Volume 7, Issue 1, January 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey of Auditing Techniques for Privacy Preserving and Ensure Data Correctness in the Cloud

Dr. S Durga Bhavani
Professor & Director of
School of Information Technology,
JNTU-Hyderabad, India

Gudlanarva Sudhakar
Lecturer of
School of Information Technology,
JNTU-Hyderabad, India

Mohammad Almechal
Student of M.Tech
School of Information Technology,
JNTU-Hyderabad, India

DOI: 10.23956/ijarcsse/V7I1/0160

Abstract— These days Cloud Computing world figuring is one of the greatest development which utilizes progressed computational power and it enhances data/information sharing and data/information storage capacities. In other words Cloud figuring in its different structures permits clients to store their data at remote area and reduce the load on the clients systems. One of the most trouble in clouds computing was issues of information respectability, information protection and information access by unapproved clients. There is a great deal of research being made to spot out the issues with these cloud specialist organizations and cloud security when all is said in done. This paper will show the diverse issues related to protection while putting away the user's information on external cloud services providers or we can say Third party cloud services providers,which is named as cloud services. Cloud computing alludes to the key framework for a forthcoming model of services arrangement that has the advantage of dropping expense by sharing processing and capacity of storage assets.

Keywords— Cloud computing, ring signatures, Shared Data, public auditing, public verifier, identity privacy.

I. INTRODUCTION

A) Cloud Computing And data correctness (Integrity) in cloud

Cloud computing is Internet based computing which made revolution in the world recently. It is the greatest development which utilize progressed computational power and enhances data sharing and data storage power. Cloud is a huge group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing assets, on-request network access and provisioned by the cloud infrastructure services [1]. One of the benefits of cloud is to reduce cost and founds in other ward we can say cheaper than traditional computing. The prime bother issue in cloud is security. The Cloud computing security contains to an arrangement of strategies, innovation and controls sent to ensure information/data, application and the related framework of cloud computing.

Information correctness (Integrity) in cloud It is a main consideration that effects on the execution of the cloud. Data honesty (Integrity) contains conventions for composing of the information in a dependable way to the tireless information stockpiles which can be recovered in a similar arrangement with no progressions later. Keeping up uprightness of shared information is very troublesome undertaking.

B) Data Auditing in Cloud

On cloud we can ready to store information/data as a gathering family and share it or adjust it inside same family group. In cloud information/data stockpiling contains two substances as cloud client (aggregate individuals) and cloud specialist/cloud server.

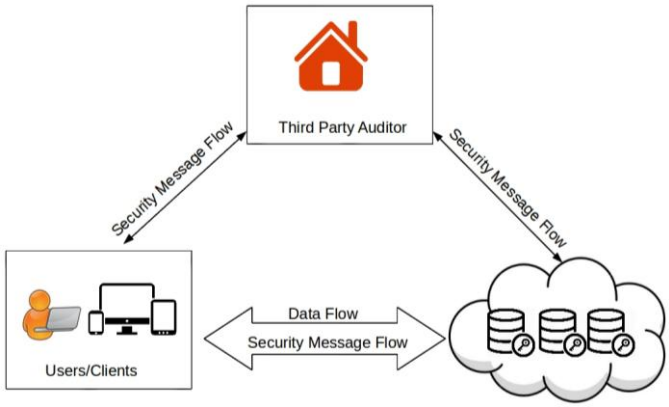

Figure: Public Auditing for Shared Data in the Cloud

Cloud client the one who stores extensive measure of information/data on cloud server which is overseen by the cloud services provider. Clients can exchange their data/information on cloud and share it inside the same group. A cloud services organization will give administrations to cloud client. The main issue in cloud information/data stockpiling is to obtain rightness and trustworthiness of information/data put away on the cloud. Cloud Service Provider (CSP) needs to give some type of system through which client will get the affirmation that cloud information is secure or is put away as it may be. No information misfortune or adjustment is finished by unauthenticated part. To accomplish security information inspecting idea is come into picture. This can be done in two ways as :

1) With trusted third party in light of who make the verification.
2) without trusted third party

II. LITERATURE REVIEW OF MECHANISMS USED FOR AUDITING

A) Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, Boyang Wang, Baochun Li, and Hui Li[2]

To provide integrity and protection of data in the cloud by introducing a third party auditor (TPA), who provide its auditing service with more powerful computation and communication abilities than regular users. In Oruta, they utilize ring signatures, to construct homomorphic authenticators , so that the third party auditor is able to verify the integrity of shared information/data for a gathering of clients without recovering the whole shared data/information. while the identification of the signer on each block in shared data is kept private from the TPA. In addition, Oruta extend thier mechanism to support batch auditing, which can audit multiple shared data in the same time of each auditing task. Meanwhile, Oruta continues to use random masking to support data protection in the same time of auditing process, and leverage index hash tables to support fully dynamic operations on shared data. A dynamic operation can be an insert, delete or update operations on any block in shared data/information.

