International Journal of Database Theory and Application
Vol.9, No.6 (2016), pp.103-108
http://dx.doi.org/10.14257/ijdta.2016.9.6.10

A Study on the Public Auditing Mechanisms for Privacy Preserving and Maintaining Data Integrity in Cloud Computing

V.Saranya[1*], R.G. Suresh Kumar[2] and T.Nalini[3]

[1] *Master of Technology, Department of Computer Science and Engineering, Rajiv Gandhi College of Engineering & Technology, Pondicherry, India.*
[2]*Research Scholar, Vels University, Chennai, India.*
[3]*Professor, Department of Computer Science and Engineering, Bharath University, Chennai, India.*
[1]*saranya.vadivelu28@gmail.com,* [2]*aargeek@gmail.com,*
[3]*drnalinichidambaram@gmail.com*

Abstract

Cloud computing in its various forms allows users to store their information at remote location and reduce the burden at their local systems. Even though this is an advantage for users but there are also many drawbacks because of this remote storage. The main drawback which needs to be dealt with is security. Recently, security is the major concern which most of the cloud service providers are facing. The users store their information in remote location with the hope of maintaining the privacy and integrity of data. In order, to maintain the privacy and integrity of users' data auditing has to be done by the Cloud Service Providers (CSP). CSP uses the Third Party Auditor (TPA) for performing the auditing. The TPA performs auditing on behalf of the data owner using different auditing mechanisms. Many auditing mechanisms have been introduced in literature. Each mechanism varies from one another in one or more characteristics. In this paper we have provided a study on the different auditing mechanisms required to preserve the privacy and integrity of data in cloud. We have presented the advantages and flaws in each mechanism compared to another. Many auditing mechanisms are arising in literature with the aim to maintain the integrity of users' data and preserve the privacy. This paper remains as the basis for different auditing mechanisms that are arising in literature. With the help of auditing mechanisms the TPA can best satisfy the needs of the users.

Keywords*: Cloud Service Provider (CSP), Third Party Auditor (TPA), auditing, auditing mechanisms, privacy, integrity*

1. Introduction

Cloud computing is the practice of storing information at remote servers hosted on internet and used to store, manage and process data. The privacy is preserved by performing auditing of information without retrieving the entire block of data. The privacy preserving auditing integrates random masking method with homomorphic mechanism [1].

Cloud computing refers to both applications delivered as a service and hardware or software that provide those services. The services offered by cloud computing was initially called as Software-as-a-Service (SaaS). But vendors use the terms Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) depending upon the products they serve.

Even though Cloud Service Providers (CSPs) offers many services the integrity of data stored in the cloud must be maintained. So to maintain the integrity the cloud data has to be retrieved to check the correctness of data. But due to large size of cloud data the entire

ISSN: 2005-4270 IJDTA
Copyright ⓒ 2016 SERSC

data cannot be retrieved to check the integrity [2]. There are two classes of basic schemes that are used to check the integrity of data. They are:

MAC Based Solution

In MAC based solution users upload the data along with MAC to cloud server and provides secret key to TPA. TPA randomly retrieves the data blocks and MAC uses the secret key to check the correctness of stored data. But there are many flaws in using MAC based solution [3]. The computation and communication complexity is increased; TPA requires knowledge of data blocks for verification, auditing of data files is limited because secret keys are fixed.

HLA Based Solution

HLA based solution supports public auditing without retrieving the data blocks. It requires constant bandwidth. Aggregate HLA can be computed which authenticates linear combination of individual data blocks. Homomorphic authenticators are basic tools used to construct data auditing mechanisms. Homomorphic authenticable signature scheme should satisfy the properties of blockless verification and non-malleability [3].

2. Survey of Mechanisms Used for Auditing

In "Privacy Preserving Public Auditing for Shared Data in the Cloud", Swapnali Sakore *et al*. [4] proposed Speke (Simple Password –Authenticated Exponential Key Exchange) algorithm. In this privacy is accomplished by splitting the data into various blocks and storing it in multiple clouds which provides more protection. The encryption key is generated and stored in the Key Storage area, and encrypted data is stored in the cloud storage area. The Encryption service is responsible of doing this process. During the decryption process the decryption service collects the data and key, but it will not decrypt the data immediately. The data will be decrypted only when the user enters the OTP (One Time Password) sent to his mail. Then the decryption service decrypts the data and the data is provided to the user. The main drawbacks of this system is, it is dependent on network traffic since it is web based, encryption of data is difficult since data owners share data under the policy over attributes from multiple authorities.

