ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 2, Issue 4, April 2015

Survey on Auditing Mechanism for Preserving Privacy in Cloud Computing

Harsha B. Patil

Department of CSE, Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal, North Maharashtra University, India

ABSTRACT: Cloud computing is an arising technology which provide various services through internet. User can remotely stored their data on the cloud. And enjoying on demand high quality cloud applications without the burden of local storage and maintenance. But the user do not fell protected because data is stored at cloud required security and integrity. The data integrity verification is done by Third party auditor (TPA),who check the integrity of data periodically on behalf of the client. Many mechanism allow data owner as well as public verifier to perform integrity checking without retrieving entire data from cloud, which is called as public auditing.TPA verify the integrity of shared data in several auditing tasks would be very inefficient so that batch auditing mechanism is used. And also support for dynamic operations on data blocks i.e. data update, delete and append.

KEYWORDS:Cloud Computing, Privacy preserving, Security, Integrity, Data storage, TPA**.**

I.INTRODUCTION

With cloud computing , cloud service providers offers users to access and to share resources cost. Cloud storage services share user's data with other users in group. data sharing is standard feature in most cloud storage offers Dropbox, iCloud and Google Drive.

In cloud storage , integrity of data , is related with exploration and infidelity because data stored in the cloud can easily be lost or corrupted due to human errors and hardware/software failures . The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then checking the correctness of signatures (e.g., RSA) or hash values (e.g., MD5)of the entire data is verify data integrity. .The main reason is the size of cloud data which is large . When data have been corrupted in the cloud to verify data integrity, downloading the entire cloud data that cost or even waste users amounts of computation and communication resources. There are two classes of basic scheme

MAC Based Solution:

It is used to authenticate the data.User upload data blocks and MAC to CS provide its secret key SK to TPA. The TPA will randomly retrieve data blocks and MAC uses secret key to check correctness of stored data on the cloud. There are problems occurs such as

1.Computation and Communication complexity.
2. For verification ,TPA requires knowledge of data blocks.
3.It have additional online burden to users because of limited use and stateful verification.
4.Having limits on data files to be audited as secret keys are fixed.
5.It supports dynamic data as well as static data.
6.After using all possible secret keys to recomputed MAC, the user has to download all the data & republish it on CS.
7.TPA need to maintain & update states for TPA and it is very difficult.

HLA Based Solution:

1.It supports efficient public auditing without retrieving data block. It is aggregated and required constant bandwidth.
2.It is possible to compute an aggregate HLA which authenticates a linear combination of the individual data blocks.Pseudo random function (PRF) is randomly generates using a linear combination of sampled block in the server's response is masked.

Homomorphicauthenticators are basic tools to construct data auditing mechanisms. A homomorphic authenticable signature scheme should satisfy the properties such as blockless verification and non-malleability.

Non-malleability is that an attacker cannot generate valid signatures on invalid blocks by linearly combining existing signatures.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 2, Issue 4, April 2015

Blockless verification: Blockless verification allows a verifier to check the correctness of data stored in the cloud server.it is a linear combination of all the blocks in data. Verifier believes that all blocks in data are correct if the combined block is correct means that to check the integrity of data, verifier does not need to download all the blocks.

Public auditing is to allow a public verifier as well as a data owner itself without downloading the entire data to efficiently perform integrity checking from the cloud. In these mechanisms, data is divided into many small blocks, where the owner is independently sign each block; and during integrity checking, a random combination of all the blocks instead of the whole data is retrieved.A public verifier could be a data user,who would like to utilize the owner's data through cloud.A public verifier work as a third-party auditor (TPA) to provide expert integrity checking services. Existing public auditing mechanisms is used to verify shared data integrity .But there is a privacy issue introduced in shared data with using existing mechanisms is the leakage of identity privacy to public verifiers. It is difficulty to preserve identity privacy from public verifiers during public auditing, during protecting confidential information.

