Public Auditing Using Proxy Resignatures on Efficient User Revocation in the Cloud

Bheemireddy Harshitha Reddy[1], M.N. Bhaskar [2]

M.Tech, Dept. of CSE, Shri Shiridi Sai Institute of Science and Engineering, Affiliated to JNTUA, AP, India[1]

Assistant Professor, Dept. of CSE, Shri Shiridi Sai Institute of Science and Engineering, Affiliated to JNTUA,

AP, India[2]

ABSTRACT: With information storage and sharing offerings within the cloud, customers can effectively regulate and share information as a bunch. To make sure shared data integrity will also be confirmed publicly, users within the group ought to compute signatures on the entire blocks in shared information. Specific blocks in shared knowledge are quite often signed by using special customers due to information adjustments carried out through different customers. For protection causes, once a consumer is revoked from the team, the blocks which have been earlier signed through this revoked user need to be re-signed through an existing person. The easy method, which enables an current consumer to down load the corresponding part of shared data and re-signal it in the course of person revocation, is inefficient as a result of the giant dimension of shared information within the cloud. In this paper, we propose 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, we allow the cloud to resign 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, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously.

KEYWORDS: Cloud computing, Data integrity, Public auditing, User revocation

I. INTRODUCTION

A. CLOUD COMPUTING

Cloud computing is nothing but internet based computing which made revolution in today's world. It is the biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider.The advantage of cloud is cost savings. The prime disadvantage is security. The cloud computing security contains to a set of policies, technology & controls deployed to protect data, application & the associated infrastructure of cloud computing.

Some security and privacy issues that need to be considered. The only thing was the cloud computing lacks regarding the issues of data integrity, data privacy, and data accessed by unauthorised members.

B. DATA INTEGRITY

Integrity is nothing but consistency. It is a major factor that affects on the performance of the cloud. Data integrity contains protocols for writing of the data in a reliable manner to the persistent data storages which can be retrieved in the same format without any changes later. Maintaining integrity of shared data is quite difficult task. Numbers of mechanisms have been proposed to protect integrity of data. Concept of attaching Signature to each block of data is

used in these mechanisms. Data Integrity is most important of all the security issues in cloud data storages as it ensures completeness of data as well as that the data is correct, accessible, consistent and of high quality.

Data model consist of three types of integrity constraints:

Entity integrity

Referential integrity
Domain integrity

C. PUBLIC DATA AUDITING IN CLOUD

On cloud we can able to store data as a group and share it or modify it within a group. In cloud data storage contains two entities as cloud user (group members) and cloud service provider/ cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud and share it within a group. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done by unauthenticated member. To achieve security data auditing concept is come into picture. This can be achieved in 2 ways as without trusted third party With trusted third party based on who does the verification.

In cloud computing architecture data is stored centrally and managing this centralised data and providing security to it is very difficult task. TPA is used in this situation. The reliability is increased as data is handled by TPA but data integrity is not achieved. TPA uses encryption to encrypt the contents of the file. It checks data integrity but there is threat of TPA itself leaks user's data.

Researchers of specify way to achieve storage correctness without Trusted Third Party (TTP). They achieve this by using secure key management, Flexible access right managements and light weight integrity verification process for checking the unauthorised change in the original data without requesting a local copy of the data.

II. LITERATURE REVIEW

A. TECHNIQUES USED IN PUBLIC AUDITING ON CLOUD
There are some different techniques which used in different auditing mechanisms. This section introduce some the techniques like MAC, HLA etc. which are used for different purposes like data authentication, data integrity in auditing schemes on cloud.

1. MAC Based Solution

This technique used for data authentication. In this mechanism user upload data blocks with MAC and Cloud provider provides Secret key SK to TPA. Here TPA's task is to retrieve data blocks randomly and MAC uses SK to check correctness of data. Limitations of this technique are:
Online burden to users due to limited use (i.e. Bounded usage) and stateful verification. Complexity in communication and computation Maintaining and updating TPA states is difficult. User need to download all the data to recompute MAC and republish it on CS. This technique only supports for static data.

2. HLA Based Solution

This technique performs auditing without retrieving data block. HLA is nothing but unforgettable verification meta data that authenticate. It checks integrity of data block by authenticating it in linear combination of the individual

blocks. This technique allows efficient data auditing and consuming only constant bandwidth, but its time consuming as it uses linear combination for authentication.

