ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DATA STORAGE SECURITY IN CLOUD COMPUTING USING THIRD PARTY AUDITOR (TPA)

Rahul K. Morghade*, Sonal Honale
* Department of Computer Science & Engineering Abha Gaikwad Patil College of Engineering, Nagpur

DOI: 10.5281/zenodo.58555

ABSTRACT

Cloud Computing is evolving and considered next generation architecture for computing. Typically cloud computing is a combination of computing recourses accessible via internet. Historically the client or organisations store data in data centres with firewall and other security techniques used to protect data against intrudes to access the data. Since the data was confined to data centres in limits of organisation, the control over the data was more and well defined procedures could be used for accessing its own data. However in cloud computing, since the data is stored anywhere across the globe, the client organisations have less control over the stored data. To built the trust for the growth of cloud computing the cloud providers must protect the user data from unauthorised access and disclosure. One technique 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 management, maintainence perspective etc. Other way could be this kind of security service like computing hash of data and verifying integrity of data, encryption/decryption service if provided by same cloud storage provider, the data compromise 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 responsibilities 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 maintainance 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.

INTRODUCTION

Cloud computing describes the combination of logical entities like data, software which are accessible via internet. Client data is generally stored in banks of servers spread across the globe. 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 maintainance, the security service provided by the cloud storage provider, the information might be compromised. The forementioned approches burdens the client by which makes it additionally accountable for securing it data before storing it to the cloud storage.

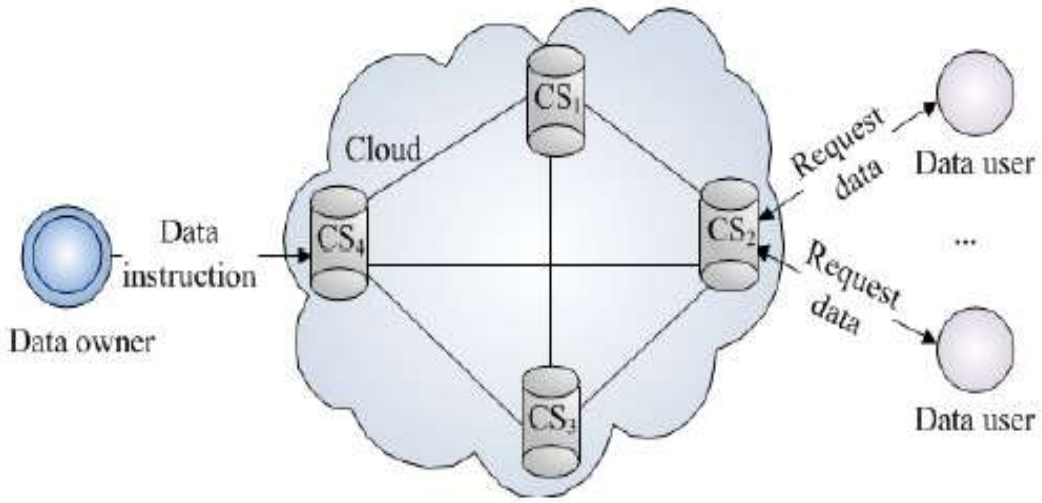

Fig. 1.1: A Typical Cloud Environment

Our objective is to build a security service which will be provided with a trusted 3rd party, 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.