Oruta properties:

1) Public Auditing: The third party auditor is able to publicly verify the integrity of shared data for a group of users without retrieving the whole data/information.
2) Unforgeability: Only a client in the group can generate substantial check data on shared information/data.
3) Correctness: The outsider evaluator(TPA) can accurately distinguish whether there whether there is any damage block in shared data.
4) Privacy Identity :The TPA can't recognize the signer on each block in shared data while auditing process.

Oruta algorithms: KeyGen, SigGen, Modify, ProofGen and ProofVerify.

1) KeyGen, users generate their own public/private key pairs.
2) SigGen, a user (either the original user or a group user) is able to compute ring signatures on each block in shared data/information. Every client in the group is able to do an insert, delete or update operations on a block, and compute the new ring signature on this new block in Modify.
3) ProofGen is operated by the TPA and the cloud server together to generate a proof of possession of shared data.
4) ProofVerify, TPA check the proof after virfication of this proof will send an auditing reports to the client. security properties of Oruta, including its integrity,correctness, protection and identity privacy.

Oruta, the first privacy-preserving public auditing mechanism for shared data/information in the cloud, utilize ring signatures to develop homomorphic authenticators, so the TPA is able to check or observing the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy.

B) AFS: Privacy-Preserving Public Auditing With Data Freshness in the Cloud P. Maheswari, B. Sindhumathi[3].

AFS Authenticated File System is additionally a protection saving component which is the totally lock like Oruta except data freshness. It works on authenticated file system. It verifies the freshness of the data while performing the file operations. The freshness of the blocks can be confirmed by the Mac block and the freshness of the block version. AFS guarantee data freshness with this layers :

- Lower layer stores a MAC for each block that enables random access. A version number additionally is connected with the MAC block which is increased by each new data block.

- The upper layer consists of Markle tree. Block versions are stored by its leaves while hashes of children are stored by insider hubs. AFS based on identity privacy also on ring signature. Be that as it may, it can't detect the client status on the mischief cases.

C) Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud Boyang Wang , Hui Li and Baochun Li [4].

Knox also based on homomorphic MAC which decreases the space to store the checked data block, with group signature. Homomorphic MAC used in this technique uses pseudo-random function. Knox incorporates six algorithms: KeyGen, Join, Sign, ProofGen, ProofVerify and Open.

1) KeyGen, the original user of shared data generates a group public key and a group manager private key.
2) Join, the original user, who goes as the group manager, can issue private keys to users.
3) Sign: A client (either the original user or a group user) is able to sign blocks using private key and the group public key.
4) ProofGen, the cloud create a proof of possession of shared data to the TPA.
5) ProofVerify is operated by the TPA to verify the integrity of the proof.

6) Open :The original client can reveal the identity of the signer on each data block.

Knox is work on the a group of users which have a group manager which can revoke the user on his misbehavior. security of Knox, including its correctness, unforgeability, identity privacy and traceability.

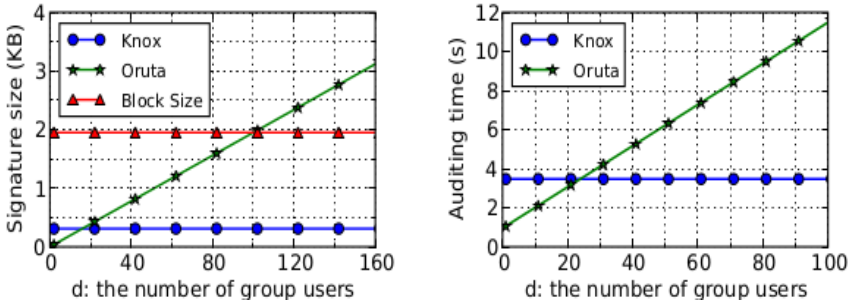

Figure: Impact of group size on signature size and auditing time (Form same reference paper)[4]

In this figures above they show the impact of group size d on both signature size (KB) and auditing time (s).one of the pros of Knox is not affected by the number of users in the group.

D) Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Member, and Wenjing Lou.[5]

The another privacy preserving technique is introduced in this mechanism. It deal with the homomorphic authenticator with random masking. This scheme includes the linear block of the data that has been sampled using the random masking which is generated through pseudo random function in the server response.
This mechanism consists of two phases, Setup and Audit:

- Setup: The user initializes the public and secret parameters of the framework by extracting KeyGen, and pre-processes the data files by using SigGen to creat the verification metadata. The user then save the data file and the verification metadata at the cloud server, and deletes the local copy. As part of preparing to the process, the user may change the data file F by expanding it or including additional data to be save in the server.
- Audit: The TPA provide an audit message or challenge to the cloud server to ensure that the cloud server has retained the data file properlyin the auditing time. The cloud server will extract a response message from same function of the stored files and its verification metadata by extracting GenProof. Then the TPA verifies the response by VerifyProof.

In this mechanism to achieve privacy-preserving public auditing, they propose to uniquely integrate the random masking with homomorphic linear authenticator method. In this protocol, the linear combination of blocks after sampling in the server response is covered with randomness generated the server. With random masking, the TPA no longer has all the necessary information to create or develop a correct group of linear equations and hence can't determine the user's data files content, regardless of what number linear combinations of the similar set of file blocks can be gathered. Oppositely, the integrity validation of the blocks authenticators pairs still can be achevied. Properties of this Protocol. public auditing-ability, There is no secret keying material or states for the TPA to keep up amongst audits, and the auditing protocol does not represent any potential on-line burden on clients or users. Storage correctness thus follows from that of the underlying protocol. Support for Batch Auditing,Support for Data Dynamics. This mechanism can be extended into multiple auditing tasks in a batch manner.

E) Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds Huaixi Wang,Yan Zhu, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau.[6]

They proposed the fragment structure to reduce the storage of signatures in their public auditing mechanism and to provide dynamic operations on data they also used index hash tables. Actually its same as Wang et al. [4] mechanism but They develop their mechanism to have capability of batch auditing by using aggregate signatures to operate multi auditing tasks from multi users efficiently.

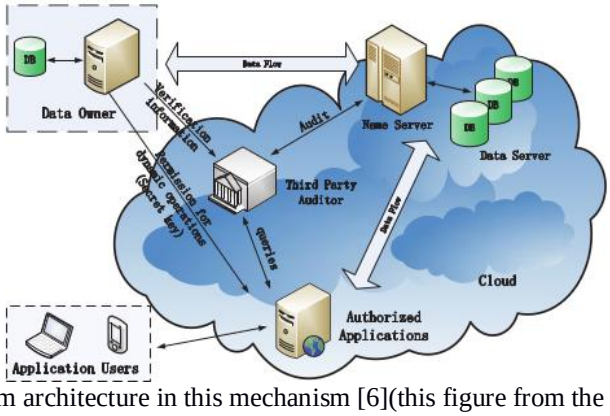

Figure: The audit system architecture in this mechanism [6](this figure from the same reference paper).

In this mechanism TPA must do this audit functions:

-TPA should be able to make regular checks on the integrity and availability of the delegated data at appropriate intervals;

-TPA must be able to organize, manage, and handle the outsource data rather than data owners, and support the dynamic data operations for an authorized applications.

- TPA must be able to capture the evidences for arguments about the instability of data in terms of authentic records for all operations.

Three main processes in this mechanism:

1) Tag Generation: the client (data owner) uses the secret key sk to pre-process a file, which comprises of an accumulation of n blocks, create a group of public verification parameters (PVP) and index-hash table (IHT) already put away in TPA, transmits the file and some verification tags to CSP, and may delete its local copy.
2) Audit for Dynamic Operations: An authorized applications, who have the secret key sk of data owner, can manipulate the external data and update the related index hash table (IHT) stored in TPA. The privacy of sk and the checking algorithm verfiy that the storage server can't cheat the authorized applications and forge the valid audit records.
3) Periodic Sampling Audit: by utilizing an intuitive proof protocol of retrievability, TPA (or other applications) issues a "Random Sampling" challenge to audit the correctness and availability of external data in terms of the confirmed information stored in TPA.

Efficient method for periodic sampling audit to minimize the computation costs of third party auditors and storage service providers but has a small, constant amount of overhead, which minimizes computation and communication costs.