3. Using Virtual Machine

Abhishek Mohta proposed Virtual machines concept which use in case of Software as a Service (SaaS) model of the cloud computing. In this mechanism as shown in Fig when user request CSP for service CSP authenticate the client and provide a virtual machine by means of Software as a service. Virtual Machine (VM) uses RSA algorithm for cryptography, where client encrypt and de-crypt the file. A SHA-512 algorithm is also used for making the message digest and check the integrity of data. This also helps in avoiding unauthorised access and providing privacy and consistency. Limitation to this technique is it is useful only for SaaS model.

4. Using EAP

As mentioned by S. Marium Extensible authentication protocol (EAP) can also use through three ways hand shake with RSA. Using EAP they proposed identity based signature for hierarchical architecture. They provide an
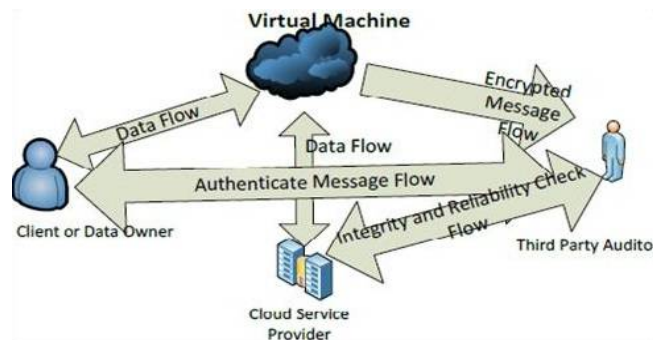

Fig. 1 Architecture of Cloud Data Storage Service using Virtual Machine

authentication protocol for cloud computing (APCC). As compare to SSL authentication protocol APCC is more lightweight and efficient. It also used Challenge – handshake authentication protocol (CHAP) for authentication.

5. Using Automatic Protocol Blocker

Balkrishna proposed efficient Automatic Protocol Blocker technique for error correction which checks data storage correctness. Kiran Kumar proposed automatic protocol blocker to avoid unauthorized access. When an unauthorized user access user data, a small application runs which monitors user inputs, It matches the user input, if it is matched then it allow user to access the data otherwise it will block protocol automatically. It contains five algorithms as keygen, SinGen, GenProof, VerifyProof, Protocol Verifier. Protocol Verifier is used by CS. It contains three phases as Setup, Audit and Pblock.

6. Random Masking Technique

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).

B. DIFFERENT PUBLIC AUDITING MECHANISMS ON CLOUD

This section consist different mechanisms, different system proposed by authors which are used for auditing in cloud computing.

1. Compact Proofs of Retrievability

Hovav Shacham and Brent Watersy[9] proposed proof-of-retrievability system. In this system, data storage center must prove to a verier that he is actually storing all of a client's data. They have proposed two homomorphic authenticators the first, based on PRFs, gives a proof-of-retrievability scheme secure in the standard model. The second, based on BLS signatures [8], gives a proof -of-retrievability scheme with public variability secure in the random oracle model. Frameworks explained by them allow to argue about the systems unforgeability, extractability, and retrievability with these three parts based respectively on cryptographic, combinatorial, and coding-theoretical techniques.

2 Provable Data Possession at Untrusted Stores

Giuseppe Ateniese et all introduce a model which based on provable data possession (PDP). This is used for verifying that server is processing the original data without retrieving it. In this model probablistic proof of possession is generated by sampling random sets of blocks from the server.This helps to reduces I/O cost.
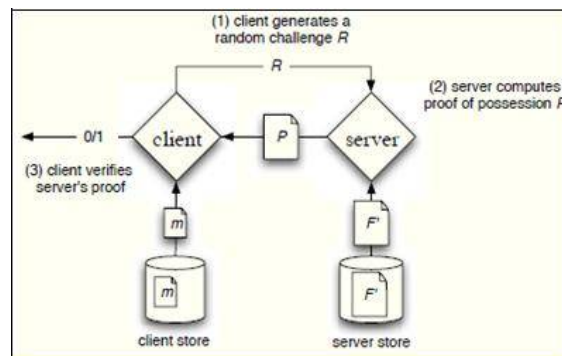

Fig.2 Provable Data Possession at Untrusted Stores

As shown in Fig.2 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. DP model for remote data checking supports large data sets in widely-distributed storage systems. A key component of this mechanism is the homomorphic verifiable tags.