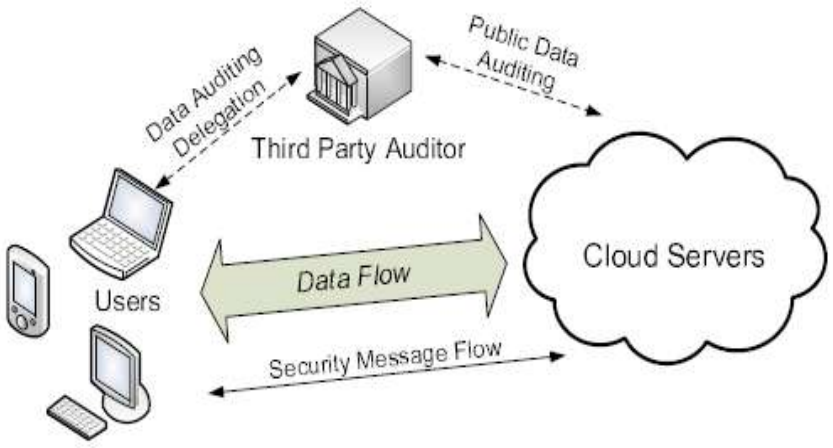

Fig 1.2: The architecture of cloud data storage service

ISSN: 2277-9655
Impact Factor: 4.116

System Design

The system provides hash, access list, encryption/decryption by a trusted 3rd party over the network in the form of "Software as a Service" (SaaS). The system has a separate storage service which is also provided as a SaaS. The data storage for each client is done in database in the form of "BLOB". The trusted 3rd party which provides these security services does not store any data at its ends, and stores only master key for each client for data encryption and decryption, and hash of the data which is calculated on client side. To enhance the security, the communication between client and security server is secured using Diffie Hellmen key, which is used as a input for AES. This division of responsibility has big effect, as no single provider has access to other data and security key, hash at the same time. Figure show the use case diagram of the system.

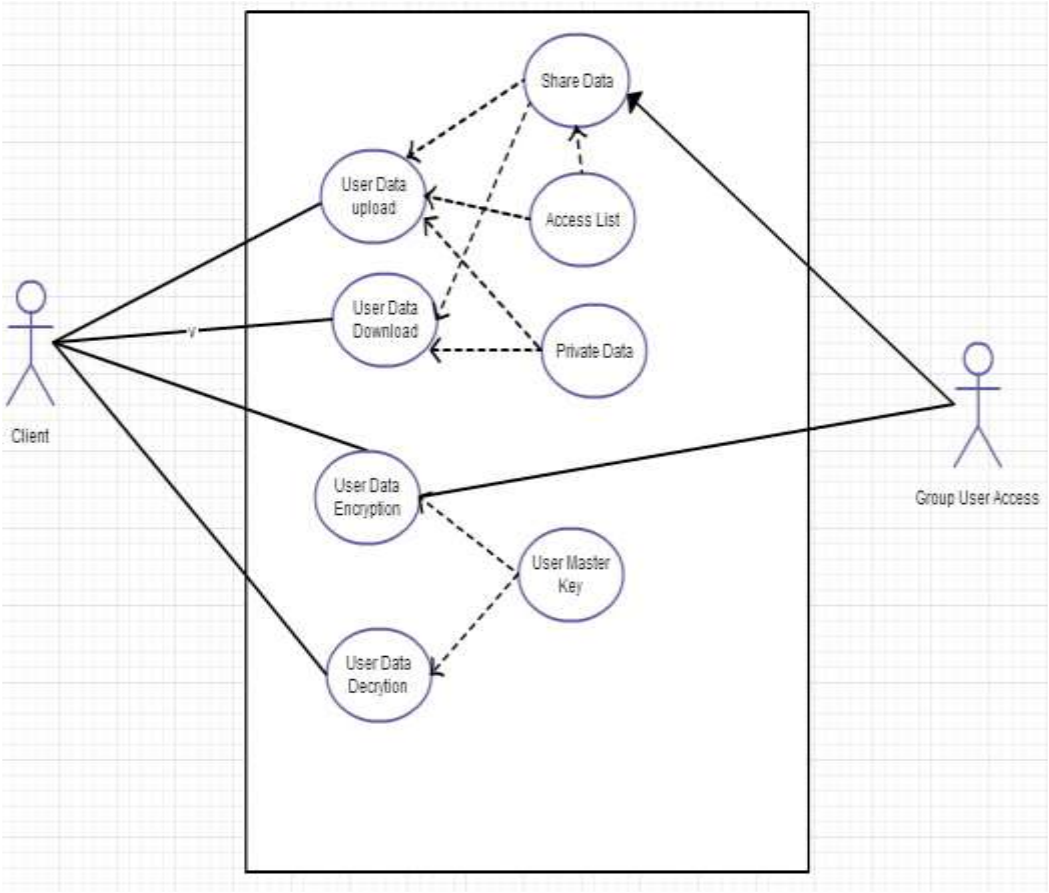

Figure 3.2: Use Case

Auditing:

