ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Evaluation of Public Auditing For Personal and Shared Data with Efficient User Revocation in Cloud Computing

Chinta Mounika
M.Tech Student,
Department of Computer Science and Engineering,
B.V.C Engineering College,
Amalapuram, Odalarevu.

B.S.N Murty
Assosicate Professor & HOD,
Department of Computer Science and Engineering,
B.V.C Engineering College,
Amalapuram, Odalarevu.

Abstract:

Cloud provides services like data storage and data sharing in a group. Users can remotely store their data on cloud and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. But the management of the data and services may not be fully trustworthy on cloud, as users no longer have physical possession of the outsourced personal data so data integrity protection becomes a difficult task. Maintaining the integrity of shared data services where data is shared among number of cloud user, is also a challenging task. This paper gives privacy preserving public auditing system for data storage security in cloud computing and for that it uses homomorphic linear authenticator with random masking technique. Homomorphic authenticable proxy resignature scheme with Panda public auditing mechanism checks shared data integrity along with efficient user revocation. Furthermore, these mechanisms are able to support batch auditing by verifying multiple auditing tasks simultaneously.

Index Terms:

Data storage, privacy-preserving, public auditing, shared data, user revocation, cloud computing.

INTRODUCTION:

CLOUD Computing provides characteristics as on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk, these characteristic makes cloud computing suitable for enterprises. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From user's perspective, including both individuals and IT enterprises, remotely storing data to the cloud provide advantages as a relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. As user don't have control over data after storing it in cloud so the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices but there is threat of data integrity. Secondly, Cloud service provider (CSP) might by discard data that has not been or is rarely accessed, or even hide data loss incidents so as to maintain a reputation. To address these problems, public key based homomorphism linear authenticator (HLA) technique can be used for auditing and by integrating the HLA with random masking, protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server during the efficient auditing process. The aggregation and algebraic properties of the authenticator further benefits the design for batch auditing. In share data services, as data is modified by different users that's why different blocks in shared data is signed by different users .

Each block is attached with a signature and integrity of data relies on the correctness of all the signatures. Once a user is revoked from group, at that time the block signed by the revoked user must be resigned by the existing user for security reasons. In basic method, first data blocks are downloaded by existing user and then upload process is done after verifying the correctness and resigning of block by existing user, which results in large amount of communication and computation cost due to large size of shared data in cloud.To protect the integrity of data in the cloud, a number of mechanisms have been proposed. In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred toas public auditing (or denoted as Provable Data Pos-session). This public verifier could be a client who would like to utilize cloud data for particular purposes(e.g., search, computation, data mining, etc.) or a third-party auditor (TPA) who is able to provide verificationservices on data integrity to users. Most of the previous works focus on auditing the integrity of personal data. Different from these works, several recent works focus on how to preserve identity privacy from public verifiers when auditing the integrity of shared data. Unfortunately, none of the above mechanisms, considers the efficiency of user revocation when auditing the correctness of shared data in the cloud. With shared data, once a user modifies a block, she also needs to compute a new signature for the modifiedblock. Due to the modifications from different users, dif-ferent blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group.

LITERATURE SURVEY:

The concept of public audit ability was given by Ateniese et al. [8]. They have described this concept in their defined provable data possession (PDP) model for making sure the ownership of data files on no trustworthy storage and used Rivest Shamir Adleman based homomorphic linear authenticators for auditing of outsourced data. Provable data possession model allows client (who has stored data on un-trusted server) to verify, that the server possesses the original data without retrieving it. PDP model creates probabilistic proofs of possession by sampling random sets of blocks from the server. This significantly minimizes I/O costs. The client maintains a constant amount of metadata to verify the proof. The response protocol sends a modest, constant quantity of information, which reduces network communication. Hence, the PDP model for distant information inspection supports large data sets in widely-distributed storage systems. Authors have presented two provably-secure PDP schemes that are more capable than prior solutions, even when compared with schemes that achieve weaker guarantees.

In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments by execution confirm the practicality of PDP and tell that the performance of PDP is restricted by disk Input output and not by cryptographic computation. For auditors who are external, linear combination of sample blocks were required and when directly used, their protocol did not provided privacy preserving and thus may leak the user data to auditors. Shacham et al. [7] built proof of retrievability (PoR) model and constructed a random linear function based homomorphic authenticator which enables limitless number of inquiry and requires minimal communication overhead. Shacham et al.s first methods, built from BLS signatures and secure in the random oracle model, characteristics of a proof-of retrievability protocol in which the clients inquiry and servers response are both very short.

