A Survey on Various Techniques of Data Storage on Cloud using Third Party Auditor

Sankalp Gupta
Mtech (CSE)
Truba College of Engineering, Indore

Garima Joshi
ME(CSE)
Institute of Engineering & Technology, Indore

Pragya Shukla, Ph.D
Professor
Institute of Engineering & Technology, Indore

Praveen K.Guatam, Ph.D
Professor,
Truba college Of Engineering,Indore

ABSTRACT
In present scenario cloud computing emerges as one of the most powerful computing technology to provide dynamic service on demand on very large scale over the internet. Cloud computing offers various features like scalability, pay on use, using these features giants companies use cloud to store their data, In cloud computing data stores on cloud at remote location and cloud user hopes that his/her data is secured at cloud, but many times his/her data is altered, deleted or modified. So that cloud user to check integrity, confidentiality and security of data in a span of time, but cloud user and organization not able to put an eye on cloud provider all the time so they resort a TPA (Third Party Auditor) to work on behalf of cloud user. In this paper we discuss various Third Party Auditing schemes which ensure data integrity and privacy with their advantages and disadvantages,

Keywords
TPA, cloud, privacy, data, storage.

1. INTRODUCTION
Cloud computing provides novel methods of delivering computing resources and data storage where client/user accomplish their application at remote server with boundless storage space capacity and enjoying features of cloud computing like scalability, availability, elasticity, on demand service and pay per use. By data outsourcing users ca n be relived and feel more comfort from the burden of local data storage and maintenance, but due to remote data storage cloud user have no possession to check data integrity and privacy.Due to cost effective functioning of cloud giant business companies and organization adopting the cloud paradigm, because of cost effectiveness companies and organization saves lot of money on developing infrastructure for data storage and also free to maintain it. However migrating data over cloud is still serious apprehension for the organizations, because they worried about data security, integrity, confidentiality and their privacy. Despite cost effective environment and its excellent features of cloud it is still serious issue regarding privacy preservation of data at cloud storage [1].

In order to devise privacy preservation and secure cloud storage on off premises many researches design their techniques. In this paper we discuss various Third Party Auditing (TPA) techniques which use for auditing store data at cloud server.

2. TPA AND CLOUD
2.1 Introduction: TPA (Third Party Auditor)
For understanding off premises Third Party Auditing (TPA) techniques it is necessary to understand the working of TPA. Third Party Auditor (TPA) is a system or person who has expertise proficiency and capabilities that assess cloud storage security and integrity on behalf of cloud user or its request [2]. Before TPA came into existence cloud user relay on cloud server for data storage privacy and integrity, but now cloud user depends upon TPA for ensuring the storage security, integrity as well as integrity [2]. Schematic diagram of Third party auditor shown in figure 1.

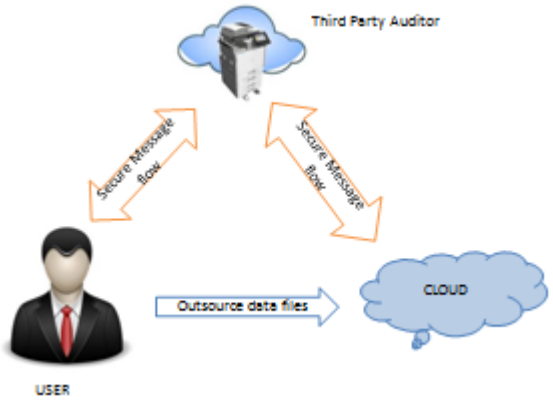

Figure -1 Third Party Auditor (TPA)

TPA comes into existence due to the fact that cloud server hide data corruption caused by server hacks or Byzantine failure, also it might be possible that it delete or misuse cloud user data. So that it is necessary to maintain an auditing authority who audit or checks data periodically on the request of user [2].

2.2 Characteristics of TPA

1. TPA audit data in periodical span of time to evaluate security provides data integrity and computational accuracy.

2. TPA verified the integrity of dynamic data stored in cloud on behalf of cloud user.

3. TPA should not required local copy of data for auditing.

4. TPA must be able to audit data without extra burden to cloud user.

3. RELATED WORK

Ateniese et.al (2007) proposed a framework named as Provable Data Possession (PDP).In this PDP protocol is used which verifies outsourced data storage site retains a file which consist n blocks. Using PDP, client first process the file named as F and add some data and expands it to a new file F'. After that client add some VMd (Verification metadata) named as M for file F' and stored it on cloud server. Generated M will also store on client local storage with metadata M. Client deleted metadata but before deletion client will execute a data possession to server by giving challenge to server to make sure that server successfully retained the file Yes or No response from server verifies the existence of file at cloud storage. In this PDP system client issue a challenge and a send request(R) to compute proof of possession P and sends to client to verify results of integrity [3].