As the SLA agreement is not transparent to the users, there comes the need to have auditing to check for SLA violation. There are two types of auditing depending upon which is being audited: Internal Audit and External Audit. Internal Audit audits the processes that takes place in providing the service. External Audit audits the quality of service such as CPU performance, availability and SLA parameters.

Audit can be both static and dynamic. In static auditing , auditing is done periodically to verify the integrity of data. Samples are taken from the data and it is verified for integrity of data. In dynamic auditing, auditing is done on dynamic data. The dynamic data operations are modification, insertion and deletion. Batch auditing is required when there is multiple owner and multiple cloud servers.

The issues arise in which entity can perform auditing. If auditing is done by Cloud providers they may hide their faults and violations. On the other hand if the user does the auditing, it adds the overhead to them. The solution is to have a third party entity to do the auditing. The third party should be neutral to both the Cloud provider and Cloud User.

Third Party Auditor (TPA):

The Cloud users send the data to Cloud service provider through the network. The user data may contains very sensitive data like user personal information, Bank details, Password, Important key Word, Business client details etc. Cloud service providers normally use Secure Socket Layer (SSL), Point to Point Tunneling protocol (PPTP), VPN for secure transaction. We are having history that attackers and intruders have win over this type of security services. While transferring the data between user and the cloud service providers very hard to avoid malicious attack. But users need assurance legally about the security over their data. For this we need a authentication mechanism based on the third party. This third party should common for both cloud user and the Cloud Service Providers. This third party monitor the activities of cloud user and cloud service provider. Normally cloud service providers and client will have a Service Level Agreement (SLA). This is a legal agreement between Cloud service provider and the client. Both parties have to follow the rules and regulations mentioned in the SLA. This agreement includes the Cloud service provider's quality of service, Standard of the service, service monitoring and controlling. The Cloud service may give lot of commitment and service offers to the cloud user due to market competition. But any point of time he has to follow it. The cloud service providers for their own benefits they will hide the data errors from the cloud user. To avoid this problem and to maintain the security standard we need a Third Party Auditor (TPA).The TPA will monitor the both client and Service Provider side activities. TPA will follow the auditing norms and techniques, also they will have list of auditing strategies. The TPA should familiar with the SLA between cloud service provider and cloud user. TPA will play promising role between this two parties. TPA having ability to check the integrity of the data which stored in the cloud. The auditing should not affect the privacy of the cloud users.

Here the cloud user mainly concern about their data security. Data Security comprises of Data integrity, Data Availability, Data Confidentiality. As the data is stored In order to verify the data integrity at un trusted servers become a big concern with cloud environment. Data security means protecting the data from the unwanted actions from unauthorized users and protecting from destroy forces. The forces may in any form of hardware failure, software failure, network failure, system failure, external forces, natural calamities etc. The unauthorized user may be intruder. We have to monitor the all user activities, if we found any unauthorized function from any user, immediately we should block the particular user before damaging the data. Data Integrity means maintaining the accuracy and consistency over the cloud user data at any point of time. The cloud user may store key information in the cloud storage, the accuracy of the user data information should be accurate in any point of time. Data Confidentiality means maintaining the secrecy about the user data. Confidentiality is a set of rules and promises to maintain the secrecy over some cloud user data information. The Cloud Service Provider should not enclose that information to anybody in any point of time.