3. Privacy Preserving Public Auditing

Cong Wang Proposed Privacy Preserving Public Auditing technique. In this technique public auditing allows TPA along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows TPA to do auditing without requesting data. Here TPA can audit the data by maintaining cloud data privacy. They have used the homomorphic linear authenticator and random masking 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 prevent the users from fear of the outsourced data leakage.

This mechanism is based on 4 algorithms:

Keygen: It is a key generation algorithm for setup the scheme.

Singen: It is used by the user to generate verification metadata which may consist of digital signature.
Gen Proof: It is used by CS to generate a proof of data storage correctness.
Verify proof: Used by TPA to audit the proofs

4.   LT Codes-based Secure and Reliable Cloud Storage Service

    Ning Cao et all explore the problem of secure and reliable cloud storage with the efficiency consideration of both data repair and data retrieval, and design a LT codes-based cloud storage service (LTCS)[12]. LTCS provides efficient data retrieval for data users by utilizing the fast Belief Propagation decoding algorithm, and releases the data owner from the burden of being online by enabling public data integrity check and employing exact repair. LTCS is much faster data retrieval than the erasure codes-based solutions. It introduces less storage cost, much faster data retrieval, and comparable communication cost comparing to network coding-based storage services.

    5. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud

    Boyang Wang et all proposed Oruta, the first privacy preserving public auditing mechanism for shared data in the cloud. They have used ring signatures to construct homomorphic authenticators,
so the TPA is able to audit the integrity of shared data, without retrieving the entire data. They have used HARS and its properties for constructing Oruta.

III. 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 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.
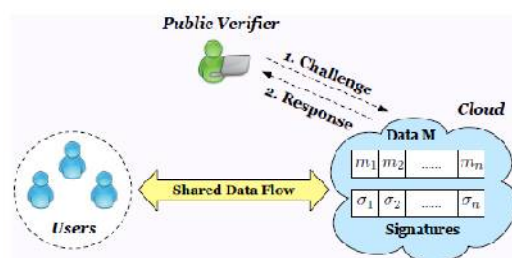

Fig 3: SYSTEM ARCHITECTURE

User Module:
Registration:
In this module each user registers his user details for using files. Only registered user can able to login in cloud server.

File Upload:
In this module user upload a block of files in the cloud with encryption by using his secret key. This ensures the files to be protected from unauthorized user.

Download:
This module allows the user to download the file using his secret key to decrypt the downloaded data of blocked user and verify the data and reupload the block of file into cloud server with encryption .This ensure the files to be protected from unauthorized user.

Reupload:
This module allow the user to reupload the downloaded files of blocked user
into cloud server with resign the files(i.e) the files is uploaded with new signature like new secret with encryption to protected the data from unauthorized user.

Unblock Module:
This module allows the user to unblock his user account by answering his security question regarding to answer that provided by his at the time of registration. Once the answer is matched to the answer of registration time answer then only account will be unlocked.

Auditor Module:
File Verification module:
The public verifier is able to correctly check the integrity of shared data. 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.

Files View:
In this module public auditor view the all details of upload, download, blocked user, reupload.

Admin Module:
View Files:
In this module public auditor view the all details of upload, download, blocked user, reupload.

Block User:
In this module admin block the misbehave user account to protect the integrity of shared data

IV. CONCLUSION

Cloud computing is world's biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. It increases the ease of usage by giving access through any kind of internet connection. As every coin has two sides it also has some drawbacks. Privacy security is a main issue for cloud storage. To ensure that the risks of privacy have been mitigated a variety of techniques that may be used in order to achieve privacy. This paper showcase some privacy techniques and different methods for overcoming the issues in privacy on untrusted data stores in cloud computing. There are still some approaches which are not covered in this paper. This paper categories the methodologies in the literature as encryption based methods, access control based mechanisms, query integrity/ keyword search schemes, and auditability schemes.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing".

[2] 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.

[3] 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.

[4] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012

[5] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012.

[6] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, "Automatic   Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing", International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012

[7] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012

[8] 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

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

[10] 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.

[11] 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.