Preserving Privacy by Public Integrity Auditing Of Shared Cloud Data

S. Radhika, PG Scholar
Department of Computer Science and Engineering
Sri Vidya College of Engineering & Technology
Virudhunagar.
Mail id: radhika.mecse@gmail.com

M.Sukumar M.Tech., Assistant professor
Department of Computer Science and Engineering
Sri Vidya College of Engineering & Technology
Virudhunagar.
Mail id : msukumar.btech@gmail.com

Abstract—Now a days it is a growing trend to outsource storage .Cloud computing is a network based computing through Internet. Cloud services are used for storing user data in the cloud and also shares data to multiple users. Recently the main problems in cloud are data integrity, data privacy and data access by unauthorised users. Trusted Third Party (TTP) is used to store and share data in cloud. Third Party Auditor (TPA) will perform verifying integrity and identity of the signer on each block. Here, privacy preserving mechanism supports public integrity auditing for shared cloud data. This public integrity auditing scheme based on vector commitment and verifier local revocation group signature. This scheme supports the public validation and efficient user revocation and efficiency, confidently, countability and traceability properties are involved.

Keywords— Cloud computing, Data Integrity, Public Auditing, GroupSignature,UserRevocation.

I. Introduction

[A] Cloud Computing

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. A cloud infrastructure provides a framework to manage scalable, reliable, on-demand access to applications. A cloud is the "invisible" backend to many of our mobile applications. A model of computation and data storage based on "pay as you go" access to "unlimited" remote data center capabilities. Several large Web companies (such as Amazon and Google) are now exploiting the fact that they have data storage capacity that can be hired out to others. This approach, known as cloud storage allows data stored remotely to be temporarily fetched on personal computers, mobile phones or other Internet-attached devices. Amazon's Elastic Compute Cloud (EC^2) and Simple Storage Solution (S3) are good examples.

The fundamental advantage of cloud computing are cost, easy to learn and use, flexibility, Maintenance. The main disadvantage of cloud are security, wireless connection, performance and reliability. Cloud Service Providers (CSP) are used to providing services to users. Some CSP's are Amazon Web Services (AWS), Elastic Compute Cloud (EC2), Simple Storage Service (S3), and Virtual Private Cloud (VPC) , Salesforce.com / Sales Cloud 2 (CRM), Service Cloud 2 (Support), Force.com (Development Platform), Chatter (Collaboration), Google Apps (AppEngine), VMware – vSphere (Virtualization).

[B] Data integrity

Integrity is nothing but reliability. Data Integrity is a major part that affects on the performance of the cloud. Data integrity means data should be correctly stored on the cloud storage server without any adjustment and if any violations i.e. if the data is get lost, altered or compromised can be detected. But integrity of shared data maintenance is quite difficult task. Numbers of mechanisms have been planned to protect integrity of data. The Main 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, available, consistent and of high quality.

Data model consist of three types of integrity constraints:

- Entity integrity
- Domain integrity
- Referential integrity

[C] Public Data Auditing in Cloud

On cloud we know how to 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 and Third party auditor (TPA). **Cloud user** is a person or participants 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** is important actor of cloud architecture.CSP will provide services to cloud user. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will find the verification that cloud data is secure or is stored as it is. No data loss or modification is done by unauthenticated member. **Third party auditor** (TPA) has more capabilities than the user and checks the integrity of data for the user and his audit reports helps the users in evaluating the risk.

[D] THIRD PARTY AUDITOR

The Third party auditor is a kind of supervisor. The Third Party Auditor who has resources and knowledge that a user does not have and check the integrity that is difficult for users to check. The auditors can identify with the threats and they know best practices. The audit reports helps the user to evaluate the risk of their services. It also helps the cloud service provider in improving their cloud platform.

Functions of Third Party Auditor (TPA) in cloud environment should take following functionalities into consideration:
1) No data leakage or data learning
2) Audit without downloading
3) Integrity Verification
4) High Performance
5) Scalability
6) Dynamic data operation support
7) Batch Auditing

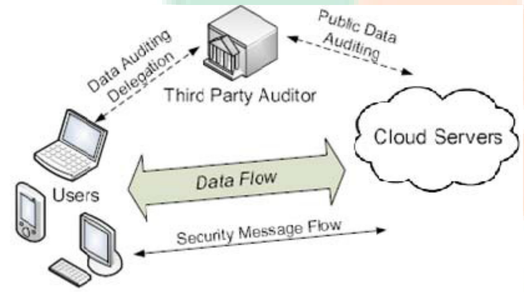

Fig.1 Architecture of Cloud Data Storage Service

II Problem Statement

2.1 System Model

In this cloud storage model involves three parties: the cloud server, a group of users and a public verifier as shown in fig 2.1. There are two types of users in a group: the innovative user and a number of group users. The innovative user initially creates shared data in the cloud, and shares it with group users. Both the innovative user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata are both stored in the cloud server. A public verifier, such as a third party auditor providing authority data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of data stored in the cloud. When a public verifier wishes to check the shared data, it first sends an auditing challenge to the cloud. After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing verification. In actual fact, the process of public auditing is a challenge and response protocol between a public verifier and server.