The auditing process consists of three different type of phases. Planning, Execution and Reporting. In planning stage the TPA have to finalize the following important tasks, Content to audit, Time schedule of the auditing, duration of auditing, area of auditing, audit team size etc. The audit time and team size depends up on the size of the content. Execution is the important phases. In this phase we have to analysis the security threats in the cloud storage, monitor the previous threats and determine the level of previous threats. Also have to do the data integrity check. Reporting is the report of execution phase, this report will help the Cloud service provider to improve their service. The third party audit report mention the complete details about the cloud user activities and performance of the cloud service providers. According to this audit report Cloud Service Providers can monitor the activities of the user, if any user acting like the attacker we can cancel the agreement. At the same time Cloud Service Provider can improve the service efficiency of the service by this audit report. Because this audit report indicate the both user and cloud service provider performance.

ISSN: 2277-9655
Impact Factor: 4.116

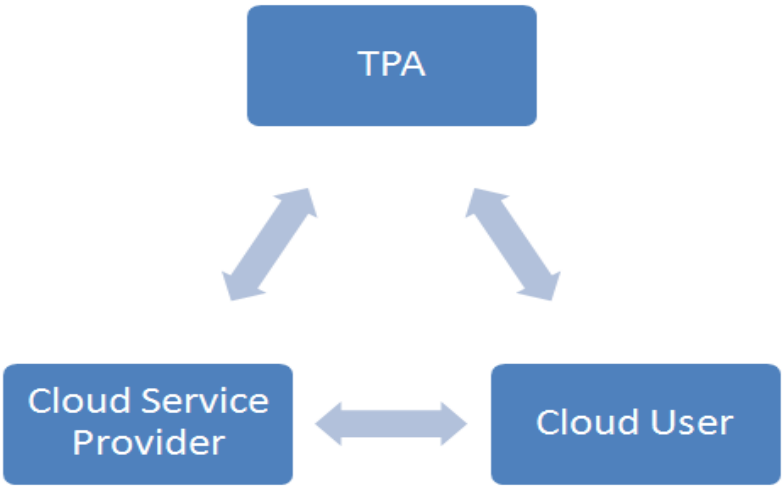

Fig: TPA in Cloud

Public Batch Auditing means TPA can do simultaneous integrity check on multiple cloud user's data, which stored in a multiple cloud.

Role of TPA:
The TPA process works in three steps: Key Generation , Server integrity proof, integrity verification.

Key Generation: Key generation is done by the Owner. The data is encrypted using the private key of the owner and public key is transferred along with the data.

Server Integrity proof: TPA dispute the server to give a proof of data integrity. The server sends the proof.

Integrity Verification: On receiving the proof from the Server, TPA verifies the integrity without encrypting the data. The tag in the data helps the TPA to check the data efficiently.

The Auditing can be done periodically on samples of data. Over the period, the samples are collected and verification is done for the samples. This type of auditing falls under static category. On verification if the auditor is convinced with the data integrity, the auditor erases the local data.

Dynamic Auditing
As data in Cloud is dynamic, static auditing is not enough. A dynamic auditing is needed to verify the data integrity of the dynamic data. But as data are dynamic in cloud, it is not easy to have an auditing efficiently. Server can enforce Replay attack and forge attack to fail the auditing process. The dynamic operations include modification, insertion and deletion. Whenever dynamic operation is performed, the owner sends the update message to the auditor representing the index number of that message. The Auditor updates the table. The message m and the tag are replaced by the new message and tag in message modification. The new message m and new tag are inserted in insertion operation. The message m and tag are deleted from the index table and all the entries below the deleted message move upwards.

