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

A Study on Panda: Public Auditing for Shared Data with Efficient User Revocation in Cloud

J.Navaneetha
Associate Professor
Department of CSE
Tirumala Engineering College.

K.Mahesh
Associate Professor
Department of CSE
Tirumala Engineering College.

C.V.Kavya Sree
M.Tech Student
Department of CSE
Tirumala Engineering College.

Abstract

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 resignatures, 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 the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

*Index Terms—**Public auditing, shared data, user revocation, cloud computing.***

INTRODUCTION

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. ne 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 (or denoted as Provable Data Possession). 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 verification services 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 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.

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

Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. It describes a new supplement, consumption, and delivery model for IT services based on the Internet. It has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its wide range of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk.

As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

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, who 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 the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user.

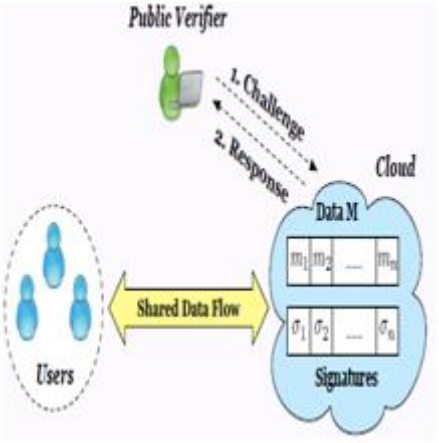

Fig :- public auditing

LITERATURE SURVEY

Ensuring Data Storage Security in Cloud Computing:

In this Paper, author focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

A View of Cloud Computing :- Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be

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

concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue.

Compact Proofs of Retrievability:

In this paper, first scheme was built from BLS signatures and secure in the random oracle model, features a proof-of-retrievability protocol in which the client's query and server's response are both extremely short. This scheme allows public verifiability: anyone can act as a verifier, not just the file owner.Second scheme, which builds on pseudorandom functions and is secure in the standard model, allows only private verification. It features a proof-of-retrievability protocol with an even shorter server's response than our first scheme, but the client's query is long.

Provable Data Possession at Untrusted Store:

In this paper author introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it.The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication.

PROBLEM STATEMENT

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.

Drawbacks:-

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.

PROBLEM DEFINITION

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 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 re-signatures 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

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

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.

RING SIGNATURES

The ring signatures concept is first proposed by Rivest et al. in 2001. With ring signatures, a verifier is convinced that a signature is computed using one of group member's private keys, but the verifier is not able to determine which one. This property can be used to preserve the identity of the signer from a verifier. We have reviewed that the following algorithms will help us to construct our proposed mechanism.

KeyGen: In KeyGen each user in the group generates her public key and private key.

ReKey: For each pair of user in the group, cloud computes a resigning key with ReKey.

ProofGen: Proof of possession of shared data is generated.

ProofVerify: In ProofVerify TPA verifies the correctness of proof responded by cloud.

ReSign: In ReSign algorithm signature of revoked user is converted to the original user.

RingSign: In a RingSign a user in the group signs a block with their private key & all group members public key.

RingVerify: In this verifier is allowed to check whether the given block is signed by that the group member only.

IMPLEMENTATION

Public Verifier: The public verifier is able to correctly check the integrity of shared data. That means it checks the correctness of the shared data that is share by the user.

User: User is the person who shares the data in the group or as a group.

Cloud: This is an entity that provides data storage service.

Public Auditing: The public verifier can audit the integrity of shared data without retrieving the entire data from the cloud, even if some blocks in shared data have been re-signed by the cloud.

Correctness: The public verifier is able to correctly check the integrity of shared data.

Efficient and Secure User Revocation: On one hand, once a user is revoked from the group, the blocks signed by the revoked user can be efficiently re-signed. On the other hand, only existing users in the group can generate valid signatures on shared data, and the revoked user can no longer compute valid signatures on shared data.

Scalability: 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.

RELATED WORK

Provable Data Possession (PDP), first proposed by Ateniese et al., allows a public verifier to check the correctness of a client's data stored at an untrusted server. By utilizing RSA-based homomorphic authenticators and sampling strategies, the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public verifiability or public auditing. Shacham and Waters designed an improved PDP scheme based on BLS (Boneh-Lynn- Shacham) signatures.

To support dynamic operations on data during auditing, Ateniese et al. presented another PDP mechanism based on symmetric keys. However, it is

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

not publicly verifiable and only provides a user with a limited number of verification requests. Wang et al. utilized the Merkle Hash Tree to support fully dynamic operations in a public auditing mechanism. Erway et al. introduced Dynamic Provable Data Possession by using authenticated dictionaries, which are based on rank information. Zhu et al. exploited the fragment structure to reduce the storage of signatures in their public auditing mechanism. In addition, they also used index hash tables to provide dynamic operations for users.

Wang et al. leveraged homomorphic tokens to ensure the correctness of erasure code-based data distributed on multiple servers. To minimize the communication overhead in the phase of data repair, Chen et al. introduced a mechanism for auditing the correctness of data with the multi-server scenario, where these data are encoded with network coding. More recently, Cao et al. constructed an LT code-based secure cloud storage mechanism. Compared to previous mechanisms this mechanism can avoid high decoding computation costs for data users and save computation resources for online data owners during data repair. Recently,Wang et al. proposed a certificateless public auditing mechanism to reduce security risks in certificate management compared to previous certificatebased solutions.

When a third-party auditor (TPA) is introduced into a public auditing mechanism in the cloud, both the content of data and the identities of signers are private information to users, and should be preserved from the TPA. The public mechanism proposed by Wang et al. is able to preserve users' confidential data from the TPA by using random maskings. In addition, to operate multiple auditing tasks from different users efficiently, they also extended their mechanism to support batch auditing. Our recent work first proposed a mechanism for public auditing shared data in the cloud for a group of users. With ring signature-based homomorphism authenticators, the TPA can verify the integrity of shared data but is not able to reveal the identity of the signer on each block. The auditing mechanism in is designed o preserve identity privacy for a large number of users. However, it fails to support public auditing. Proofs of Retrievability (POR) is another direction to check the correctness of data stored in a semi-trusted server. Unfortunately, POR and its subsequent work do not support public verification, which fails to satisfy the design objectives in our paper

CONCLUSION

In this paper, analyses of proposed work is done and have a tendency to propose a completely unique public auditing mechanism for the integrity of shared knowledge with economical user revocation in mind. By utilizing the thought of proxy re-signatures, give tendency to enable third party to re-sign blocks on behalf of existing users throughout user revocation and other third party auditor is often able to audit the integrity of shared knowledge while not retrieving the complete knowledge from the cloud. Additionally, a resource broker (third party) creates revocation list and initial user key. Moreover, this mechanism is in a position to support batch auditing by verifying multiple auditing tasks at the same time. We proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud with multiple trusted third party auditors. When a user in the group is revoked, this allow third party to re-sign blocks that were signed by the revoked user with proxy re-signatures done by TTP along with checking integrity of shared data.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revoation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[2] 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," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.

[6] 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.

[7] 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.

[8] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.

[9] 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.

[10] 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.

[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.

[12] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013.

[13] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted.

[14] 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.

[15] S. R. Tate, R. Vishwanathan, and L. Everhart, "Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware," in Proceedings of ACM CODASPY'13, 2013, pp. 353–364.