ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Review on Augmented Security by TPA in Cloud Computing

Sashibala, Deepika Goyal

M.Tech(pursuing), Dept. of CSE, Advanced Institute of Technology and Management, Palwal, Haryana under the Affiliation of Maharshi Dayanand University, Rohtak, Haryana, India

Assistant Professor, Dept. of CSE, Advanced Institute of Technology and Management, Haryana under the Affiliation of Maharshi Dayanand University, Rohtak, Haryana, India

ABSTRACT: Cloud Computing is evolving and thought of next generation design for computing, generally cloud computing could be a combination of computing recourses accessible via net. Traditionally the client or organizations accumulate data in data centers with firewall and other safety measures techniques used to guard data against intrudes to access the data. Since the data was confined to data centers in limits of association, the direct over the data was more and well distinct procedures could be used for access its own data. However in cloud computing, since the data is stored anywhere across the globe, the client organization has less control over the stored data. To built the reliance for the growth of cloud computing the cloud providers must protect the user data from unauthorized access and disclosure. One modus operandi could be encrypting the data on client side before storing it in cloud storage, however this technique has too much burden from client perspective in terms of key administration, continuance viewpoint etc. Other way could be this kind of security service like computing hash of data and verifying truthfulness of data, encryption/decryption service if provided by same cloud storage provider, the data conciliation cannot be ruled out since same provider has access to both storage and security service. Divide and rule can be one of the techniques, meaning dividing the errands amongst different cloud services providers can benefit the client. A trusted 3rd party cloud provider be used to provide security services, while the other cloud provider would be data storage provider. The trusted 3rd party security service provider would not store any data at its end, and its only confined to providing security service. The application or software will provide data integrity verification by using hashing algorithm like SHA-1, provide encryption/decryption using symmetric algorithm like AES, and defining band of people who can access the shared data securely can be achieved by defining access list. The Software is only responsible for encryption/decryption, computing/verifying the hash of the data and does not store any data in trusted 3rd party security system server. The encrypted data along and original data hash are stored in Separate Cloud (Security Cloud), therefore even if the storage cloud system administrator has access user data, since the data is encrypted it will be difficult for the system administrator to understand the encrypted data. While the user downloads the data from Storage Cloud, it is decrypted first and then new hash is calculated which is then compared with hash of original data stored in Security Cloud. Finally, this software/application provides the user with the ability to store the encrypted data in Storage cloud and hash and encryption/decryption keys in security cloud service, and no single cloud service provider has access to both. Other benefit of delegating responsibility to trusted 3rd party is that it reliefs the client from any kind of key management or over head is maintenance of any key information related to data on it device, because of which it allows the client to use any browser enabled devices to access such service.
.

KEYWORDS: Cloud computing; Hash service; encryption and decryption service; data protection and integrity, third part auditor (TPA).

I. INTRODUCTION

With evolution of computers the life of people became more and more easily. They were able to keep their data on their devices, and started finding ways to make them accessible to others, for example say by using floppy, writable disks, which was followed by portable hard-disk, all these where expensive in their own way during their time. The

DOI: 10.15680/IJIRCCE.2017. 0504096

data was very much private on personal devices like PC, laptops, mobile phones etc, therefore sharing data with others was considered to be expensive. As the world of computing got more advanced the ways for sharing data started becoming cheaper and cheaper. In recent years a new term has evolved call"Cloud" which is provided by different provides, and which is nothing but facility or service of different resources or components like hardware, platform, storage's, software etc, and it is gaining importance because it frees the user from maintenance perspective on a investment of some money for the use of these services provided by cloud service providers. Now to provide such service to the client, naturally the provider's must have and rather can have access to resources which are used by the people/clients. Among the reasons these access are greatly required are for maintenance perspective. And definitely since billions of clients will be thinking about using such service, the infrastructure ought to be capable enough to support them, and these resources ought to be shared between billions of client's. Service availability, data synchronization between different devices, availability of data via any devices which includes browser facility make cloud more attractive. Now since the info gets shared or stored in providers area, the client gets worried about privacy of its data, although there are certain agreements and SLA which are agreed by cloud provider and client. Now although client have a platform to generally share the info, the expense of securing his/her data or in a nutshell making its data private gets costlier. The cloud term is of interest not just to the patient clients but to organizations as well. With organization as a consumer the concern of data security becomes multi-fold. Consider a typical example of small scale business that has different departments like HR, Finance, etc. We will focus on finance department since finance details of any business/company/organization are considered to be very sensitive and must be confidential. Therefore if the little scale company thinks of using the cloud services like storage. Storing all account/finance related information in cloud stored makes it prone to leakage of sensitive information tell un-authorized users. Therefore securing this finance data is vital before it gets uploaded to the storage cloud, and just in case the data stored in cloud storage gets tampered there should be a method to verify the integrity of the data, moving further specific band of people should have access to this data which may be folks from finance department of client company or special auditors. Simply speaking the client must have the ability to store the data securely, verify the integrity of the data, share the data securely with specific band of people.

