Survey of Secure Data Auditing in Cloud

Ms. Narahare Anuradha[1], Ms. Valte Pooja[2], Ms. Raykar Mayuri[3], Ms. Suhasini Ingwale[4] ,

Prof. D. V. Bhate[5]

[1]*Student, Computer Engg., Zeal COE, Vadgoan (bk), India*
[2]*Student, Computer Engg., Zeal COE, Vadgoan (bk), India*
[3]*Student, Computer Engg., Zeal COE, Vadgoan (bk), India*
[4]*Student, Computer Engg., Zeal COE, Vadgoan (bk), India*
[5]*Assistant Prof., Computer Engg., Zeal COE, Maharastra, India*

ABSTRACT

Cloud computing, also known as on-demand computing is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. But Cloud is not trusted entity, it may read the uploaded data for his benefit. Thus, privacy and integrity of uploaded data is of main importance. The simple solution is to use encryption and signature for privacy and integrity of data. There are different researches who work on this problem. This paper focuses on various privacy and integrity protection techniques in cloud. The objective of this paper is to study various public auditing schemes that will keep users identity private in overall auditing process.

Keyword: - *Ring Signature, Homomorphic Authenticable Ring Signature (HARS), Privacy Preserving, Public Auditing, Cloud Computing.*

1. INTRODUCTION

The cloud storage model the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a web-based content management or cloud storage gateway systems [7].

Security issues become more complex in a network environment. Many technologies are available to encrypt data and thus help to ensure its privacy and integrity. They ensure that: Data remains confidential, Data cannot be modified and identity of sender can be verified. The digital signature and any secure encryption algorithm achieve the goals of data integrity and privacy. But simple digital signature, having some drawbacks such as receiver knows the source of message. According to the goal, the identity of sender must remain secure, this is required in case of leaking any secret data without being identified and thus ring signature/group signature came into picture.

The cloud is un-trusted entity as it may read users uploaded data for getting rewards. Assume that data stored on cloud may be corrupted, deleted, modified, damaged or removed from cloud by mistake from cloud administrator. In this case, the cloud may not inform its users for the possible loss of their data, as it may damage their reputation. In such situation how user could verify the integrity of their data is a important challenge. This can be achieved using integrity checking process.

The next challenge in cloud environment is that the signature generated by user can't be generated by any adversary (unforgeability), nor adversary can copy the signature of user. This can be achieved using strong algorithm in which. Specifically, by utilizing direct anonymous attestation [8], which is adopted by the Trusted Computing Group as the anonymous method for remote authentication in trusted platform module, users are able to preserve their identity privacy on shared data from a public verifier. This approach has the main problem as it requires all the users using designed hardware, and needs the cloud provider to move all the existing cloud services to the trusted computing environment, which would be costly and impractical. The sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. So that, it is necessary to ensure the

integrity of shared data in the cloud is correct. A new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers [1].
The rest of paper is organized as follows: Section 2 covers literature review and section 3 contains concluding remarks.

2. LITERATURE SURVEY

A. Identity Privacy

The identity privacy of the user can be achieved by different ways such as,

1. Trusted Proxy

To achieve identity privacy of the signer the possible approach is to add a trusted proxy between a group of users and the cloud in the system model. More concretely, each member's data is collected, signed, and uploaded to the cloud by this trusted proxy, and then a public verifier can only verify and learn that it is the proxy signs the data, but cannot learn the identities of group members. The security of this method is still threatened by the single point failure of the proxy. Sometimes some of the group members would like to trust the same proxy for generating signatures and uploading data on their behalf. Utilizing group signatures [13] is also an alternative option to preserve identity privacy. Unfortunately, how to design an efficient public auditing mechanism based on group signatures remains open question. Trusted Computing offers another possible alternative approach to achieve the design objectives of this mechanism.

2. Global Secret Key

The identity privacy of the block signer can be reserved by employing a mechanism in which all the users share a global secret key [2][3]. Thus allowing any user in the group to sign a block on the behalf of the group and also check the integrity of their uploaded data. If the user in the group leaves, then the shared secret key must be newly generated and each block must be signed using newly generated secret key and distributed to all the group members. This causes huge burden on cloud users leaving this technique non-applicable in real time environment.

3. Ring Signature

Ring signature was first proposed by Rivest et al. [13] in 2001 using ring signatures. Using ring signatures a verifier is convinced that a signature is computed using one of group members' private keys, but the verifier is not able to determine which one. More simply, the message signer puts all the signatures of the group members on the document to be leaked. For generating his signature signing user uses his secret key and for other group member's user uses public keys of all the group members. Thus verifier sees multiple signatures on the document and verifier can't determine which actual signer of the document. Boneh et al. [12], constructed ring signature scheme constructed using bilinear maps.

