Public Auditing for Shared Knowledge with Economical user Revocation Within the Shared Cloud Setting

Mrs. R. Poornima
Assistant Professor
Department of Computer Science and Engineering
K.S. Rangasamy College of Technology,India

Kiruba. S
Dept. of Computer Science and Engineering
K.S.Rangasamy College of Technology
Tiruchengode, India

Malathi. C
Dept. of Computer Science and Engineering
K.S.Rangasamy College of Technology
Tiruchengode, India

Monika. H
Dept. of Computer Science and Engineering
K.S.Rangasamy College of Technology
Tiruchengode, India

***Abstract*:- In today's computing world in the cloud user can easily modify and share data as group. The main issues in the cloud computing was data privacy, data integrity, data access by unauthorized users. Tusted Third Party is used to store and share data in cloud computing. To verify integrity of data, users in the group need to compute signature on all the blocks in shared data. In shared data different blocks signed by different user due to data modification performed by different users. User revocation is biggest security reason in data sharing in the group. Once user is revoked from the group, the blocks which were previously signed by this revoked user must be resigned by an existing user. This allows an existing user to download the corresponding part of shared data and re-sign it during user revocation. This task is very inefficient due to the large size of shared data in the cloud.**

Keywords:- IB-DPDP,Data sharing,Data possession,Cloud security.

1. INTRODUCTION

The data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straight forward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud.

The public auditing for shar knowledge with economical user revocation in the shared cloud setting proposed a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, it allow,the cloud to re-sign blocks on behalf of existing users during user revocation.So that, existing users do not need to download and re-sign blocks by themselves. 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,this mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that mechanism can significantly improve the efficiency of user revocation.

2 PROPOSED SYSTEM

The advantages over the existing system are,the method use an identity tree instead of key tree in the scheme. Each node in the identity tree is associated with an identity. The leaf node's identity is corresponding to the user's identity and the intermediate node's identity is generated by its children's identity. Hence, in an identity tree, an intermediate node represents set users in the sub tree rooted at this node.This method propose a novel multi-cloud Authentication protocol, namely IB-DPDP, including two schemes.Each subgroup is treated almost like a separate multi-cloud group and is managed by a trusted group security intermediary identity based distributed provable data possession. IB-DPDP connects between the subgroups and shares the subgroup key with each of their subgroup members The basic scheme (IB-DPDP) eliminates the correlation among data's and thus provides the perfect resilience to data security, and it is also efficient in terms of latency, computation, and communication overhead due to an efficient cryptographic primitive called batch signature, which supports the authentication of any number of Data simultaneously. This study also present an enhanced scheme IB-DPDP, which combines the basic scheme with a data filtering mechanism to alleviate the DoS impact while preserving the perfect resilience to data security.The keys used in each subgroup can be generated by a group of IB-DPDP on Multi cloud storage Key Generation centers (IB-DPDP) in parallel. All the members in the same subgroup can compute the same subgroup key though the keys for them are generated by different KGCs. This is a desirable feature especially for the large-scale network systems, because it minimizes the problem of concentrating the work load on a single entity.

3 MODULE DESCRIPTION

In public auditing for shared data with efficient user revocation in the shared cloud environment.

3.1 GROUP MEMBER REGISTRATION & LOGIN

The first User entered the username, password, and chooses any one group id then register with Data Cloud Server. This user added in this particular group. Then entered the username, password and choose the user's group id for login.

3.2EFFICIENT KEY GENERATION& CONTROLLER USING IB-DPDP

In Key Generation module, every user in the group generates public key and private key. User generates a random, and outputs public key and private key. Without loss of generality, In the approach, assume user u1 is the original user, who is the creator of shared data. The original user also creates a user list (UL), which contains ids of all the users in the group. The user list is public and signed by the original user.

3.3 UPLOAD FILE TO DATA MULTI CLOUD SERVER

The user wants to upload a file. So the user split the files into many blocks. Next encrypt each blocks with the public key. Then, the user generate signature of each blocks for authentication purpose. Then upload each block cipher text with signature, block id and signer id.These metadata and Key Details are stored in Public Verifier for public auditing.

