ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016

Securing Shared Data in Public Cloud with User Revocation

M.Thangamani,V.Sathyapriya.,M.E

PG Scholar, Department Of Computer Science and Engineering, RVS Technical Campus Cbe,Coimbatore

Assistant Professor, Department Of Computer Science and Engineering,RVS Technical CampusCbe, Coimbatore

ABSTRACT: In the cloud environment users can easily modify and share data as a group. The public verifier is able to appropriately check the integrity of shared data. Once a user is revoked from the assembly, the blocks signed by the revoked user can be efficiently re-signed. Only existing users in the group can generate valid signatures on shared data, and the revoked user can not at all longer for computing valid signatures on shared data. In this paper, a novel public auditing mechanism (Panda) for the integrity of shared data with efficient user revocation is proposed. By using the idea of proxy re-signatures, the cloud store sign blocks is allowed on behalf of existing users during user revocation, hence that the existing users do not essential to re-sign blocks and download by themselves. In addition, a public verifier is continuously capable to audit the integrity of shared data without retrieving the entire data from the cloud even though if some part of shared data have been re-signed by the cloud. Furthermore, this mechanism is capable to support batch auditing can simultaneously verifying multiple auditing tasks. This mechanism can significantly increase the efficiency of user revocation. Cloud data can be efficiently shared among the public verifier and a large number of users are able to handle a large number of reviewing tasks simultaneously and efficiently.

KEYWORDS: Shared Data, Efficient, Signature, Re-sign, Polling Revocation, Integrity

I. INTRODUCTION

In today's world, cloud computing is an internet based computing that made revolution. It is the major innovation which improves data sharing, data storing capabilities and advanced computational power. Cloud is a huge collection of interconnected processors that is a most important change in how run application and store information. The main advantage of the cloud is low cost and the major disadvantage in this is security. This cloud computing security contains to control deployed to protect data, a set of policies, technology , application and the related organization of cloud computing. Some privacy and security issues their necessity to be considered. Owing to the growth in network bandwidth it befits earlier to deliver quality of services (QOS) as related to previous and also provision to moving the data between client and cloud without any complexity, because of releasing the hardware complexity. In online base computing, cloud provides large amount of resources and data storage to the local machine and then eradicate the local machine to keep individual data. These results users are at the obliged of their cloud service sources for the integrity and availability of their data.

A. Public Data Auditing in Cloud

In the cloud resources, we can able to store the data as a group and modify or share it within a group. Cloud data storage contains two entities. They are as follows:

1. Cloud user or group members
2. Cloud server or cloud service provider

1. Cloud user

Cloud user is a person who stores huge amount of data on cloud server which is maintained by the Cloud Service Provider (CSP). User can upload their data on cloud and share it within a group.

2. Cloud Service Provider

A cloud service provider provides services to the cloud user. The main problem in cloud data storage is to obtain integrity of data and correctness stored on the cloud. Cloud Service Provider (CSP) has to provide some

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016

mechanism through which user will get the authorization that cloud data is secure or is stored as it is. No modification or data lossis done by unauthenticated member.

So that, data auditing concept can be achieved in 2 ways for enhance the Security.

- Without trusted third party
- With trusted third party based on who does the verification.

Sound all-round management of water are keys for sustainable water services in economic, social and ecological relationships and dimensions which portends towards national water supply sustainability.

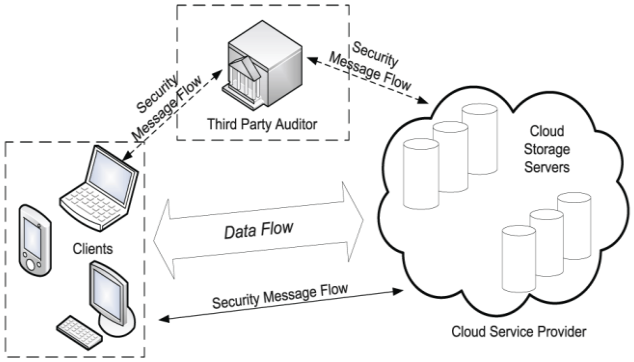


Fig 1.Architecture of Cloud data storage

The architecture of cloud data storage service as shown in the fig1.1.In this architecture; it is very difficult task to store the data centrally then managing this centralized data and providing security. So, TPA is used in this situation. The reliability is improved as data is handled by TPA but data integrity is not attained. TPA utilizes encryption technique to encrypt the contents of the file. In this paper Dropbox and Google Drive Applications can be used for ensuring user revocation.