The clients concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You can find multiple means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes more tedious for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised. The aforementioned approaches burdens the client by which makes it additionally accountable for securing it data before storing it to the cloud storage.

Cloud computing is a method in which computing power, memory, infrastructure can be delivered as a service. A Cloud computing is a set of network enabled services, guaranteed QOS, inexpensive computing infrastructures on demand with an easy and simple access. Cloud security is an evolving sub-domain of computer security, network and information security [8]. Security in cloud can be implemented remotely by client where the data centres and protocols in the security objectives of the service provider are: i) confidentiality for securing the data access and transfer ii) audit ability for checking whether the security aspect of applications has been tampered or not. Dimensions of cloud security have been aggregated into three areas like security and privacy, compliance and legal issues.

A. Cloud software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The application is accessible from various client devices through web browser.

B. Cloud platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired application created using programming languages and tools supported

DOI: 10.15680/IJIRCCE.2017. 0504096

by the provider.

C. Cloud infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, network and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating system and application.

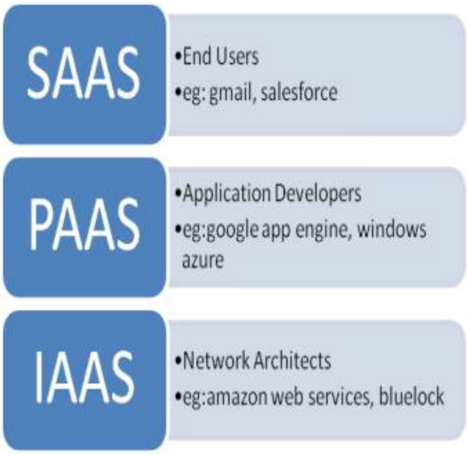

Figure 1: Various Cloud Services

a. On-demand self service**:** Computing capabilities can be provisioned to the consumers.
b. Broad network access: Capabilities are present in the network which can be accessed through standard mechanisms.
c. Resource pooling: The provider’s computing resources are pooled to serve multiple consumers with different physical and virtual resources dynamically assigned and reassigned according to the demand of consumer.
d. Rapid elasticity: Capabilities which allows rapid and elastic provisioning.
e. Measured service: Cloud systems which automatically control and optimize resource usage with a metering capability at some level of abstraction according to the type of service.

Security One of the major problem affecting the cloud computing is the integrity [4] of the cloud data. The threads of the data can overcome by using the assistance of a TPA. Introducing a model for checking the integrity over the cloud computing with the support of TPA using Digital Signature Technique.Fig.1 shows the architecture. The checking is performed over two parts: the cloud service provider (CSP) and TPA without giving any secure data.The Digital Signature first takes the user data and performs a hash function using Message-Digest Algorithm (MD5) [9]. For the generated hash value computes the signature by encrypting it with private key. On the other side decryption can be performed by the public key which contains a hash value in the reversible order of its original data. Users rely on the cloud server (CS) for cloud data storage and maintenance. They may interact with the CS to access and update their stored data for various applications. The Third Party Auditor (TPA) eliminates the auditing of client to check where his data is stored in the cloud. Since the services in cloud computing are not limited to data backup ,so the dynamic support of data such as block modification, insertion and deletion is significant [11]. The previous works lacks the support of either public auditability or dynamic data operations, where it achieves the both with remote data integrity. It first identifies the security problems and difficulties of direct extensions with full dynamic data updates from the prior works and then shows how to construct a verification scheme for the integration. By manipulating the classic Merkle Hash Tree construction for block tag authentication the efficiency of data dynamics can be achieved. To support efficient handling of multiple auditing tasks, the technique of bilinear aggregate signature to extend the result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously.