Suvarna K. Kattimani *et al*. in the paper "Privacy Preserving Public Auditing Mechanism for Shared Data in Cloud Computing with Dynamic Groups" [5], proposed bilinear maps for security analysis. The system consists of four modules, where the proprietor request owner of cloud for data to store the information and use the resource of respective cloud. Proprietor can then request the outside verifier to audit the particular information. The outside verifier sends auditing message to public cloud server and in return server sends back the auditing proof. After examining the information, the examined result is sent back to proprietor. During the auditing process if there is any error in the information, then the outside verifier requests the owner of the private cloud for erroneous block of data. The system preserves the privacy for dynamic groups, identity of the user is preserved and metadata of information is not revealed to the TPA. The major drawbacks of the system include modification of information by hacker, traceability of users not identified by proprietor, complete auditing is not performed.

In "Enhanced Oruta Mechanism for Verifying Shared Data Integrity with Data Freshness and Traceability over Cloud Data", N. Deivanayaki *et al*. [6] proposed Digital Signature Technique. In this paper, to improve Data Privacy on shared data in cloud, Traceability oruta (One ring signature to Rule Them All) mechanism to achieve traceability is proposed. The data freshness (the cloud possesses the latest version of shared data) is also proved while still preserving identity privacy. Achieving data freshness ensures that the retrieved data always reflects the most recent updates and

 Copyright ⓒ 2016 SERSC

prevents rollback attacks. Achieving data freshness is essential to protect against misconfiguration errors. In this paper the data integrity in the cloud is well verified using the TPA and digital signature technique and the system is expected to reach a fine grade of data validity and quality.

The system provides traceability of users and identification of fake users by using version counter and logs of users and users update data by getting permission from the data owner. But no complete auditing is done because TPA may or may not be present and signature is stored in the cloud which may be hacked by malicious users since the data in the public cloud is accessed by public users.

Krishna Kumar L *et al*. in the paper "Preserving Privacy Policy – Preserving Public Auditing for Data in the Cloud" [7] proposed a technique called homomorphic encryption. In this system data is shared in the format of image or file types, cloud control and share the stored data to the user group. If an owner wants to sale his/her data in the cloud means an agreement is laid between cloud and data owner. If the cloud contains many customers, then cloud provides the service after payment of a particular amount. In this case the cloud act as a marketing manager and the original user is silent and the cloud gives a particular benefit percentage to the data owner.

One of the best ways to ensure confidential data protection in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for information storage, but few offer support for data at ease. The encryption capabilities of the cloud service provider need to equal the degree of sensitivity of the data being hosted. Some private cloud contains encrypted files so the user cannot change or remove the unwanted part of the shared data.

The main disadvantage is if the owner wants to upload the 10 file means the 10 files must be uploaded at the same time otherwise if the owner uploads first 5 files and then 5 files will change the order. In this condition homomorphic algorithm is used to edit the uploaded resource data for encrypted data change into a decrypted format.

In the paper "Storing Shared Data on the Cloud via Security-Mediator", Boyang Wang *et al*. [8] have proposed a Security Mediator (SEM) and Blind Signature techniques are used. In this paper, a simple and efficient publicly verifiable approach to ensure cloud data integrity, without compromising the anonymity of data owners nor introducing significant overhead on verification metadata has been introduced. The major benefit of this approach is the decoupling of anonymity protection mechanism from the PDP itself. In other words, the anonymity protection of data owners incurs no extra cost on cloud service providers or any public verifiers. The most direct approach is to have a SEcurity-Mediator (SEM) from the organization to sign on behalf of its all members. SEM can be maintained by the organization itself and it's the interest of the organization as to who should use the data storage on its paid cloud service. So a less trust is paid by the organization on the cloud.

The role of the SEM can be played by a typical server of an organization which is used for daily authentication of its members. However, one important difference from a typical authentication server is that it owns the private signing key corresponding to the organization's public key recognized by the cloud service provider and the rest of the world. Also SEM avoids bottleneck and single point of failure. The major drawbacks are Blinding signature is prone to blinding attack and since the signing process is equivalent to decrypting with the signer's secret key, an attacker can provide a blinded version of a message encrypted with the signer's public key.