ISSN: 2277-9655
Impact Factor: 4.116

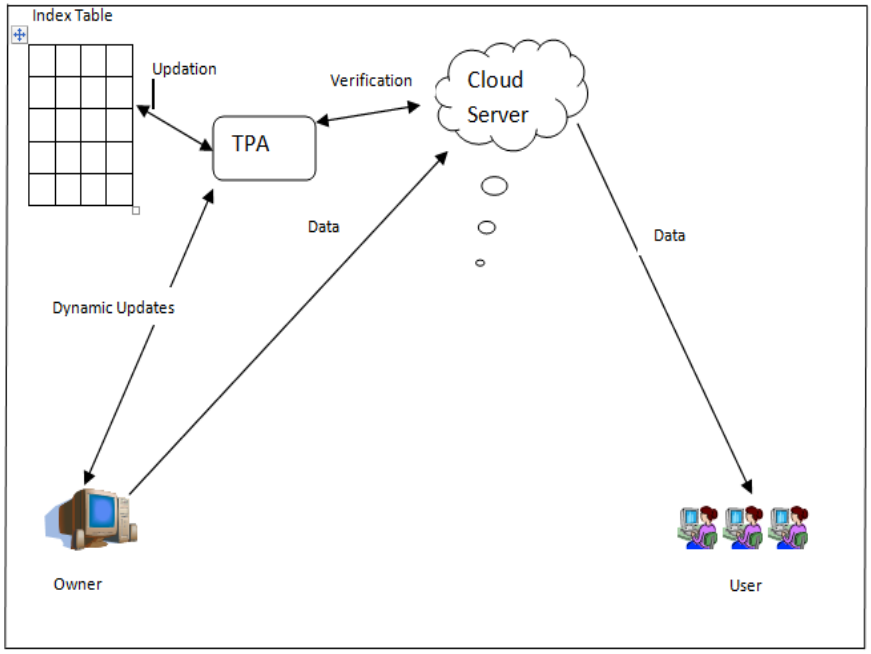

Fig: Dynamic TPA System

After performing updates in the table, the auditor conducts the data integrity test for the updated data. Auditor sends the result to the owner and he deletes the local copy of updated data.

CONCLUSION AND FUTURE WORK

We have seen how delegation of responsibility trusted 3rd party which provides security services secures user data. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can share the data securely with specific band of people without any overhead of key distribution.

To enhance the security more, a mechanism to secure the keys in security cloud can be a area of research. To reduce the overhead of network tra_c can be another area of research.

REFERENCES

[1] K.Govinda, V.Gurunathaprasad, H.Sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud through Digital Signature using RSA" International Journal of Advanced Scientific and Technical Research (Issue 2, Volume 4- August 2012) ISSN 2249-9954.
[2] S. Sivachitralakshmi,T. Judgi, "A Flexible Distributed Storage Integrity AuditingMechanism in Cloud Computing", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.
[3] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"
[4] K.Govinda, V.Gurunathaprasad, H.Sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud through Digital Signature using RSA" International Journal of Advanced Scientific and Technical Research (Issue 2, Volume 4- August 2012) ISSN 2249-9954.
[5] Nandeesh.B.B, Ganesh Kumar R, Jitendranath Mungara, "Secure and Dependable Cloud Services for TPA in Cloud Computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-3, August 2012.

[6] Boyang Wang,Baochun Li,Hui Li, "Public Auditing for Shared Data with EfficientUser Revocation in the Cloud".
[7] R.Ushadevi, V. Rajamani, "A Modified Trusted Cloud Computing Architecture based on Third Party Auditor (TPA) Private Key Mechanism", International Journal of Computer Applications (0975 – 8887) Volume 58– No.22, November 2012.
[8] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", IJCST Vol. 2, Iss ue 2, June 2011
[9] Tharam Dillon, Chen Wu and Elizabeth Chang. Cloud Computing: Issues and Challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications.
[10] M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.
[11] R. C.Merkle, "Protocols for public key cryptosystems," in Proc.of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.
[12] Akhil Behl, Emerging Security Challenges in Cloud Computing . Congress on Information and Communication Technologies (WICT), 2011 World.
[13] Mohammed A. AlZain, Ben Soh and Eric Pardede AlZain, M.A.; Soh, B.; Pardede, E. A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.
[14] Kan Yang, and Xiaohua jia (2013) An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing.
[15] Irfan Gul, Atiq ur Rehman, M.Hasan Islam, Cloud Computing Security Auditing.