This method allows public verifiability: anyone can act as a verifier, not only the file owner. Second method, which builds on pseudorandom functions (PRFs) and is protected in the regular model, allows only secret confirmation. It features a proof-of-retrievability protocol with a yet shorter servers response than the first method proposed, but the clients query is very long. Both methods depend on homomorphic characteristics to comprehensive evidence into one small authenticator value. Wang et al [6] projected a theory to combine BLS-based HLA with MHT to sustain equally publicauditability and full data dynamics. Considered a like support for incomplete dynamic data storage in a disseminated situation with added quality of data error localization. To efficiently carry public audit ability without having to recovering the data blocks themselves, resort to the homomorphic authenticator system.

Homomorphic authenticators are unforgeable metadata generated from individual data blocks, which can be strongly aggregated in such a way to reassure a verifier that a linear combination of data blocks is appropriately computed by verifying only the aggregated authenticator. In this design, here proposal is to use PKC based homomorphic authenticator (e.g. BLS signature or RSA signature based authenticator) to implement the verification protocol with public audit ability. In the following explanation, there is present the BLSbased method to illustrate the design with data dynamics support. As will be shown, the schemes designed under BLS construction can also be implemented in RSA construction. K.Ren et al [5] proposed privacy preserving system where public key based homomorphic authenticator is combined with

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

random masking which fulfill the requirement of efficient audit without demanding the local copy of data and user data privacy. Explored the technique of bilinear aggregate signature for multi user setting which allow third party auditor execute multiple number of auditing task together. C.Wang et al [4] proposed privacy-preserving public auditing system for data storage security in Cloud Computing. Homomorphic linear authenticator and random masking have been used to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users fear of their outsourced data leakage. Considering

TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, privacy-preserving public auditing protocol further extended into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that discussed schemes are provably secure and highly efficient. G.Wang et al [3] Proposed proxy provable data possession protocol for remote data checking as PPDP is major concern in public cloud when client cannot perform the remote data possession checking.

This proposed protocol is based on bilinear pairing technique and through security analysis and performance analysis author has proved that the protocol is provable secure and efficient.B. Li et al [2] has proposed a privacy preserving mechanism that supports public auditing on shared data stored in the cloud. He has used ring signature to compute verification metadata and identity of signer is kept private from public verifier, who are able to efficiently verify shared data integrity without retrieving the entire file.

Additionally this mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one and experimental results demonstrate the effectiveness and efficiency of this mechanism when auditing shared data integrity.B. Wang et al [1] proposed public auditing mechanism for shared data using homomorphic authenticator and efficient user revocation in cloud. Here semi trusted cloud re-signs the blocks which were signed by revoked user, using proxy re-signature and save a significant amount of computation and communication resources during user revocation.

EXISTING SYSTEM:

In existing mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing. This public verifier could be a client who would like to utilize cloud data for particular purposes or a third-party auditor (TPA) who is able to provide verification services on data integrity to users. With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block. Due to the modifications from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only.

DISADVANTAGES:

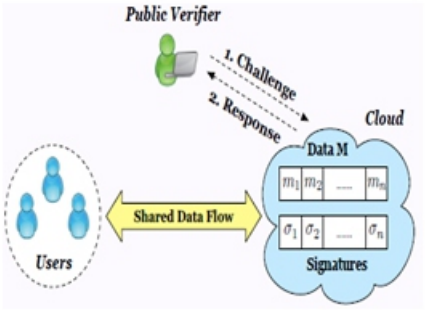
1. Straightforward method may cost the existing user a huge amount of communication and computation resources.
2. The number of re-signed blocks is quite large or the membership of the group is frequently changing.

PROPOSED SYSTEM:

In this paper, we propose Panda, a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud, which is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with nice properties, which traditional proxy resignatures do not have, our mechanism is always able to check the integrity of shared data without retrieving the entire data from the cloud. Moreover, our proposed mechanism is scalable, which indicates it is not only able to efficiently support a large number of users to share data and but also able to handle multiple auditing tasks simultaneously with batch auditing. In addition, by taking advantages of Shamir Secret Sharing, we can also extend our mechanism into the multi-proxy model to minimize the chance of the misuse on re-signing keys in the cloud and improve the reliability of the entire mechanism.



Advantages:

1. It follows protocols and does not pollute data integrity actively as a malicious adversary.
2. Cloud data can be efficiently shared among a large number of users, and the public verifier is able to handle a large number of auditing tasks simultaneously and efficiently.