Salve Bhagyashri *et al*. in the paper "Privacy-Preserving Public Auditing for Secure Cloud Storage" [9] has proposed Merkle Hash Tree (MHT) technique. In this system TPA generates a random set of keys which includes public key pk and private key sk. The signature is computed as σ on each block. Cloud Server (CS) computes root hash code based on the filename/blocks as input and CS computes the originally stored value. TPA

Copyright ⓒ 2016 SERSC

decrypts the given content and compares with generated root hash. After verification the TPA can determine whether the integrity is breached or not.

The major advantages of the system are it provides privacy preservation through public auditing and it performs batch auditing. MHT is used to split the data into blocks and authenticate each block. The drawbacks of the system include data writes or data changes in MHT involves several sequential hashes which could not be parallelized for efficiency and freshness of data stored in the cloud is not considered or monitored.

In "Traceability Mechanism for Sharing Data in Cloud", Kedar Jayesh Rasal *et al*. [10] has proposed a Key distribution Center (KDC). KDC is used to reduce risk of key exchange. So the verifier does not learn any information about the user. This method supports batch auditing and traceability. In this system the major entities involved are group manager, group users, KDC, cloud server and public verifier. The group manager conveys to KDC as to which user should share which information *i.e*. authorization of the user is given to KDC. Based on that the KDC will issue tickets to group members upon their request. If the ticket matches then the users are allowed to share data in the cloud. Key is provided to the users by the group manager. The public verifier audits the integrity of data on the request of group manager with only part of the information. Privacy is thus maintained. Also the traceability of user is maintained by using the KDC.

The major drawbacks of the system includes KDC may become a single point of failure. Every user and group manager must trust KDC for proper functioning of the architecture and KDC works only if users have registered previously. The ticket used by KDC expires within particular time. So again the users have to re-request for ticket for accessing particular service. The tickets that are re-issued are transparent to other users and may be hacked.

In "Security Conservation Based Common Evaluation of Mutual Information in Cloud Computing", Lavanya M. *et al*. [11] has proposed Token Based Ring System (TBRS). TBRS technique uses enhanced ring signature method. The data owner issues ticket token id to the users and they use this to modify data in the cloud. The users are identified in the cloud based upon this token. If users make modifications to data blocks using a token id then the token id is changed and new token id is generated by the data owner and distributed to all the users in the group. If the users have no token id or if they have some different token id then they cannot access the data blocks in the cloud and they are considered as intruder or hacker.

TBRS technique provides public auditing, data privacy, identity privacy for static group, identity privacy for dynamic group and integrity of data compared to other traditional methods. The major drawbacks includes the token issued can be used by anybody other than users in the group. So security is at risk. The token id can be manipulated by hackers. Even a hacker can enter the group because there is no entry check.

3. Comparison of Mechanisms Used for Auditing

The different mechanisms used in different papers in literature are compared with each other based upon the following terms. They are:

Dynamicity: This refers to whether the users in a group are dynamic in nature. It means whether a new user can enter the group or existing user can revoke the group.

Public Auditing: Whether the auditing is done with full-fledged and whether the integrity of data is maintained or not.

Trackability: The mechanism must be able to track the unauthorized users entering and leaving the group.

Data Privacy: The privacy of data has to be maintained and the secrecy of data must not be revealed to a user who has no authorization on data.

User Identity: The identity of the user performing modifications on the data must be preserved and must not be revealed to any other users.

 Copyright ⓒ 2016 SERSC

Freshness: The data stored in the cloud must be kept up to date. The auditing must provide the latest version of the data stored.

Efficiency: The auditing mechanism must be efficient and should take minimum computation and communication costs.

OBJECTIVE → / TECHNIQUE ↓	DYNAMICITY	PUBLIC AUDITING	TRACKABILITY	DATA PRIVACY	USER IDENTITY	FRESHNESS	EFFICIENCY
SPEKE	NO	PARTIAL	NO	LOW	LOW	NO	LOW
BILINEAR MAPS	YES	PARTIAL	NO	MEDIUM	MEDIUM	NO	LOW
DIGITAL SIGNATURE	NO	PARTIAL	YES	MEDIUM	MEDIUM	YES	LOW
HOMOMORPHIC ENCRYPTION	NO	PARTIAL	NO	MEDIUM	HIGH	NO	LOW
BLIND SIGNATURE	YES	PARTIAL	NO	MEDIUM	LOW	YES	LOW
MHT	NO	PARTIAL	NO	MEDIUM	MEDIUM	NO	LOW
KDC	NO	PARTIAL	YES	LOW	LOW	NO	LOW
TBRS	YES	PARTIAL	NO	MEDIUM	MEDIUM	NO	LOW