F) Preserving Privacy Policy- Preserving public auditing for data in the cloud by Krishna Kumar, Deepa P Sivan.[7]

In this scheme they use normal auditing mechanism but they involves data security in same task by using encryption data. In this paper also, they propose a homomorphic algorithm and third party auditing scheme to construct a secure data management mechanism with high privacy protection method. The main quality features in this method are: (1) prevention abuses attacks. (2) data security. (3) privacy protection. (4)Auditing details to the data owner .(5) word, index and content wise data searching is applicable.

G) Privacy-Preserving Public Auditing For Shared Data In The Cloud ,Swapnali Sakore, Rukmini Raut, Vaishali Shinde.[8]

In this mechanism they use Oruta as a privacy preserving public auditing mechanism. Also using ring signatures to construct homomorphic authenticators in Oruta. In addition, this mechanism used to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification.

Also here they said data is allocated into a small blocks and owner signed the block independently. During integrity checking the whole data is not retrieved instead of random combination of all the block done.

It lock same like Oruta but here they extended this mechanism and develop the effectiveness of verification for multi auditing tasks. One of the disadvantages of this mechanism , data owners may share the data under the policy over attributes from multiple authorities: difficulty to encrypt data.

H) Certificateless Public Auditing for Data Integrity in the Cloud, Boyang Wang, Baochun Li, Hui Li and Fenghua Li[9].

In this scheme, first design a homomorphic authenticate certificate less signature scheme with blockless verifiability,which traditional certificateless signature schemes do not support.

Then build the entire certificateless public auditing mechanism for verifying data integrity in an untrusted cloud based on our proposed certificateless signature scheme. As a result, This public auditing mechanism does not require a public verifier to manage certificates,which successfully eliminates the security risks introduced by PKI in previous works. Meanwhile, this public verifier is still able to efficiently audit the correctness of data in the cloud environment without retrieving the hole data blocks. To the best of our knowledge, this mechanism represents the first solution of certificateless public auditing on data integrity in the cloud.

III. CONCLUSION

We have shown the various privacy preserving techniques for public auditing From that,we can say Among all the mechanism, Oruta and AFS works on ring signature which is based on Privacy Identification. But both of them are unable to observe the identity of the client on the mischief cases. Knox is based on group signature, which is able to observe the identity of user on the mischief and can utilizing by using group manager's private key. This can be carried out by group manager only. All of above techniques uses the homomorphic authenticators with different schemes. Also we can figure out that is the mean threats for public auditing mechanisms are integrity and security threats. We can also conclude that, all the techniques not yet reach the batch auditing that can lead to multiple auditing tasks. They can be expanded further as far as the lacking behavior or also for adding up batch auditing into them. We have shown that techniques use different mechanisms and schemes to authenticate and to proof the integrity of the data blocks. Most of the techniques are protected from the attackers due to its unforgeability. Privacy preserving mechanisms are used where user's identity is highly secret. For the data freshness, Oruta, knox and the other mechanism do not contain data freshness while AFS has achieved that feature.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing".

[2] Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302,2012.

[3] AFS: Privacy-Preserving Public Auditing With Data Freshness in the Cloud P. Maheswari, B. Sindhumathi IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 56-63

[4] Boyang Wang , Baochun Li and Hui Li , "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS'12),pp. 507-525, June 2012.

[5] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Member, and Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security inCloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[6] Yan Zhu , Huaixi Wang , Zexing Hu , Gail-Joon Ahn , Hongxin Hu , Stephen S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.

[7] Preserving Privacy Policy- Preserving public auditing for data in the cloud, Krishna Kumar L , Deepa P Sivan , International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 || Volume 3 Issue 11 || November 2014 || PP.06-09.

[8] Privacy- Preserving public auditing for shared data in the cloud, SWAPNALI SAKORE, RUKMINI RAUT, VAISHALI SHINDE, International Journal of Advances In Computer Science and Cloud Computing, ISSN: 2321-4058 Volume-3, Issue-1, May-2015.

[9] Certificateless Public Auditing for Data Integrity in the Cloud Boyang Wang , Baochun Li, Hui Li and Fenghua Li, 2013 IEEE Conference on Communications and Network Security (CNS) ,10.1109/CNS.2013.6682701.

[10] Ridham Kapadiya and Jignesh Prajapati, Survey of Privacy Preserving Auditing Techniques for Shared Data in Cloud Computing ,International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 14, January 2015.

