanism to accomplish the authentication and confidentiality to access privilege with minimum cost. S Bal [2] in cloud data storage security, public audit ability is importance so that users check the outsourced data integrity. The third party auditing process on behalf of the cloud client to verify the integrity of dynamic data stored in cloud computing. In Public cloud data auditing system, TTPA utilize and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy preserving. In the dynamic data user can perform various block level operations like delete, update and append for modify the data file while maintaining the assurance of storage correctness [2].

Table 1: Comparison table of TTPA Based

No Of paper	Server/platform type of cloud storage	Key (Public/ private)	Algo.	Protocol	Data type	Cost	User/server side encryption
1	Distributed cloud storage server	Public	RSA	Bilinear Diffe-hellman	Data file pack-et	Mini-mum	User side encryption
2	Distributed cloud storage server	public	Homomorphic authenticator	Privacy preserving protocol	Dynamic data	lower	User side encryption
3	Single cloud storage sever	Public/ private	Secure SSL	Privacy proto-col	s/w and data	reduce	Server crypto coprocessor
4	Cloud storage service	Fixed length of encryption Key	RSA	Privacy policy	File sharing	Mini m-ize	User or server side
5	Different cloud storage platform	Public/ private	Cipher text attribute based encrypt-ion	Cloud storage server with protocol	File sharing	reduce	User or server side

Wassim Itani [3] Paas a set of security protocols and secure cryptographic coprocessor for providing trusted, isolated, ensuring the privacy of customer data in cloud computing. For customer registered in the privacy service every physical server running a virtual machine within crypto coprocessor. To be shared among more than one cloud customer PaaS allows the resources of the crypto coprocessor for economically feasible solution. On the crypto coprocessor more than one cloud customer for trusted third party required sharing mechanism to load the cryptographic data structure and keying material. TTP is to load a set of private/public key pairs which is allocated single customer into the persistent storage of the crypto coprocessor. When the latter and upon registers with the cloud privacy service and the cloud customer will securely receive a copy of their public/private key. Keys are updated remotely after the crypto coprocessor installed in the cloud computing. These are the use for the system to copy with dynamic user workload and changing resources due to over time. Ling Li [4] Cloud computing security issues for necessary to provide solution with TTPA for ensuring data security and reliability of cloud computing services. Also propose idea of bringing in the TPA mechanism into the file-sharing system and analyze the reliability of the system with the typical architecture of cloud storage services. If TPA supports batch audit, it can shorten audit time and reduce the computational cost for TPA. With the TPA mechanism the assurance of reliability for the system. Junfeng Tian [5] the authors present a trusted control model of cloud storage (TCMCS). Using the cipher text access control and integrity verification, TCMCS makes the users' data safe. With access control a security cloud storage model to handle and ensure the transparency of the data manipulation to all the interactions between a client and CSS. It is TCMCS that shield the differences among different cloud storage platforms, which can separate operations that protected both security and integrity of data from users' application. In the TCMCS model searching and retrieve all data files, encryption-decryption, data processor to verify information of

integrity, data backup and recovery facilities are there. And also experiment with Eucalyptus as the cloud computing platform to perform experiment steps. Get the result is TCMCS model is made users' data secure and improved the performance in data processing.

3. Conclusion

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. Also secure and efficient data dynamic operations such as update delete and append on the data blocks stored in the cloud. The Paas protocols to provide trusted and isolated execution environment in cloud computing. So, with the help of TTPA we great opportunity against the cloud computing security issues and challenges.

4. Future Work

Trusted third Party Auditor (TTPA) is a reliable independent component which is trusted by both the cloud users and server and has no incentive to conspire with either the cloud server or user during the auditing process. TTPA has the skill and competence that normal cloud users may not have. In order to save time and reduce overhead due to computation & communication operations, many researchers recommend the support of trusted third party (TTP). By leaving the resource consuming cryptographic operations on TTP for achieving confidentiality and integrity, cloud users can be worry-free. Apart from offering so many benefits, the risk of getting the TTP compromised may not be completely denied. TTP may become the bottleneck for overall operations of the system and may result into performance diminution. In this Paper, we assess recently proposed approaches which make use of TTPA to achieve data storage correctness in cloud computing. In the future, we will improve the model with TTP mechanism to make more security and efficiency.

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

[2] 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

[3] Wassim Itani, Ayman kayssi, 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.

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

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

[6] W. Jansen, T.Grance, "Guidelines on security and Privacy in Public cloud computing", NIST Special Publication *00-144, December 2011.

[7] Hiren Patel , Dhiren Patel "A Review of Approaches to achieve Data storage correctness in cloud computing Using Trusted Third party Auditor"

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

[9] Primož Cigoj "Security Aspects of OpenStack" kt.ijs.si/markodebeljak/Lectures/Seminar%20I_Primoz_Cigoj.pdf

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

[11] Sushama Karumanchi "A Trusted Storage System For The Cloud" http://uknowledge.uky.edu/gradschool_theses/22

[12] Isaac Agudo , David Nuñez, Gabriele Giammatteo, Panagiotis Rizomiliotis , Costas Lambrinoudakis " Cryptography goes to the Cloud"

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

[14] Sameera Abdulrahman Almulla, Chan Yeob Yeun "Cloud Computing Security Management" http:// ieeexplore.ieee.org/iel5/5523174/5542651/05542654.pdf

[15] 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.
[16] Krešimir Popović, Željko Hocenski "Cloud Computing Security Issues and Challenges" ieeexplore.ieee.org › MIPRO, 2010
[17] Marinela Mircea "Addressing Data Security in the Cloud" World Academy of Science, Engineering and Technology 66 2012 https://www.waset.org/journals/waset/v66/v66-99.pdf
[18] 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/.../20Dynamic%20Audit%20Services.pdf
[19] 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
[20] 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