Figure 1. Comparison of Mechanisms Used for Auditing

4. Conclusion

Thus in this paper the mechanisms used for auditing in different papers in literature has been studied and flaws in each technique has been listed out. The techniques are compared to one another based on various characteristics. Many auditing techniques arise in literature. But these techniques remain as a basis for all the auditing mechanisms and the advantages in these mechanisms can be extracted and used in future upcoming auditing mechanisms.

Acknowledgements

We are grateful and thankful to the CARD research system of our college.

References

[1] B. Banupriya, V. Sobhana and M. Sushith, "Concise Survey on Privacy Preserving Techniques in Cloud", International Advanced Research Journal in Science, Engineering and Technology, vol. 2, no. 2, **(2015)**, pp. 27-29.

[2] S. Gade and P. Kumbharkar, "IEURC: Integrity of Shared data with Efficient User Revocation in the Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 11, **(2014)**, pp. 699-702.

[3] H. B. Patil and Y. S. Patil, "Survey on Auditing Mechanism for Preserving Privacy in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 4, **(2015)**, pp. 2732-2737.

[4] S. Sakore, R. Raut and V. Shinde, "Privacy Preserving Public Auditing for Shared Data in the Cloud", Proceedings of 20th IRF International Conference, **(2015)**, pp. 19-21.

[5] S. K. Kattimani, A. A. Atwadkar and S. Nandyal, "Privacy Preserving Public Auditing Mechanism for Shared Data in Cloud Computing Environment with Dynamic Groups", International Journal of Engineering and Computer Science, vol. 4, no. 6, **(2015)**, pp. 12368-12373.

[6] N. Deivanayaki and J. A. Bebina, "Enhanced Oruta Mechanism for Verifying Shared Data Integrity with Data Freshness and Traceability over the Cloud Data", International Journal of innovative Research and Development, vol. 4, no. 2, **(2015)**, pp. 166-169.

Copyright ⓒ 2016 SERSC

[7] L. K. Kumar and D. P. Sivan, "Preserving Privacy Policy-Preserving Public Auditing for Data in the Cloud", International Journal of Engineering Science Invention, vol. 3, no. 11, **(2014)**, pp. 06-09.
[8] B. Wang, S. S. M. Chow, M. Li and H. Li, "Storing Shared Data on the Cloud via Security-Mediator", IEEE 33rd International Conference on Distributed Computing Systems, **(2013)**, pp. 124-133.
[9] S. Bhagyashri and Y. B. Gurav, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IOSR Journal of Computer Engineering, vol. 16, no. 4, Ver. III, **(2014)**, pp. 33-38.
[10] K. J. Rasal and S. A. Kahate, "Traceability Mechanism for Sharing Data in Cloud", International Journal of Computer Science Engineering and Technology, vol. 5, no. 4, **(2015)**, pp. 86-89.
[11] M. Lavanya, C. Bhoomica, J. Vishwapriya and V. Vaithiyanathan, "Security Conservation Based Common Evaluation of Mutual Information in Cloud Computing", ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 11, **(2015)**, pp. 4733-4737.

Authors

V. Saranya, Pursued B. tech in Computer Science & Engineering and graduated from Rajiv Gandhi College of Engineering and Technology in 2012. Pursued MBA in HRM and graduated from Pondicherry University in 2014. Currently pursuing M. tech in Computer Science & Engineering at Rajiv Gandhi College of Engineering & Technology. Her areas of interest includes Cloud computing.

Suresh Kumar RG, Pursued MCA at Annamalai University in 2001. Pursued M. Tech (Information Technology) from AAD University in 2005. Currently pursuing PhD in Computer Science & Engineering at Vels University. He is a Sun Certified Professional and His main research areas include Client Server computing, Cloud computing and Utility Computing.

T. Nalini, Pursued MCA at Madras University in 2001, M. Tech (CSE) from Bharath University in 2007 and PhD in Computer Science & Engineering at Bharath University in 2006. She published 104 International Journals and she is a Director for Social Network Research Center at Bharath University.

 Copyright ⓒ 2016 SERSC