B. Security Issues

In cloud computing,the security is a major issue. It is a sub domain of network security, data security or else computer security. Some privacy and security issues that essential to be considered are as follows:

1. Authentication
2. Correctness of data
3. Availability:
4. No storage Overhead and easy maintenance
5. No data Leakage
6. No Data Loss

C. Cloud Computing Threads

- Data Tempering Threat
- Spoofing Identity Theft
- Log In
- Information Disclosure on up/download Intra-Cloud
- Denial of Service(DOS) Attack
- Repudiation Attack

II. RELATED WORKS

A. DYNAMIC PROOFS OF RETRIEVABILITY VIA OBLIVIOUS RAM

This paper explains the first solution providing proofs of irretrievability for dynamic storage wherever the client may perform arbitrary reads or writes on any position within the data by running an effective protocol with the server. The client can implement an effective audit protocol to ensure that the server retains the modern version of the

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016

client data at any point in time. The communication and computation complexity of the client and server in these protocols is individual poly logarithmic in the size of the client's data. In this solution the starting point is to divided the data into minor blocks and excessively encode each block of data individually, hence that an update inside any data block only features a few code word symbols. To prevent the server from identifying and eliminating too many codeword symbols be appropriate to any single data block is the main difficulty. Using the algorithmic techniques of oblivious RAM, this scheme is done by hiding wherever several code word symbols of some individual data block are stored on the server and while they are being accessed by the client.

B. ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING

In spite of the possible gain achieved from the cloud computing. In today's world, most enticing technology area due to its cost-efficiency, flexibility and at least in part. Cloud computing transfers the application database and software to the large data center wherever the services and data management may not be fully dependable. In this article the major discussion on the cloud data storage security, the security is an important aspect of Quality of Services(QOS). To ensures the correctness of user data in cloud an flexible and effective distribution scheme two way handshakes based on token management. The homomorphic token is utilized with distributed verification of erasure-coded data and this scheme attains the integration of data error localization and storage correctness insurance that is the identification of misbehaving servers.

C. REMOTE DATA CHECKING FOR NETWORK CODING-BASED DISTRIBUTED STORAGE SYSTEMS

In this research a novel efficient and secure RDC scheme for network coding-based distributed storage systems is proposed. This RDC-NC mitigates many new attacks that stem from the fundamental principle of network coding in the network. This scheme is capable to preserve in an combative setting the minimal communication overhead of the repair component achieved by network coding in a compassionate setting. This scheme is implemented and then experimentally shows that it is computationally low-cost for both clients and servers.

D. HOURGLASS SCHEMES: HOW TO PROVE THAT CLOUD FILES ARE ENCRYPTED

This paper proposed the hourglass schemes to prove correct encryption of files at rest by imposing a resource requirement (e.g., computation, storage or time) on the process of translating files from one plaintext (i.e., encoding domain) to a different ciphertext (i.e., target domain). These hourglass schemes exploit common cloud infrastructure features such as limited file-system parallelism and the usage of rotational hard drives for at-rest files. In this paper an hourglass scheme s described for files of modest size which exploits access one-way permutations to prove correct file encryption whatever the basic storage medium.

III. CIPHERTEXT-POLICY ATTRIBUTE BASED ENCRYPTION

An Attribute-Based Encryption (ABE) is an encryption scheme wherever users with some attributes can decrypt cipher texts associated with these features. Though, the length of the cipher text depends on the number of attributes in previous ABE schemes.

A new Cipher text-Policy Attribute-Based Encryption (CP-ABE) with constant cipher-text length in this system.CP-ABE is a type of public-key encryption by which the cipher text and the secret key of a user are dependent upon characteristics. At least one individual key grants access for proof access data.

Security Model for CP-ABE semantic security under CPA(chosen-plaintext) attack is demonstrated by an IND-sAtt-CPA game. This game is carried out between an adversary A and challenger wherever the challenger pretends the protocol implementation and responses queries from A.

Step 1: Init: The adversary chooses the challenge access tree T* and provides it to the challenger.
Step 2: Setup: The challenger runs Setup to generate (pk;mk) and provides the public key pk to the adversary A.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016

Step 3: Phase1: A creates a secret key request to the Keygen oracle for any attribute or element. Set ω={*aj*| *ajϵ* Ω}with the restriction that a The challenger returns Keygen(ω; mk).

Step 4: Challenge: A sends to the challenger two messages m0;m1. Hence the challenger preferences a random bit b 1g and returns cb = Encrypt(mb, T*,pk).

Step 5: Phase2: A may continue querying Keygen with the same limitation as in Phase1.

