Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 347 – 352

Procedia Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

A REVIEW ON CLOUD DATA SECURITY AND ITS MITIGATION TECHNIQUES

Selvamani K[a], Jayanthi S [b]

[a]*Assistant Professor, Department of CSE, Anna University, Chennai*
[b]*Research Scholar, Department of CSE, Anna University, Chennai*

Abstract

Cloud providers offer several storage services for their users in efficient manner. Cloud users are allowed to store their data in cloud server using cloud storage and reduce the burden of storing and retrieving in local machine. The data can be shared by a user in a group and the facility shakes the integrity of the shared data due to access by many users as well as hardware and software for users. It is necessary to ensure the integrity of shared data before using that data for some process as well as the correctness of the cloud storage. Public auditing mechanism is employed to audit the correctness of the shared data. Both data owner and the Third Party Auditor (TPA) can audit shared data integrity without downloading the data from cloud server. This research paper attempts to point out various techniques to solve the privacy and security issues of the data in public auditing scheme in cloud environment.

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)

Keywords: Cloud computing; Data storage; Public Auditing; Security and Integrity

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.192

1 Introduction

In the era of Cloud Computing, there are several opportunities that enables data stored remotely to be temporarily cached on desktop computers, mobile phones or other internet devices. The software industries as well as individuals who store their data in the cloud are in flexible manner that has some benefits like avoidance of capital expenditure on personal maintenances, hardware, software, relief of online burden of data storage. In order to ensure the integrity of the data and to reduce the online burden it is important to enable public auditing service for cloud storage, so that user may resort to Third -Party Auditor (TPA) to audit the data. The TPA who has capabilities and expertise can periodically check the integrity of the data stored in cloud server. Enabling public auditing service will play an important role for data privacy and security for minimizing the risk for the data from hackers.

1.1 Security In Cloud Storage

Security and reliability are the two main challenges in cloud computing. Client's data in the cloud can be accessed by other clients. So there arise security issues on clients' data. To achieve security on cloud data there are so many techniques and algorithms are available. Some of these are:

Encryption- A technique which uses complex algorithm to hide the original information with the help of encryption key.

Authentication processes- which creates a user name and password to access the data.

Authorization practices – Provides authorization to clients, who can access data stored on cloud system.

However, clients are worried that data stored on a remote storage system is vulnerable. The hackers could also attempt to steal the data which are stored in the physical machines. A disgruntled employee could modify or destroy data using his authorized user name and password. Cloud storage companies invest a lot of money in security measures in order to limit the possibility of data theft or corruption.

1.2 Privacy and Security Issues in Cloud Storage

Privacy and Security threats may vary according to the type of cloud scenario. The following issues are addressed in cloud storage [1][2]:

- **The threats occur against the information assets residing in cloud computing environments.**
- **The type of attackers and their capability of attacking the cloud.**
- **Lack of training and expertise, unauthorized secondary usage.**
- **Addressing transborder data flow restrictions, Legal uncertainty**
- **Data Location , transfer and retention, Data security and disclosure of breaches**
- **Emerging cloud security risks.**

2. Literature Survey

Many works pertaining to cloud security has been proposed and implemented by many researchers in the past years. Some of the few important works has cited in this survey paper. Among them, Qian Wang et.al. [7] has proposed a model to solve the problem of integrity of data stored in the cloud. The TPA has allowed verifying dynamic data in cloud storage through auditing process and motivating public auditing system in the cloud. Proposed protocol support public auditing and block less verification. Data dynamics can be achieved by MHT construction for block tag authentication. Using aggregate signature the TPA can perform multiple auditing tasks simultaneously from different user's settings.

The authors Cong Wang et.al.[8] proposed a flexible distributed storage auditing mechanism to ensure data storage correctness in cloud. Homomorphic token and distributed erasure-coded data technique was utilized to check the integrity of stored data. It allows user to perform dynamic operation on outsourced data including block modification, deletion etc and support TPA to audit the data, so user can delegate auditing task to TPA and worry-free to use cloud storage services. Auditing result gives strong storage correctness and also simultaneously achieves data error localization that is identification of misbehaved server. This scheme helps low computational and communication cost to the user. The proposed scheme is efficient against data modification attack, server colluding attack, byzantine failure.