To solve this kind of privacy issue on shared data .ORUTA is proposed.Oruta is a privacy preserving public auditing mechanism .In oruta ring signature is used to construct homomorphic authenticators because of that public verifier is able to verify the integrity of shared data without retrieving the entire data during the identity of the signer on each block in shared data is kept private from the public verifier.oruta also support for batch auditing.It perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks.Oruta stands for "One Ring to Rule Them All".

II.RELATED WORKS

Provable Data Possession at Untrusted Stores(2007)

G. Ateniese,R.Burns,R.Urtmola,J.Herring,L.Kissner,Z.Peterson and D.Song introducing provable data possession (PDP)that allows client to stored data at an untrusted server to verify that server possesses the original data without retrieving it.PDP generates probabilistic proofs of possession by sampling random sets of blocks from the server.It reduces I/O costs. The client have a constant amount of metadata to verify the proof .The challenge/response protocol minimizes network communication.It transmits a small and constant amount of data.PDP supports to public databases such as digital libraries,astrobnomy/medical/legal repositories,archives etc. .PDP schemes have drawback is that it works only for static databases[17].

PORs: Proofs of Retrievability for Large Files(2007)

A.Juels and B.S.Kaliski describes POR which allows a server to convince a client that can be retrieve a file that was previously stored at the sever.POR scheme uses disguised blocks (called sentinels) hidden among regular file blocks in order to detect data modification by the server.The goal of POR is to accomplish these checks without users having to download the files themselves.POR provides quality of service guarantees means a file is retievable within a certain time bound.

POR protocol encrypts F and randomly embeds a set of randomly valued check blocks called sentinels .The use of encryption renders the sentinels indistinguishable from other file blocks. The verifier challenges the prover by specifying the positions of a collection of sentinels and asking the prover to return the associated sentinel values.Ifprover has modified or deleted a substantial portion of F,then with high probability it will also have suppressed a number of sentinels[2].

Compact Proofs of Retrievability(2008)

HovavShacham and Brent Waters focuses on a proof of retrivabilitysystem,in that a data storage center convinces verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient ad provably secure means that it should be possible to extract the client's data from any prover that passes a verification check.there are two scheme. First scheme is built from BLS signatures and secure in the random oracle model. It has the shortest query and response of any proof of retrievability with public verifiability.Second scheme ,which builds on pseudorandom functions(PRFs)and is secure in the standard model.It has shortest response of any proof of retrievability scheme with private verifiability.Both scheme depends on homomorphic properties to aggregate a proof into one small authenticator value[3].

Scalable and Efficient Provable Data Possession(2008)

G.Ateniese,R.D.Pietro,L.V.Mancini and G.Tsudik worked on an efficient PDP mechanism based on symmetric keys.It support update and delete operations on data but insert operations are not available in it.It exploits symmetric keys to

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 2, Issue 4, April 2015

verify the integrity of data ,it is not public verifiable.It having drawback ,it provides a user with a limited number of verification requests[4].

Short Signatures from the weilPairing(2001)
D. Boneh, B. Lynn, and H. Shacham worked on Short signature scheme,which is based on Computational Differ-hellman assumption on certain elliptic and hyper-elliptic curves.For similar level of security the signature length is half the size of a DSA signature.Short signature scheme is designed because signature are typed in by a human or signature are sent over a low bandwidth channel[5].

Dynamic Provable Data Possession(2009)
Dynamic provable data possession (DPDP), which extends the PDP model to support provable updates on stored data developed by C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia. Consider a file F consisting of n blocks, it define an update as inserting a new block or modifying an existing block or deleting any block.An update operation describes the most general form of modifications a client may wish to perform on file.
DPDP solution is based on variant of authenticated dictionaries, where rank information used to organize dictionary entries. It supports efficient authenticated operations on files at block level such as authenticated insert and delete. Provable storage system enables efficient proofs of a whole file system, enabling verification at different users and same time not having to download the whole data[6].