IMPLEMENTATION:

Proxy Re-signatures:

Proxy re-signatures, first proposed by Blaze et al., allow a semi-trusted proxy to act as a translator of signatures between two users, for example, Alice and Bob. More specifically, the proxy is able to convert a signature of Alice into a signature of Bob on the same block. Meanwhile, the proxy is not able to learn any private keys of the two users, which means it cannot sign any block on behalf of either Alice or Bob. In this paper, to improve the efficiency of user revocation, we propose to let the cloud to act as the proxy and convert signatures for users during user revocation.

Shamir Secret Sharing:

An (s, t)-Shamir Secret Sharing scheme [18] (s ‘2t − 1), first proposed by Shamir, is able to divide a secret $ into s pieces in such a way that this secret $ can be easily recovered from any t pieces, while the knowledge of any t − 1 pieces reveals absolutely no information about this secret $. The essential idea of an (s, t)-Shamir Secret Sharing scheme is that, a number of t points uniquely defines a t−1 degree polynomial.

Efficient and Secure User Revocation:

We argue that our mechanism is efficient and secure during user revocation. It is efficient because when a user is revoked from the group, the cloud can re-sign blocks that were previously signed by the revoked user with a re-signing key, while an existing user does not have to download those blocks, re-compute signatures on those blocks and upload new signatures to the cloud.

The re-signing preformed by the cloud improves the efficiency of user revocation and saves communication and computation resources for existing users. The user revocation is secure because only existing users are able to sign the blocks in shared data.

As analyzed , even with a re-signing key, the cloud cannot generate a valid signature for an arbitrary block on behalf of an existing user. In addition, after being revoked from the group, a revoked user is no longer in the user list, and can no longer generate valid signatures on shared data.

Support Dynamic Data:

To build the entire mechanism, another issue we need to consider is how to support dynamic data during public auditing. Because the computation of a signature includes the block identifier, conventional methods — which use the index of a block as the block identifier (i.e., block mj is indexed with j) — are not efficient for supporting dynamic data .

Specifically, if a single block is inserted or deleted, the indices of blocks that after this modified block are all changed, and the change of those indices requires the user to re-compute signatures on those blocks, even though the content of those blocks are not changed.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSION AND FUTURE WORK:

This paper discusses Privacy preserving public auditing mechanisms, homomorphism linear authenticator with random masking have been used to guarantee that the third party auditor would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the user's fear of their outsourced data leakage. Homomorphism authenticable proxy re-signature scheme with Panda public auditing mechanism checks shared data integrity along with efficient user revocation.

Furthermore, these mechanisms are able to support batch auditing by verifying multiple auditing tasks simultaneously. In future work we would be focusing on developing a complete framework that would cover all integrity aspects related to data with identity privacy for dynamic group. We thought this channelized project would lean to aid the institutions/organizations to encourage towards the Cloud environment and construct rich IT infrastructure. Unfortunately, how to design such type of collusion resistant proxy re-signature schemes while also supporting public auditing (i.e., block less verifiability and non-malleability) remains to be seen.

Essentially, since collusion-resistant proxy re-signature schemes generally have two levels of signatures (i.e., the first level is signed by a user and the second level is re-signed by the proxy), where the two levels of signatures are in different forms and need to be verified differently, achieving block less verifiability on both of the two levels of signatures and verifying them together in a public auditing mechanism is challenging. We will leave this problem for our future work.

REFERENCES:

[1] John W. Rittinghouse James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 © 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–610.

[3] B. Wang, B. Li and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", ACNS2012 .

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.

[5] P. Maheswari, B. Sindhumathi "AFS: PrivacyPreserving Public Auditing With Data Freshness in the Cloud" IOSR Journal of Computer Engineering (IOSRJCE) PP 56-63 .

[6] B. Wang, B. Li, and H. Li, "Panda: Public Auditing For Shared Data with Efficient User Revocation in The Cloud" IEEE Trans. Services Computing, Dec.2013

[7] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 552–565 .

[8] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 552–565.

[9] Lakshmi et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(8), August - 2014, pp. 54-62 .

[10] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," in the Proceedings of EUROCRYPT 98. Springer Verlag, 1998, pp.127–144 .

[11]Zahir Tari, RMIT University, "Security and Privacy In Cloud Computing", IEEE Cloud Computing Published by the IEEE Computer Society 2014.

[12]B. Wang, B. Li, and H. Li, "Oruta: Privacy- Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud 2012, 2012, pp. 295–302.

[13]Zhifeng Xiao and Yang Xiao, Senior Member, IEEE, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials, vol. 15, no. 2,Second quarter 2013.

[14]C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533

[15]http://techatftc.wordpress.com/2012/05/15/what-does-it mean-to-preserve-privacy/