Step 6: CP-ABE scheme is said to be protected against an adaptive chosen-plaintext attack (CPA) The negligible advantage in the IND-sAtt-CPA game has only if any polynomial-time adversary wherever the benefit is defined to be □ =|PrPr[*b* '= *b*]-1/2

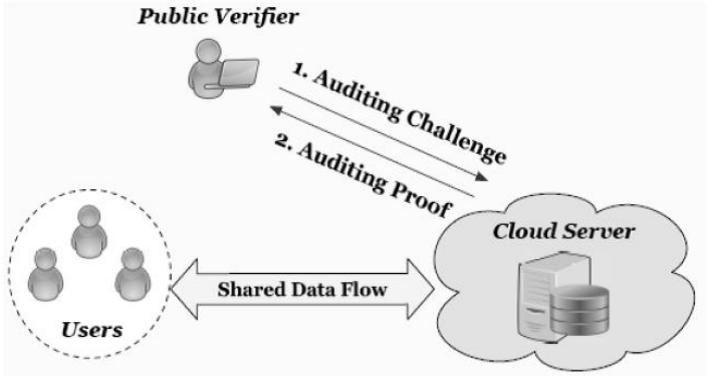


Fig.3.The system model includes the cloud, the public verifier, and users.

Fig. 2 illustrated the system model in this paper includes three entities: users (who share data as a group), the public verifier and the cloud. The cloud offers data storage and sharing services to the group. Although, the public verifier such as a client who would like to utilize cloud data for particular purposes for example, data mining, computation, search, etc., or a third-party auditor (TPA) aims to check the integrity of shared data via a response and challenge protocol who can provide verification services on data integrity with the cloud. In this group there are a number of group users and one original user. The original user is the original owner of data and creates then shares the data with other users in groups through the cloud. A user in the group can modify a block in shared data by performing an insertion, deletion or updating operation on the block. Both the original group and original users are able to download, modify, and access shared data.

A. Drawbacks

- Maintenance Cost is high for checking all the resigning keys in the cloud.
- Security and Integrity is low.
- Require more bandwidth to download.

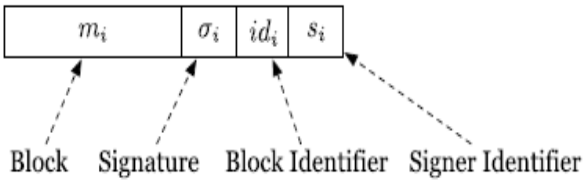
IV. PROPOSED APPROACH

In this paper, a novel public auditing mechanism is proposed for the integrity of shared data with efficient user revocation in mind. This approach includes six algorithms: KeyGen, ReKey, SigGen, ReSign, ProofGenand ProofVerify. In KeyGen, users generate their own private or public key pairs. In this user as an original user is considered, who is creator of user list and shared data. Rekey is a resigning key created by the cloud. The resigning key sends to the user. In SigGen is used to own private key and all the group members in public keys, user is capable to calculate ring signatures on blocks in shared data. ReSigna user is revoked from the group, after the re-signing, the original user removes user from User List (UL) and signs the new UL. ProofGenis operated by a public verifier and the cloud server together to interactively create a proof of possession of shared data in cloud. In ProofVerify, the public verifier audits the integrity of Shared data by verifying the proof.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016



A. Advantages

- In this scheme, any user in the group can store and share data files with others by the cloud.
- User revocation can be achieved without updating the private keys of the remaining users.
- The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.

V. CONCLUSION

In this paper, a new public auditing mechanism for shared data with efficient user revocation is proposed in the cloud. When a user in the group is revoked, a semi-trusted cloud is allowed to re-sign blocks that were signed by the revoked user with proxy re-signatures. This mechanism results shows that the cloud can increase the efficiency of user revocation and the existing users in group may save a communication resources and significant amount of computation during user revocation.

REFERENCES

[1] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud"IEEE transactions on services computing, vol. 8, no. 1, January/February 2015.

[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] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in the Proceedings of ASIACRYPT 2001. Springer- Verlag, 2001, pp. 514–532.

[5] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Stroage Systems," in the Proceedings of ACM CCSW 2010, 2010, pp. 31–42.

[6] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in the Proceedings of ACM CCS 2009, 2009, pp. 213–222.

[7] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems (TPDS), vol. 24, no. 6, pp. 1182–1191, 2013.

[8] 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.

[9] 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 2012, 2012, pp. 265–280.

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

[11]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.

[12]David Cash, Alptekin Kupcu, Daniel Wichs,"Dynamic Proofs of Retrievability via Oblivious RAM" inInternational Association for Cryptologic Research, 2013.

[13]Bo Chen, Reza Curtmola, Giuseppe Ateniese, Randal Burns,"Remote Data Checking for Network Coding-based Distributed Storage Systems"proceeding in the year 2001.