The authors Cong Wang et. al.[9] are the first to consider that, Secure cloud storage system supports privacy-preserving public auditing . User can resort TPA and verify integrity of stored data in cloud storage. It consists of four algorithms namely key generation, signature generation, generate proof, proof verify. MAC based solution gives additional burden to the user in terms of key management and HLA and does not support privacy preserving. Disadvantage of this scheme is auditing a specific file is limited and secret key must be of fixed priority. Public key based homomorphic linear authenticator and HLA with random masking technique was proposed. It consists two phases such as setup and audit phase. TPA can verify integrity of data without learning original content so that the identity of the user can be preserved.

The authors Boyang Wang et.al[10] has envisioned that data can be easily shared by group. While user is revoked from the group, the revoked user data block resigned by existing user. In this paper, a novel public auditing mechanism for the integrity of the shared data with efficient user revocation was proposed. Proxy re-signature technique was utilized with help of this method and the user can re-sign the revoked user block and need not to download data from server to verify the shared data integrity and also maintain the whole data integrity. Shamir secret sharing was extended into multi proxy model to reduce chance of misuse on resigning key. Further implementation focus on collusion resistant proxy re-signature. It has not support public auditing.

In the main scheme for ensuring sharing , by Xuefeng Liu et al.[11] presented Sharing data in Multi owner manner still preserving identity and data privacy due to frequent change of membership. In this paper the authors proposed a secure multi owner data sharing for dynamic groups and it was implemented. Group signature and dynamic broadcast encryption technique are used to share a data with other members in a group. User revocation can be easily achieved through revocation list without updating secret key of the remaining user and also provides

control access to the users. New granted user directly decrypt data file without contacting data owner. Encryption computation cost, storage overhead of the proposed scheme is independent of the revoked users.

From the author's Yan Zhu et.al[12] perspective, this work focused on a dynamic audit services and integrity verification of data in outsourced cloud storage. Audit service has been constructed based on random sampling, fragment structure, index hash table. The Proposed method is based on probabilistic query and periodic verification to improve the performance of auditing process. This method provides less storage for storing verification meta data and verifies the data integrity with low computation.

Ateniese et al.[13] are the first to consider in "Provable Data Possession" (PDP) model which ensures the possession of data files on untrusted storages [14]. This technique is used to permit a client to frequently, efficiently and securely verify the server who stores client potentially very large amount of data. That is the server might delete some part of the data or it might not store all data in cloud storage. PDP is a public key based technique which allows any verifier to query the server and POR verifies the integrity of cloud data using special blocks called sentinels. But this model discloses the information of user to the external parties and the privacy gets violated.

Juels et al.[3] in their research explained " Proof of Retrievability"(POR)model in which error correcting codes are used for retrievability of data file on service .But every time the user does not possible to check the data, which introduce burden to the user. This POR is used for only encrypted data, but we are introducing privacy-preserving public auditing for secure cloud storage independent to encryption, so this concept does not works.

Shacham and Waters[4] offered an improved POR scheme with improved security concept built from BLS signatures. But this concept is not good for privacy-preserving. Shan et al.[5]introduce TPA concept to reduce online burden and keeps the privacy-preserve.

Chen et al.[6] discussed a mechanism for auditing the correctness of data with multiple server.

Drawbacks in existing methods

1. Existing system does not support traceability.
2. Verification time and size of the signature linearly increase with number of user in group
3. Data freshness while still preserving identity privacy.
4. TPA can learn the original data during public auditing.

3. Proposed Work

In our proposed research work we find the solution to support both data and user's traceability based on signature and perform multiple auditing tasks simultaneously by using aggregate signature and also TPA gives detailed information on data error location to the cloud user.

Users send an auditing request to TPA, after receiving a request TPA send a auditing challenge to the cloud server. The CS generates proof based on verification signature and pass the auditing proof to TPA. TPA validates the proof and sends the auditing report to the user.