B. Data Integrity

1. Merkle Hash

If the verifier has original message then it can compute merkle-hash root and challenge cloud server for the same. Any mismatch between two computed merkle-hash root values denotes that file has been modified.

2. Homomorphic authenticators

The verifier can check integrity of client's data stored at an untrusted server using homomorphic authenticators. In homomorphic authenticators the verifier can audit the integrity of uploaded data without retrieving the entire data by utilizing RSA-based homomorphic authenticators and sampling strategies. But this mechanism is only suitable for auditing the integrity of personal data. Verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values [4].

4. Aggregate Signature

Zhu et al. [5] proposed notion of aggregate signatures for reducing the cost of signatures storage. To provide dynamic operations on data they also used index hash tables. The public mechanism proposed by Wang et al. [4] is able to preserve users' confidential data from a public verifier by using random masking. They extended their mechanism to enable batch auditing by using aggregate signatures to operate multiple auditing tasks from different users efficiently, [13]. Wang et al. [4] used homomorphic tokens to ensure the correctness of erasure codes-based

data distributed on multiple servers. This mechanism is able to support dynamic data as well as to identify misbehaved servers.

Shacham and Waters [11] designed two improved schemes. The first scheme is built from BLS signatures and the second one is based on pseudo-random functions. To support dynamic data symmetric keys verifies the integrity of data, it is not public verifiable and only provides a user with a limited number of verification requests. Wang et al. [8] utilized Merkle Hash Tree and BLS signatures to support dynamic data in a public auditing mechanism. Erway et al. [9] had introduced dynamic provable data possession (DPDP) with the help of authenticated dictionaries, which are based on rank information.

5. Provable Data Possesion (PDP)

In PDP client pre-computes tags for each block of a file and the tag, file pair is uploaded on cloud. The client can verify the integrity of their uploaded data by challenging cloud server by generating challenge on a randomly selected set of file blocks. The server generates a proof of possession for each integrity request. The client is thus convinced of data possession, without actually having to retrieve file blocks.

Chen et al. [6] introduced a mechanism for auditing the correctness of data under the multi-server scenario. Where instead of using erasure codes data is encoded using network coding. Cao et al. [3] constructed an LT codes-based secure and reliable cloud storage mechanism. Compare to previous work [12], [14], this mechanism can avoid high decoding computation cost for data users and save computation resource for online data owners during data repair. Jachak K. B. 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) [8].

Dan Boneh, Craig Gentry [12], resented the idea of total signatures and developed a proficient total signatures plan taking into account bilinear maps. Key era, total, and confirmation oblige no cooperation. Author's demonstrated security of the framework in a model that gives the foe his decision of open keys and messages to fashion. For security, the extra limitation that a total signature is substantial just in the event that it is a conglomeration of signatures on particular messages is presented. This limitation is fulfilled normally for the applications as a main priority. All the for the most part, the imperative can be fulfilled by prep finishing general society key to the message before signing. Few applications for total signatures also discussed. Case in point, they can be utilized to diminish the span of declaration chains and decrease correspondence data transfer capacity in protocols, for example, SBGP.

C. Threat Models

A. Integrity Threats

An adversary may try to corrupt the data stored on cloud server. Even, cloud service provider itself may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors. It may be possible that, cloud service provider may not inform its users about its possible data losses because it may damage its reputation.

B. Privacy Threats

An adversary such as third party integrity verifier may try to reveal the identity of the signer on each block in shared data based on verification metadata. Once the public verifier reveals the identity of the signer on each block, it can easily distinguish a high-value target from others..

4. CONCLUSIONS

Cloud is designed to provide a service to the external users. To compensate their needs the resources should be highly available. In this paper various integrity verification techniques and identity privacy techniques are discussed. The homomorphic signature and ring signatures are proven to be better for allowing integrity verification and identity privacy. The homomorphic ring authenticator allows user to public verify integrity of their data without using copy of original message making overall system secure. The aggregate key is also useful technique for keeping signature size constant even while using multiple signatures..

REFERENCES

[1]. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage,"IEEE Trans.Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[2]. D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[3]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFO-COM, 2012.
[4]. 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, 2012.
[5]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau,"Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,"Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.
[6]. 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.
[7]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing,"Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.
[8]. 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.
[9]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession,"Proc. 16th ACM Conf. Com-puter and Comm. Security (CCS'09), pp. 213-222, 2009.
[10]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,"Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.
[11]. H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc.14th Int'l Conf. Theory and Application of ryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.
[12]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)". Springer-Verlag, 2003, pp. 416432.
[13]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems,"Comm. ACM,vol. 21, no. 2, pp. 120-126, 1978..