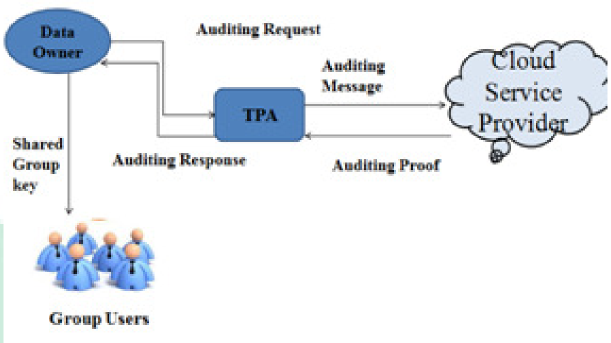

Fig 2.1 Cloud Storage System

III Methodology

To Support public auditing the four schemes are proposed.They are Keygen, Siggen, Genproof, Verify proof

□ Keygen: The keygen process implement between user and cloud server. The public key and secret key are represented as sk, pk. Using both secure key(sk) and public key (pk) these Keys are generated using Public Key Algorithm(asymmetric method).Data owner can access the cloud server .The generated key is known only to the Data owner and the cloud server.

□ Siggen: In Siggen process data file stored in cloud is pre-processed. Data owner creates metadata for the file to be stored in a Cloud. Data owner can send the metadata to the TPA after publishing in the cloud for later on audit.

□ Genproof: In Genproof process, the TPA issues an audit message to the cloud server to specify that the data has retained properly at the time of later audit. The Cloud generates proof of possession of stored data under a challenge of the TPA.

□ Verifyproof**:** In Verify proof process the TPA has to check the proof response from the cloud. This algorithm verifies the message from the cloud by using the metadata stored in TPA. The user can verify with TPA by sending the private key and public key to view whether the data is stored in cloud server.TPA send the response to the cloud server for the verification of data file.TPA matches the user's metadata with the metadata stored in cloud.TPA can validate the user to the cloud server if metadata matches.

IV Scheme construction

The public auditing can be constructed in two different phases such as Setup and Audit

4.1 Setup:

In the setup scheme, the user register with the TPA and initializes the secret keys (public key and private key) to store the data file in cloud by executing the KeyGen process. Metadata is created when data file is preprocessed using siggen. User has access rights to add some extra metadata to the cloud.

4.2 Audit:

In Audit scheme, to make sure that data file is retained properly and audit message is issued by TPA to cloud. Response message is executed by GenProof for the stored data file with the help of verification metadata.

4.3 Batch auditing**:**

With the establishment of preserving privacy by public integrity auditing, TPA simultaneously handles multiple auditing upon different users' allocation. The individual auditing of these tasks for the TPA can be monotonous and very inefficient. If the auditing allocation on distinct data files from different users is given then it is more profitable for the TPA to batch these multiple tasks together and audit at one time. So a secure batch auditing protocol for simultaneous auditing of multiple tasks can be obtained. This batch auditing reduces the computation cost on the TPA side. This is because of aggregation. Also invalid responses are identified in a fast manner than individual verification.

4.4 Data dynamics:

Data dynamic means the users can perform data insertion, data modification and deletion at any instance of time, TPA checks the integrity of outsourced data to be stored in the cloud server. Data can be inserted by Data owner in cloud server by creating metadata along with the file name to be inserted. File size should not exceed. In cloud storage, sometimes the user may need to modify file stored in the cloud, from its current value to a new one. Data owner can delete the file by viewing the metadata from table .Users cant delete file unless they are provided permission from Data owner. Data owner want to increase the size of his stored data by increasing size of file for appending. Anticipate that the most frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of files (not a single file) at one time.

V Performance Evaluation

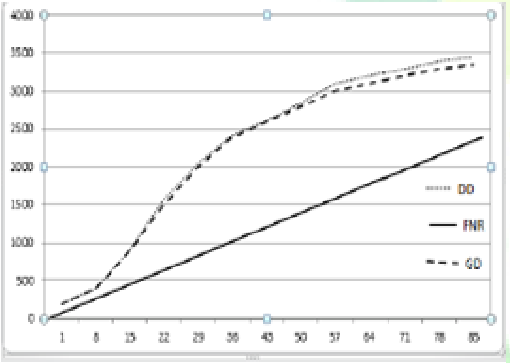

Fig 5.1 Query time cost

As shown in Figure 5.1, the **Query** time cost of this scheme is linear with the data items number q, which will take approximately 4 seconds to query about 1000 data items. However, we need to emphasize that the computation cost is at the cloud storage server side, which is very powerful compare with the Linux system running on our laptop. More over, the server does not need to run the whole **Query** algorithm every time as analyzed in the previous section. Actually, in the **Verify** algorithm, the computation overhead mostly comes from the group signature scheme. More precisely, to verify the validity of this phase, we need firstly to verify the integrity of the signature, which means that our scheme need to generate the time costed parameters such as R1, R2, and R3. Actually, the computation time cost of our scheme a constant number. Also, it is around 5 times that of the most efficient scheme