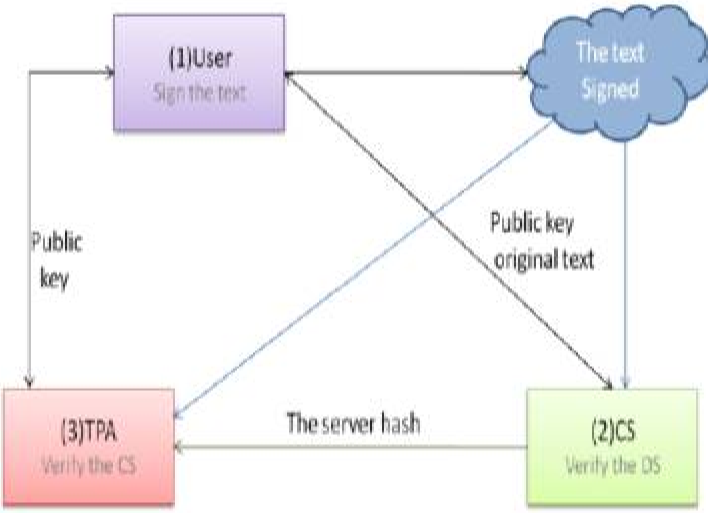

Fig.2: The Architecture of data integrity checking in cloud

II. LITERATURE REVIEW

Every coin has 2 side, and cloud computing is no exception. There is criticism about privacy in cloud model, because of the fact that administrator have access to data stored in the cloud. They can unintentionally or intentionally access the client data. Traditional security or protection techniques need reconsideration for cloud. Except for private cloud where organization does not have control over the equipment, the progress of cloud is seems little slow, because organizations think instead of compromising on the security of the data, they are still willing to invest in buying private equipment to setup there own infrastructure. Security issues which are of concern to the client can be classified into sensitive data access, data segregation, bug exploitation, recovery, accountability, malicious insiders, and account control issues. Like different disease have different medicines, different cloud security issues have different solutions, like cryptography, use of more than one cloud provider, strong service level agreement between client and cloud service provider. Heavy investment is needed to secure the compromising data in cloud. Cloud can grow only if it is possible to build a trust in client, and which can be built only if security concerns are being addressed.
Following are some of the concerns:
1. System Complexity Compared to traditional data centre the cloud architecture is much more complex. Therefore while considering security, security of all these components and interaction of these components with each other needs to be addressed [13].
2. Shared Multi-tenant Environment Since the cloud need to provide service to millions of client, a logical separation of data is done at different level of the application stack [13]. Because of which a attacker in the face off client can exploit the bugs gaining access to data from other organizations [13].
3. Internet-facing Services The cloud service which is accessed over the internet via browser, the quality of service delivered on the network is another concern [13].
4. Loss of control As the data of client is stored anywhere across the world control loss over physical, logical of system, and alternative control to clients assets, mis-management of assets are some additional concerns [13].

Cryptography is a field of computer science & mathematics which deals with information security and related issues, in particular encryption and authentication. In greek the word kryptos mean ”hidden” while the word graphein mean ”to write”. During encryption a plain-text is converted into cipher text, while the reverse process termed as decryption converts the cipher text into plain-text. The cipher is in unreadable format.

AES: The Advanced Encryption Standard (AES) is a symmetric key encryption/decryption algorithm for converting plain-text to cipher text and vice-versa. Since the same key or master key is used, the must be kept secret or with trusted 3rd party, because compromise of this key would mean compromise to the data. Deffie Hellman Diffie Hellman key exchange is a technique to exchange cryptographic keys between 2 parties with no prior knowledge of each other. It allows the 2 parties to establish a secret key which can be used for further secured communication.