Privacy Preserving public auditing for data storage security in cloud computing(2010)
C. Wang, Q. Wang, K. Ren, and W. Lou describes Privacy preserving public auditing system for data storage security in cloud computing ,where TPA can perform the storage auditing without demanding the local copy of data. Homomorphic authenticator and random masking technique are used to guarantee that TPA would learn any knowledge about the data content stored on the cloud server during the efficient auditing process. It not only eliminates the burden of cloud user fron auditing but also soften the user's fear of their outsourced data leakage.Consider TPA may concurrently handle multiple audit sessions from different users for their outsourced data file,it can extends privacy preserving public auditing protocol into multiuser setting ,where TPA can perform the multiple auditing tasks in a batch manner i.e. simultaneously[7].

Aggregate and Verifiably Encrypted Signatures from Bilinear Maps(2003)
D. Boneh, C. Gentry, B. Lynn, and H. Shacham introduces An aggregate signatures are useful for reducing the size of certificate chains by aggregating all signatures in the chain.It is useful for reducing message size in secure routing protocols such as SBGP.Aggregate signature provides verifiably encrypted signatures that signature enable the verifier to test that a given ciphertext C I the encryption of a signature on a given message Verifiably encrypted signatures are used in contract signing protocols. It is also used to extend the short signature scheme to give simple ring signatures[8].

Ensuring Data storage Security in cloud Computing(2009)
To ensure the correctness of user's data in cloud data storage,a effective and flexible distributed scheme with explicit dynamic data support is proposed by C. Wang, Q. Wang, K. Ren, and W. Lou. It including block update,delete and append.It rely on erasure correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.By utilizing the homomophic token with distributed verification of erasure coded data .During the storage correctness verification across distributed servers,it achieves the integration of storage correctness insurance and data error localization.It guarantees the simultaneous identification of the misbehaving servers[9].

Remote Data Checking for Network Coding based Distributed Storage Systems(2010)
B. Chen, R. Curtmola, G. Ateniese, and R. Burns evaluated Remote Data checking (RDC)is a technique by which clients can establish that data outsourced at untrusted servers remains intact over time.RDC is useful as prevention tool that it allow clients to periodically check if data has been damaged and it is used as repair tool when damage is detected Initially in the context of single server ,RDC was extended to verify data integrity in distributed storage systems that depend on replication and on erasure coding to store data redundanty at multiple servers. RDC-NC is a novel secure and efficient RDC scheme for network coding based distributed storage systems.It alleviates new attacks that stem from the underlying principle of network coding.it preserve in an adversarial setting the minimal communication overhead of the repair component achieved by network coding[10].

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 2, Issue 4, April 2015

LT Codes-based Secure and Reliable cloud storage service(2012)
N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou explores the problem of secure and reliable cloud storage with efficiency consideration of both data repair and data retrieval and design a LT codes-based cloud storage service(LTCS)..By utilizing the fast BeliefPropagation decoding algorithm, LTCS provides efficient data retrieval for data users and releases the data owner from the burden of being online by enabling public data integrity check and employing exact repair[11].

Proofs of Ownership in Remote Storage Systems(2011)
S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg identify attacks that exploit client side deduplication,allowing an attacker to gain access to arbitrary size files of other users based on a very small hash signatures of files.An attacker knows hash signature of a file can convince the storage service that it owns that file,hence the server lets the attacker download the entire file. To overcome such attacks,proofs of ownership(PoWs)is introduced ,which client efficiently prove to a server that the client holds a file,rather than short information about it[12].

Secure and Efficient Proof of storage with Deduplication (2012)
Q. Zheng and S. Xu introduces Proof of storage with deduplication or POSD, to fulfil data integrity and duplication simultaneously. POSD scheme is proven secure in the Random Oracle model based on the Computational Diffie-Hellman assumption[13].