3.4 DOWNLOAD FILE FROM CLOUD SERVER

The next user or group member wants to download a file. So the user gives the file name and get the secret key. Then entered this secret key.If this secret key is valid then the user able to decrypt this downloaded file. Else, the next user entered wrong secret key then the user1 blocked by Public Verifier. If this secret key is valid then decrypt each block and verify the signature. If both signatures are equal then combine all blocks then get the original file.

3.5 PUBLIC AUDITING WITH USER COLLISION IN PUBLIC VERIFIER

In Public verifier method, the User who entered the wrong secret key then blocked by the public verifier. Next the user sadded public verifier collision user list. Then the user wants to tries to download any file, the Data Cloud Server replies his blocked information. Then the user wants to un collision, so they ask the public verifier. Finally the public verifier unrevocked this user.Next the user able to download any file with its corresponding secret key. In this approach, by utilizing the idea of proxy re-signatures, once a user in the group is collision, the Data Cloud Server is able to re-sign the blocks, which were signed by the collision user, with a resigning key. As a result, the efficiency of user collision can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the Data Cloud Server, who is not in the same trusted domain with each user, is only able to convert a signature of the collision user into a signature of an existing user on the same block, but it cannot sign arbitrary blocks on behalf of either the collision user or an existing user.

The User who entered the wrong secret key then blocked by the public verifier. Next they added public verifier revoked user list. Then the user wants to tries to download any file, the Data Cloud Server replies the blocked information. Then the user wants to un revocation, so ask the public verifier. Finally the public verifier unrevocked this user.Next the user able to download any file with its corresponding secret key.

4 CONCLUSION

The public auditing for shared knowledge with economical user revocation within the shared cloud setting proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, which allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Experimental results show that the cloud can improve the efficiency of user revocatison, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

This investigated proofs of storage in cloud in a multi-user setting. This introduced the notion of identity based data outsourcing and proposed a secure IBDO scheme. It allows the file-owner to delegate her outsourcing capability to proxies. Only the authorized proxy can process and outsource the file on behalf of the file-owner. Both the file origin and file integrity can be verified by a public auditor. The identity-based feature and the comprehensive auditing feature make the scheme advantageous over existing PDP/PoR schemes. Security analyses and experimental results show that the proposed scheme is secure and has comparable performance as the SW scheme.

It revisited the identity based distributed provable data possession scheme in multi cloud storage and demonstrated that the scheme fail to achieve the soundness.The server can still generate a valid proof to proof that the data are stored intact.It is a generic construction of ID-PDP protocols by using general signature schemes and traditional PDP protocols and proved it's security.

ACKNOWLEDGEMENTS

We Acknowledge DST- File No.368. DST – FIST (SR/FIST/College-235/2014 dated 21-11-2014) for financial support and DBT – STAR College – Scheme - ref.no: BT/HRD/11/09/2018 for providing infrastructure support.

REFERCENCE

1. B. Wang, H. Li, and M. Li, "Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics," in the Proceedings of IEEE ICC.
2. 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..

3. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud.
4. H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of Springer-Verlag.
5. M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos, "Hourglass schemes: how to prove that cloud files are encrypted," in the Proceedings of ACM CCS.
6. Cao N, Yu S,Yang z "LT Codes-based Secure and Reliable Cloud Storage Service", in the Proceedings of IEEE INFOCOM.
7. Hu H ,Chen S, Zhu Y"Dynamic Audit Services for Outsourced Storage in Clouds," in the Proceedings of IEEE.
8. Yuan J and Yu S, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud", in the Proceedings of ACM .
9. Li M, Cao N, Lou W, "FindU Private-Preserving Personal Matching in Mobile Social Networks", in the Proceedings of IEEE INFOCOM.
10. Tate S.R, Vishwanathan,Everhart L "Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware", in the Proceedings of ACM.