VI Related Work

Boyang Wang, Baochun Li and Hui Li are the members of IEEE explore the concept of [1] "Oruta: Privacy-Preserving Public Auditing for Shared data in the Cloud" in 2014. Privacy Preserving mechanism used in public auditing for shared data. They have also used ring signature to verify the information needed to check the integrity of shared data. The result is effectiveness and efficiency. [2] "Group Signature with Verifier Local Revocation" in Group signature construct a Short Group Signature Scheme that supports VLR (Verifier-Local Revocation).Here this model, revocation messages are only sent to signature verifiers. Strong Diffie-Hellman assumption and the Decision Linear assumption are based in this group signature. The difficulty of this system are still number of problems interrelated to VLR signatures. [3] "Asymmetric Group Key Agreement" Here they construct one round ASGKA protocols, which it is used as a broadcast scheme but trusted dealer do not needed to allocate secret keys. ASGKA is not in favour of active attackers. [4] "Proof of Retrievability Theory & Implementation" .They proposed a theoretical framework for the design of POR. Here framework are improved and the previously proposed POR construction of Juels-Kaliski and Shacham Waters, and also sheds light.Here new framework used to simplified and improved JK and SW. [5] "New Publicly Verifiable Databases with efficient updates" proposed the smart framework to construct efficient Verifiable database (VDB) which support public verifiability from new primitive named vector commitment. In this system, VDB framework from vector commitment is exposed to VDB so it's called as Forward Automatic Updates (FAU) attack. They can achieve the desired security properties. [6] "Public Auditing for Shared Data with Efficient User Revocation in the Cloud" They proposed the novel public auditing mechanism for the public integrity of shared data with efficient group user. They used Proxy re-signatures that allow the cloud to resign blocks on behalf of existing users during user revocation. So the existing users need not to download and resign the blocks by themselves. Finally their mechanism can significantly improve the efficiency of group user revocation. [7] "Short Signatures from the Weil Pairing" ,construct a short signature scheme based on the Diffie-Hellman assumption and hyper-elliptic curves. they used Diffie-Hellman to solve the problem that reduces the signature of length. [8] "Efficient Algorithm for Pairing –Based Cryptosystems" implement the new algorithm in cryptosystem based on the Tate pairing. This algorithm not only used for pairing evaluation process but also used as elliptic curve scalar multiplication and square root extraction. [9] "Collision –

Free Accumulators and Fail-stop signature schemes without Trees*" they construct a fail-stop signature scheme. [10] "Short Group Signature" construct Short Group Signature Scheme. Here security of their group signature is based on the stong Diffie-Hellman assumption and a bilinear groups are called decision linear assumption. From this they can prove security of their system,in the random oracle model. [11] "Fully Homomorphic encryption using ideal lattices" they construct fully homomorphic encryption scheme using ideal lattices.their results are divided into three steps are construct encryption scheme ,ideal lattices and decryption scheme.

Conclusion

Cloud computing provides many benefits to their abuser but security is most important issues in cloud computing. As user store their data to cloud data centers but as user does not recognize the exact location of their data so integrity of data is especially important. To check the integrity of data there are many solutions offered. One of solution is to get the support of a third party auditor. Different authors provide different solutions for implementing third party auditor. Each scheme have its delicate merits and demerits.

The system to realize secure and efficient integrity auditing of data for share dynamic data with multi-user adaptation. In this paper, the concept of authorized data deduplication was proposed to achieve the data security by including differential constitutional rights of users in the duplicate check. The system vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with group user revocation are used to get the auditing remote data integrity.

ACKNOWLEDGMENT

I would like to thank my supervisor for his most support and encouragement. I sincerely thank to my parents and friends, who provide the advice and financial support.

REFERENCES

[1]M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee,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, April 2010

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

[3]Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing",Proc. 14th European Conf. Research in Computer Security (ESORICS09), pp. 355-370, 2009.

[4]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.

[5]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.

[6]Boyang Wang, Baochun Li, Panda: Public auditing for Shared Data with Efficient User Revocation in the Cloud, 2014.

[7]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.

[8]H. Wang, "Proxy Provable Data Possession in Public Clouds", IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, Oct.-Dec. 2013.

[9]C. Wang, Q. Wang, K. Ren ,"Privacy-Preserving Public Auditing for Secure Cloud Storage Auditing", IEEE transaction on computer, 2013.

[10]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.

[11] Designated-Verifier Provable Data Possession in Public Cloud Storage. International Journal of Security and Its Applications Vol.7, No.6 (2013), pp.11-20.

[12]Rovira i Virgili Univ., Tarragona,et.al, EfficientRemote Data Possession Checking in Critical Information Infrastructures.

[13] Giuseppe Ateniese et.al ,"Scalable and Efficient Provable Data Possession".

[14] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma, Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation, IEEE 2015.

[15] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. of ACM CCS*,Illinois, USA, Nov. 2009, pp. 213–222.