Oblivious Outsourced Storage with Delegation (2011)
M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sionintroduces,Consider multiple clients want to share data on a server, while hiding all access patterns. Outsourcing private data to untrusted servers has an important challenge.so the solution for this problem is Oblivious RAM (ORAM) techniques. Data owners can delegate rights to external new clients enabling them to privately access portions of the outsourced data served by a curious server.ORAM allows for delegated read or write access while ensuring strong guarantees for the privacy of outsourced data. The server does not learn anything about client access patterns while client do not learn anything more than their delegated rights permit[14].

Efficient and Private Access to Outsourced Data(2011)
S. D. C. di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati exploited For data outsourcing, it presented an indexing technique that proves to be efficient while ensuring content access and pattern confidentiality. The shuffle index have advantages such as first is the underlying structure is B+ trees, which are used in relational DBMSs to support the efficient execution of queries. Second is the possibility for the use of multiple indexes, defined on distinct search keys, over the same collection of data[15].

Proofs of Retrievability via Hardness Amplification (2009)
YevgeniyDodis, SalilVandan Daniel Wichs develops PORs as an important tool for semi-trusted online archives In a POR,unlike a POK,there is no need to have knowledge of F to the prover or the verifier.Existing cryptographic techniques help users ensure the privacy and integrity of files they retrieve.The goal of a POR is to accomplish these checks without users having to download the files themselves.A POR can provide quality of service guarantees,i.e. it show that a file is retrievable within a cetain time bound[18].

Knox:Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud(2012)

Boyang Wang, Baochun Li and Hui Li introduces Knox is a privacy preserving mechanism for data stored in the cloud and shared among a large number of users in a group. In knox ,group signature is used to construct homomorphicauthenticators,so that a third party auditor (TPA)is able to verify the integrity of the shared data for users without retrieving the entire data .In it the identity of the signer on each block in shared data is kept private from TPA. Knox exploits homomorphic MACs to reduce the space used to store verification information[16].

Oruta : Privacy Preserving Public Auditing for Shared Data in the Cloud(2014)
B. Wang, B. Li, and H. Li describes Oruta exploits ring signature to compute verification metadata needed to audit the correctness of shared data. In this mechanism , the identity of the signer on each block in shared data is kept private from public verifier ,who are able to efficiently verify shared data integrity without retrieving the entire file. this mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one[1].

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 2, Issue 4, April 2015

III.CONCLUSION

The concept of cloud computing drastically improving day by day. TPA checks the integrity of data. Homomorphic linear authenticator and random masking guarantees that TPA does not learn any knowledge about data content stored on cloud sever during auditing process. Use of batch auditing ,computation cost is reduced.

REFERENCES

1. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2014.
2. A. Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007.
3. H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90107, 2008.
4. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm'08), 2008.
5. D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001.
6. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.
7. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
8. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003.
9. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.
10. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.
11. N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, 2012.
12. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of Ownership in Remote Storage Systems," in Proc. ACM Conference on Computer and Communications Security (CCS), 2011, pp. 491–500.
13. Q. Zheng and S. Xu, "Secure and Efficient Proof of Storage with Deduplication," in Proc. ACM Conference on Data and Application Security and Privacy (CODASPY), 2012.
14. M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, "Oblivious Outsourced Storage with Delegation," in Proc. Financial Cryptography and Data Security Conference (FC), 2011, pp. 127– 140.
15. S. D. C. di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati, "Efficient and Private Access to Outsourced Data,"WANG et al.: ORUTA: PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD 15 in Proc. IEEE International Conference on Distributed Computing Systems (ICDCS), 2011, pp. 710–719.
16. B. Wang, B. Li, and H. 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.
17. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.
18. Y. Dodis, S.P. Vadhan, and D. Wichs, "Proofs of Retrievability via Hardness Amplification," Proc. Theory of Cryptography Conf. Theory of Cryptography (TCC), pp. 109-127, 2009.