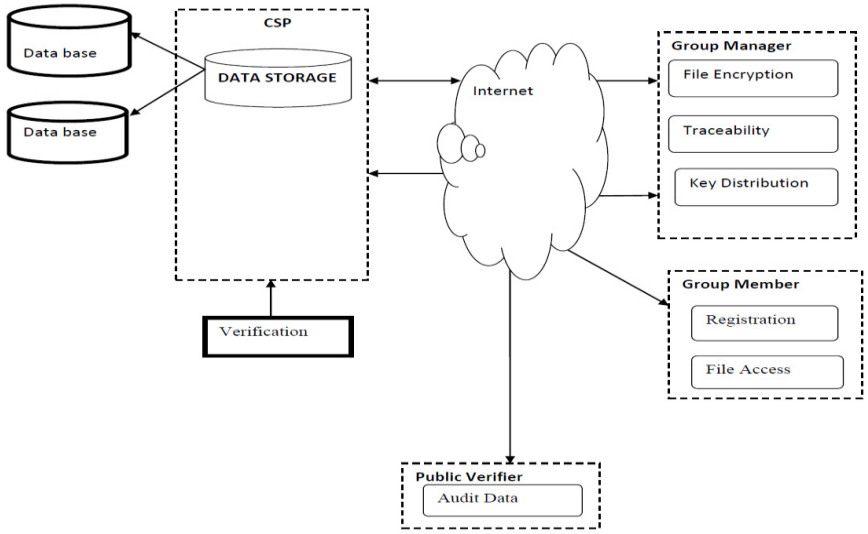

Fig.1 Public auditing in cloud

3.1 Public auditing mechanism

3.1.1 Key generation

Data owner preprocessed the file and generate own private key and group public key. New user request to the owner after accepting request new user join to the group and generate own private key. Any member of the group can access and share data files.(Fig.1)

3.1.2 Signature generation

User who have valid private key can only generate verification signature. Both data and signature stored in cloud server.

3.1.3 Data dynamics

User can able to perform dynamic data operations includes data insertion, deletion and update data over the encrypted outsourced data.

3.1.4 Traceability

A group manager can open signature on some special situation and trace the issue related to user. Tracing can be categorized into two ways, data traceability and operation traceability. In data tracing user can visually check the historical sequence of file creation, deletion, and transfer to other. The history displayed with personal information such as file name, etc.

3.1.5 Data error location

TPA gives detailed information on data block errors. Auditing method can directly locate the problem signature and point out specific data blocks where the errors are and when the auditing result is negative.

4. Conclusion

Cloud computing is a technology which is used worldwide through the internet. This survey is focused on privacy and security issues in cloud data storage and addressed some privacy approaches for overcoming the issues in privacy on untrusted data stores in cloud computing. In this paper, the methodologies as encryption based methods and auditability schemes are used. In

this work data integrity verification in cloud storage correctness can be efficiently verified by TPA. TPA cannot learn any data content during public auditing so identity can be preserved and also perform multiple auditing task simultaneously. Data owner can able to trace issues related to the user based on verification of meta data and identified the misbehaving user and also auditing results gives detailed information on data error location. In future our work will be focussed on Data freshness preserving identity privacy.

References

[1] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,3-42.

[2] Mohammed, A., AlSudiari, T., & Vasista, T. G. K. 2012. Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications.Advanced Computing: An International Journal (ACIJ), 3 (2), 159-169.

[3] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.

[4] H. Shacham and B. Waters, "Compact Proofs of retrievability,"Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008

[5] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[6] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Storage Systems," in *Proc. ACM*

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370..

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.

[9] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.
Computers, preprint, 2012, doi:10.1109/TC.2011.245

[10] Boyang Wang, Baochun Li, Hui Li, " Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud" IEEE Trans.

[11] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE.Transactions on Parallel and Distributed Systems (TPDS), vol. 24,no. 6, pp. 1182–1191, 2013

[12] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen,"Dynamic Audit Services for Outsourced Storage in Clouds,"IEEE Transactions on Services Computing, accepted **.**

[13] G.Ateniese et al., "Provable Data Possession at Untrusted Stores," Proc. ACMCCS '07, Oct. 2007, pp. 598–609.

[14] Ateniese, G., Burns, R., Curtmola, R., Herring, J.,Kissner, L., Peterson, Z., & Song, D. 2007, October. Provable data possession at untrusted stores. InProceedings of the 14th ACM conference on Computer and communications security (pp. 598-609). ACM.