REVIEW OF VARIOUS AUDITING TECHNIQUES FOR PRIVACY PRESERVING IN PUBLIC CLOUD

[1]Nivedita Roy Gupta, [2]Prof. Umesh Kumar Lilhore

[1]M.Tech Research Scholar, [2]Associate Professor and PG Coordinator
Department of Computer Science& Engineering, NIIST Bhopal (M.P), India

***ABSTRACT*- Cloud computing is a fast growing and widely used technique. It serves computing resources to cloud user on "Pay and Use" basis. Due to high availability of computing resource, attract cloud user to utilize its services. A cloud user stores their various private data and files over cloud server. A Cloud user can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is data security.TPA maintains the availability and integrity of user data over cloud server. Many researchers have proposed their work or new algorithms to achieve security or to resolve this security problem. In this review paper we are presenting analysis and study of various privacy preserving methods for cloud computing.**

***Keywords*-Cloud computing, TPA, Cloud Security, Privacy preserving**

1. INTRODUCTION

Cloud Computing is an on-demand service over a network servers which are hosted on Internet to process, store and organize the data, rather than a local server or personal computer. The Cloud services and applications run on distributed network which provides a virtual resource for end user. These resources could be accessed by standard Internet and networking protocols [7]. Data integrity verification is one of the massive responsibilities with cloud data, because the probability of involvement in malicious activity of a cloud user and cloud provider is very high. There are many way to address this problem. User can use encryption and decryption process. However, it requires huge computing time and functional overheads. Applying data auditing may be the other way to address this problem.

Even if cloud provides such amazing services to its clients, there are some problems related to cloud such assecurity of data stored in cloud and integrity of data. The data security can be guaranteed using encryption techniquebefore sending data to cloud server and integrity of data can be guaranteed by signing data blocks using userssignature such that, except user no one can be able to generate similar signature. Even with this provision there ispossibility of leakage of data, as the integrity of data is verified by third party auditor thus the data needs to becopied from cloud server to third party auditor and problem starts [11]. As third party auditor can initiate brute-forceattack on saved copy of data without client knowledge. Often users may want to hide their identity whilepublic auditing. This increases complexity of auditing process.

2. CLOUD COMPUTING

The term cloud computing is referred as "The Cloud" which used as a "Metaphor" for the "internet" so cloud computing is a "type of internet based computing". It is a new and an innovative idea of 21st Century for IT industries. The purpose of the cloud computing is dynamically deliver the computing resources and capabilities as a services over the web. It is a new technology of computing in which dynamically scalable and often virtualized resources are provide as a service over the internet.

Cloud computing involved different hosted services over the internet which are IaaS (Infrastructure-as-a-service), PaaS (Platform-as-a-service), and SaaS (Software-as-a-service).IaaS service provide the infrastructure like memory, space, storage etc to users [1,4]. Saas service provides different application rather installing to its own system. PaaS service provides cloud application to developer and responsible for virtualization of resources and makes it as a single layer.

2.1 Types of Cloud-

Cloud deployment models are-

1) **Public cloud-** A public cloud is one standard of cloud computing, in which a cloud service provider provide a virtual environment, make a pool shared resources, such as applications and storage, offered to the general public over the web. Public cloud services are offered to users as pay-per-usage.
2) **Private cloud-** Organizations choose to build their private cloud as to keep the strategic, operation and other reasons to themselves and they feel more secure to do it.
3) **Hybrid model-**It consists of multiple service providers. It provides the services of both public and private cloud. It is used by organization when they need both private and public clouds both.

3.TPA AUDITING &ISSUES IN DATA PRIVACY

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. 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.Figure 3.1 shows working of TPA. A guaranteed security service will enhance the business performance of the cloud service provider.

Security is an essential service to be provided to the clients, a cloud service provider should assure. Secure cloud is a reliable source of information. Protecting the cloud is a very important task for security professionals who are in charge of the cloud. Cloud can be protected by protecting the data, making sure data is available for the customers, delivering high performance for the customers, using Intrusion Detection System on cloud and to monitor any malicious activities.

For the safety purpose, the provider's must provide a support system for the client's so that every client must be able to recover their own data loss in the cloud environment. Therefore, the encryption technique must be adopted in cloud by the provider's to their client's for integrity and authentication of data. When it comes to Security, cloud has lot of difficulties. The provider's must make sure that the client does not face any problem such as data loss or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user and there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud.

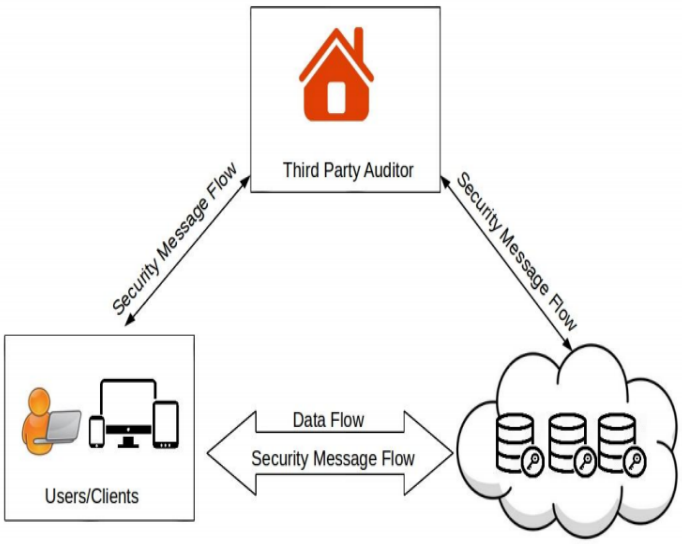

Figure 3.1 TPA Auditing

3.1 Characteristics of TPA –

TPA has following characteristics

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.