Cong Wang et al.(2010) proposed an improved scheme of verify data integrity privacy preservation of data at cloud using concept of Third Party Auditor(TPA), since cloud user doesn't have expertise on auditing process so that client resort a TPA to audit data.TPA audit data on behalf of user and check data integrity, confidentiality and privacy of data at cloud storage. In this technique TPA enables to divide file (F) into n number of blocks and send to client. Suppose file is denoted by F and sequenced into N number of Block by M1, M2……Mi…..Mn using following function [4].

$$K^*(0,1) \xrightarrow{*} (0,1)$$

In this model cloud user generate public key, private key and VMd to server. TPA verifies each blocks of file and recovers it if it is malicious.

Venktesh. M. et al(2012) also provided a similar solution to Cong Wand et al TPA model, but they added RSA (Rivest, Shamir, Adelman) algorithm for security and integrity of data storage. In this proposed scheme client generates signature for each block of file with secret key using RSA and a Hashing Algorithm

$$Ti = h(Mi).gMi.rsk$$

$$Ø = \{Ti\}$$

where Ø is signature for all blocks.

They used Merklee hash Tree (MHT) is constructed by using all blocks, this tree is signed root by client with secret key

$$Sigrsk\ (H\ (R)=H\ (R\ )\ .rsk$$

In next step client sends file, hash and signed root (F, Ø, sigrsk (H (R)).during Audit process client through a challenge to server by selecting specific block. Server sends proof back to client. Clients verify it using MHT and secret key [5].

Sarfaj Nawaj Brohi et al(2013) proposed recent technique using Trusted Third Party Auditing (TTPA)which contains five concepts RBAC(Resilient Role Base Access Control),partial homomorphic cryptography, metadata generation and sound stenography, efficient Third Party Auditing(TPA) and backup and recovery process. In this scheme they encrypts data storage file using public key and secret code. Encrypted file sends to cloud server, data inside file will be homomarphically encrypted and stored. Whenever client needs, it is decrypted using private key. After storing file cloud server breaks file into number of blocks and generate Verification Metadata (VMd). Client admin downloads and store VMd at its local storage and request cloud server to encrypt file, public key, private key and VMd using sound stenography. In sound stenography sound-1 contains public key and VMd and sound-2 contains private key. Now TTPA download all these parameters to local storage and processed auditing process using fresh metadata and stored metadata, Based on results TTPA sends report to cloud server if data is malicious it request server to recover it [6].

4. SUMMARY

It is very hard to remember all the working of all techniques because each have its algorithms and flow of working like PDP uses meta data, Cong model used homomarphic encryption and venktesh model used RSA algorithm with TPA. So we summarize all the important concepts into tabular form so that it is easy to understand. In table we summarize working of improved techniques with their year of creation and their main concepts.

A summarize working of all techniques shown in table 1 below.

TABLE 1: TPA techniques and their concepts

Sno.	Researchers	Year	Concepts used
1.	Ateniese, G., R. Burns, R. Curtmola, J. Herring and L.Kissner	2007	Provable Data Possession (PDP) protocol used VMd(Verification Metadata)
2.	Wang, C., Q. Wang, K. Ren and W. Lou	2010	Third Party Auditing (TPA) using Homomarphic cryptography with random masking

3.	Venkatesh, M.,M .R. Sumalatha and C. SelvaKumar	2012	Third Party Auditing (TPA) using RSA (Rivest, Shamir, Adelman) algorithm
4.	Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat and Jamalul-lail Ab Manan	2013	Trusted Third Party Auditing (TTPA)which contains five concepts RBAC(Resilient Role Base Access Control),partial homomarphic cryptography, metadata generation and sound stenography, efficient Third Party Auditing(TPA) and backup and recovery process

5. CONCLUSION

In this research paper we discuss various techniques using concept of TPA. Each of technique has it own methodology to check integrity, privacy of data at cloud server with its pros and cons. Despite several improved technique there will be a need to more researched required in this security area of cloud computing. By doing this we will surely utilized cloud more ease with less burden of privacy preservation of data and its integrity

6. REFERENCES

[1] K.Meenakshi, Victo Sudha George 2014 " Cloud Server Storage Security Using TPA".

[2] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan. S 2011 "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud"

[3] Ateniese, G., R. Burns, R. Curtmola, J. Herring and L.Kissner *et al*., 2007. " Provable data possession at untrusted stores."

[4] Wang, C., Q. Wang, K. Ren and W. Lou, 2010."Privacy-preserving public auditing for data storage security in cloud computing."

[5] Venkatesh, M., M.R. Sumalatha and C. Selva Kumar, 2012. "Improving public auditability, data possession in data storage security for cloud computing."

[6]Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat and Jamalul-lail Ab Manan 2013 "Design and implementation of a privacy preserved off-premises cloud storage"