SHA: SHA stands for ”Secure Hash Algorithm”, SHA-1 is a cryptographic hash function technique where hash of data is computed. As compared to SHA-0, SHA-1 is widely used because it corrects errors in SHA hash specification, which led to weakness.

II. PROPOSED WORK

Our objective in the scheme is to build a security service which will be provided with a trusted 3rd party (TPA), and would lead to providing only security services and wouldn’t store any data in its system.
Detailing it further.
1. To construct Web service system which would provide data integrity verification? Provide encryption/decryption of the consumer data.
2. Defining access list for sharing data securely with specific band of individuals.
3. To construct thin client application which would call this web service before uploading/downloading the data to and from cloud.

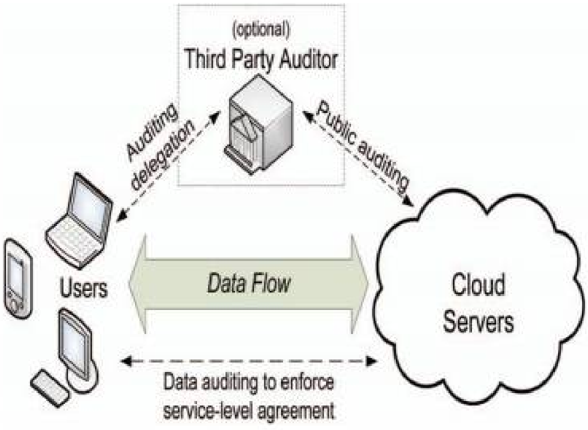

Figure3: Proposed TPA Scheme

In the cloud data storage, users store their data and no longer posses the data locally. In the distributed cloud servers, the correctness and availability of the data files being stored. One of the key issues is to effectively detect any unauthorized data modification and corruption. The Third Party Auditing allows to save the time and computation resources with reduced online burden of users. Security for the TPA can be provided by along with homomorphic tokens developed using our own augmented hashing algorithm and ensure coded data with appropriate TPA signatures.

REFERENCES

1. Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, and Song D, “Provable data possession at untrusted stores,” in Proc. of CCS’07. New York, NY, USA: ACM, 2007, pp. 598–609
2. Ateniese G, Pietro R.D, Mancini L.V, and Tsudik G, “Scalable and efficient provable data possession,” in Proc. of SecureComm’08. New York, NY, USA: ACM, 2008, pp.1-10.
3. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, andP. Rogaway. UMAC: Fast and secure message authentication.In CRYPTO, volume 1666 of LNCS, pages 216–233, 1999.
4. Bowers K.D, Juels A, and Oprea A, “Hail: A high-availability and integrity layer for cloud storage,” in Proc. of CCS’09. Chicago, IL, USA: ACM, 2009, pp. 187–198.
5. M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery,” ACM Trans. Computer Systems, vol. 20, no. 4,pp. 398-461,2002
6. Chang E.C, and Xu J, “Remote integrity check with dishonest storage server,” in Proc. of ESORICS’08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.

7. Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing environments," in Proceedings of Natural Sciences and Engineering, Sweden, pp. 2-4, 2010.
8. Cong Wang,Qian Wang,Kui Ren Ninig Cao and Wenjing Lou"Towards Secure and Dependable storage services in cloud computing",IEEE Transaction on service computing,vol 5,no 2,june 2012
9. Dalia Attas and Omar Batrafi " Efficient integrity checking technique for securing client data in cloud computing", October 2011
10. Jaison Vimalraj.T,M.Manoj"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", March2012
11. Kayalvizhi S,Jagadeeswari "Data Dynamics for Storage Security and Public Auditability in Cloud Computing", February 10, 2012
12. Metri P. and Sarote G., "Privacy Issues and Challenges in Cloud computing," International Journal of Advanced Engineering Sciences and Technologies, vol. 5, no. 1, pp. 5-6, 2011.
13. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012
14. D. Srinivas "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011
15. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing tokeep online storage services honest," in Proc. Of HotOS'07., CA USA: USENIX Association, 2007, pp. 1–6.
16. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality ofService (IWQoS '09), pp. 1-9, July 2009