3.2 Challenges in Cloud computing-

Cloud computing have following issues-

a) Data protection- To be considered protected, data from one customer must be properly segregated from that of another; it must be stored securely when "at rest" and it must be able to move securely from one location to another. Cloud providers have systems in place to prevent data leaks or access by third parties. Proper separation of duties should ensure that auditing or monitoring cannot be defeated, even by privileged users at the cloud provider.

b) Authentication- The authentication of the respondent device or devices like IP spoofing, RIP attacks, ARP poisoning (spoofing), and DNS poisoning are all too common on the Internet. TCP/IP has some "unfixable flaws" such as "trusted machine" status of machines that have been in contact with each other, and tacit assumption that routing tables on routers will not be maliciously altered. One way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged.

c) Data Verification- Things like tampering, loss and theft, while on a local machine, while in transit, while at rest at the unknown third-party device, or devices, and during remote back-ups. Resource isolation ensures security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache.

d) Infected Application- Vendor should have the complete access to the server for monitoring and maintenance, thus preventing any malicious user from uploading any infected application onto the cloud which will severely affect the customer. Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures (application-level firewalls) be in place in the production environment

e) Availability- Cloud providers assure customers that they will have regular and predictable access to their data and applications.

4. RELATED WORK IN DATA AUDITING& CLOUD SECURITY

C. Wang et al.[5], used a scheme based on a homomorphic authenticator which is uniquely integrated with random masking technique for preserving privacy in auditing. Ring Signature Basically ring signature is a technique to hide details of signer of block from auditor, such that one can check integrity of data by computing signatures on block,

but he has no way to detect who is real signer of the data block [2].

In this technique, user puts all the signature of group members with its own signature, thus whenever third party auditor sees signature on block he finds all the signature of group members. To make things work in paper [6] an approach was used in which each user signs blocks with global private key which is assumed to be distributed to each group member and kept secretly by group members. If one user from the group is leaving the group or compromised, then new global private key is generated and shared among the rest of the group members. This introduces large overhead on users in terms of key distribution and key management. [6].

Trusted Proxy [4] another way to hide identity privacy is by employing trusted proxy who manages all the groups and their file uploading, downloading operations. Users uploads there data to proxy server which stores user signatures and signs the data block with its own signature, thus cloud server and third party auditor only sees signature of trusted proxy server enabling identity privacy. But the limitation of this approach is that it; it's a single point failure mechanism in terms of fault tolerance and public auditing. Utilizing group signature is also an alternative way for identity privacy but it does not provide public auditing mechanism [7].

Wang et al. [4] is able to preserve users' data confidentiality from a public verifier by employing random masking. There extended mechanism supports batch auditing using aggregate signatures to operate multiple auditing tasks from different users. [3].

Threat Models Two types of threats are related to the integrity of shared data, first is adversary may try to corrupt the integrity of shared data and second one is CSP may intentionally or un-intentionally corrupt (or even remove) data from its storage. This may happen due to hardware failures or because of human errors. In such situation, CSP may inform users about such damage to save their reputation [1][8]. Threat model related to privacy focuses on the third party auditor who is chosen for verifying the correctness of stored data integrity. The third party auditor may try to reveal the identity of the signer on each block to gain some information about data or identity of signer of block [1][8].

Homomorphic Authenticators Homomorphic authenticators [12](also called homomorphic verifiable tags) are basic tools to construct public auditing mechanisms. The unforgeability, a homomorphic authenticable signature scheme, which denotes a homomorphic authenticator based on signatures, should also satisfy the following properties [8]. Block less verifiability It allows a verifier to audit the correctness of data stored in the cloud server with a special block, which is a linear combination of all the blocks in data. If the integrity of the combined block is correct, then the verifier believes that the integrity of the entire data is correct. In this way, the verifier does not need to download all the blocks to check the integrity of data [1] [8]. Non-malleability It indicates that an adversary cannot generate valid signatures on arbitrary blocks by linearly combining existing signatures [8].

Batch Auditing It also supports batch auditing through which efficiency is improved. It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost. Through this scheme, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will be faster [8][9].

Data Dynamics It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. Paper [3] proposed scheme which support simultaneous public audit ability and data dynamics.

It uses Merkle Hash Tree (MHT) which works only on encrypted data. It uses MHT for block tag authentication. Paper [2] proposed Virtual machines which uses RSA algorithm, for client data/file encryption and decryptions. It also uses SHA 512 algorithm which makes message digest and check the data integrity.

The Digital signature [9] is used as an identity measure for client or data owner. It solves the problem of integrity, unauthorized access, privacy and consistency. Dhiyanesh [12] proposed Mac based and signature based schemes for realizing data audit ability and during auditing phase data owner provides a secret key to cloud server and ask for a MAC key for verification.

Paper [10] proposed privacy preserving Third party auditing without data encryption. It uses a linear combination of sampled block in the server's response is masked with randomly generated by a pseudo random function (PRF). Curtmola et al. [12] aim to ensure data possession of multiple replicas across the distributed storage system. They extend the PDP scheme in to cover multiple replicas without encoding each replica separately, providing guarantees that multiple copies of data are actually maintained. In [6], Bowers et al. utilize a two-layer erasure-correcting code structure on the remotely archived data and extend their POR model to distributed scenario with high-data availability assurance.

Proof of Ownership (POW) The POW protocol allows user to efficiently prove to a cloud server about his ownership, rather than short information about the file such as a hash value. This is somewhat similar to proofs of retrievability (POR) and proofs of data possession (PDPs) with a role reversal here client is the proover is cloud server. Pietro et.al [5] proposed three correlative protocols to achieve an efficient POW. The main idea of their protocols is to challenge random K bits of file F. The probability that a malicious user is able to output the correct value of K bits of the file where each bit is selected at a random position is negligible in security parameter k, but their scheme cannot be adopted for encrypted files.

Proof of Retrievability (POR)A proof of retrievability (POR) is a compact proof by a file system (prover) to a client (verifier) that a target files F is intact, in the sense that

the client can fully recover it. As PORs incur lower communication complexity than transmission of F itself, they are an attractive building block for high-assurance remote storage systems. A POR is a protocol in which a server/archive proves to a client that a target file integrity is valid, and thus client can recover their files whenever needed. In traditional POR, client needs to download file F and check the digital signature of that file to guarantee integrity [17]. The client can pre-process the file before uploading and insert some secret in that file, such that it can be used for checking consistency of file in PORs / PDPs technique

5. CONCLUSIONS AND FUTURE WORK

In this paper we have analyze and review various different security issues briefly. In both larger and smaller scale organizations they are using cloud computing environment because of large advantage of cloud computing. The cloud computing has different security issues in threats in user view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. The bond between service providers and users is necessary for providing better cloud security. In this paper we analyse the security issues, threats and challenges in wide acceptance of cloud computing, because there may be loss of data and privacy. Researchers Scholars and IT security professionals must press forward towards practical achievements in security and privacy to users. Our study identifies top security concerns of cloud computing, these concerns are security risks, techniques, problems, challenges and security issues of cloud computing and its methods.

In future work we will propose an improved data security and auditing scheme for cloud server (Private and Public cloud). Proposed method and existing method both will be implemented and various comparison parameters such as encryption time, TPA auditing time and avalanche effect will be calculated.

REFERENCES

[1] Rajat Saxena∗ and Somnath Dey," Cloud Audit: A Data Integrity Verification Approach for CloudComputing, Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016), Science Direct 2016, PP 142-152

[2] Swapnali More, Sangita Chaudhari," Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization 2016, ScienceDirect, PP 69-77

[3] Ankita R. Makode, V. B . Bhagat, :" Privacy Preserving For Secure Cloud Storage", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169,Volume, 4 Issue, 4, PP 475-479

[4] F. Seb´ e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´ e, Y. Deswarte and J.-J. Quisquater, Efficient Remote Data Possession Checking in CriticalInformation Infrastructures, IEEE Trans. Knowl. Data Eng., vol. 20(8), pp. 1034–1038, (2008).

[5] C. C. Erway, A. K¨ upc¸¨ u, C. Papamanthou and R. Tamassia, Dynamic Provable Data Possession, In ACM Conference on Computer andCommunications Security, pp. 213–222, (2009).

[6] L. Chen, Using Algebraic Signatures to Check Data Possession in Cloud Storage, Future Generation Comp. Syst., vol. 29 (7) pp. 1709–1715,(2013).

[7] A. Juels and B. S. K. Jr., Pors: Proofs of Retrievability for Large Files, In ACM Conference on Computer and Communications Security,pp. 584–597, (2007).

[8] H. Shacham and B. Waters, Compact Proofs of Retrievability, IACR Cryptology ePrint Archive 2008, vol. 73, (2008).

[9] Y. Dodis, S. P. Vadhan and D. Wichs, Proofs of Retrievability via Hardness Amplification, In TCC, pp. 109–127, (2009).

[10] K. D. Bowers, A. Juels and A. Oprea, Proofs of Retrievability: Theory and Implementation, In Proceedings of the 2009 ACM Workshop onCloud Computing security, ACM, pp. 43–54, (2009).

[11] A. Juels, K. D. Bowers and A. Oprea, Hail: A High-Availability and Integrity Layer for Cloud Storage, In ACM Conference on Computerand Communications Security, pp. 187–198, (2009).

[12] C. Wang, Q. Wang, K. Ren and W. Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, In INFOCOM,pp. 525–533, (2010).

[13] Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,In Computer Security–ESORICS 2009, Springer, pp. 355–370, (2009).