Review on Public Auditing for Cloud Storage using Third Party Auditors

Priyanka Bhor
M. Tech Student
Computer Science and Technology
Usha Mittal Institute of Technology
SNDT University

Sumedh Pundkar
Assistant Professor
Computer Science and Technology
Usha Mittal Institute of Technology
SNDT University

ABSTRACT

Cloud computing is recent blooming technology which provides various services like storage, platform, applications etc. through internet. In cloud computing, data owner hosts (stores) their data on cloud servers and data users access those data through cloud servers any time and from any place. This leads to data outsourcing on cloud in high amount. But because of vast amount of data on cloud, it increases security challenges again on data integrity, authenticity and confidentiality in the form of data hacking. Here data owner has no idea about the whereabouts of storage locations. To check for the data loss, data owner has to be online continuously and monitor the data all the time; hence increases the overhead on data owner which owner surely wants to avoid because that's the reason of using cloud services. So the strong need of security mechanism, introduces the concept of Third Party Auditor (TPA) to the world. Cloud's public audit ability lets third party auditor (TPA) checks for data integrity. Here in this paper, various issues and challenges come across when data is stored on cloud, has been analyzed. Various papers discussed here, describes various techniques for secure cloud storage to provide privacy preserving public auditing.

Keywords

Cloud Computing, Cloud Storage, Public Auditing, Third Party Auditors, Encryption, Integrity.

1. INTRODUCTION

Now-a-days cloud computing or on-demand computing is receiving progressive attention from both academic as well as industrial community. But a major hurdle to the adoption of cloud-based services is security. The cloud computing derive, characteristics pertinent to information security problems from traditional computing platforms. Since cloud is distributed in nature, it enables many new types of attacks. There are several major problems that the cloud faces such as Replace Attack, Forge Attack and Replay Attack. Cloud users, most prominently, at the enterprise and government level, are anxious about losing control of their data once it is placed in the cloud. The abstractness of cloud storage makes it difficult for consumers to feel sufficiently satisfactory that their data is well guarded by cloud service providers (CSP). Encryption could relieve this issue. However, if someone wants to manipulate their encrypted data in the cloud, the secret key to decrypt their own data must be shared with the CSP. This sort of overcomes the idea of a secret key. Allotting this key would allow the current CSP (or future CSP if the service changes hands) access to data. To resolve this problem Asymmetric Key encryption Algorithm can be used.

The main objective of Asymmetric Key encryption Algorithm here is to achieve the integrity in cloud computing to enhance the security features of untrusted systems or applications that stores and handles sensitive data. Asymmetric Key encryption method allows specific types of computations to be fulfilled on cipher text and obtain result means no need of reading original data which when decrypted, agrees the result of operations performed on the plaintext. The concept of third party auditor (TPA) can be introduced to audit outsourced data without demanding local copy of user, no additional online burden for the cloud owner, server. ElGamal encryption can be defined with the help of any cyclic group G. Its security depends upon the criticality of a certain problem in G which is related to computing discrete logarithms. A TPA has expertise and capabilities, hence, can do a more efficient work and convince both cloud service providers and owners.

2. RELATED WORK

2.1 An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Kan Yang ,Xiaohua Jia ,2012.

Due to outsourcing of data on cloud server for data access by users, there is increase in challenges which required checking data integrity of cloud storage. In this paper, for dynamic data storage, an efficient privacy preserving auditing protocol is proposed. Here data dynamic operations are checked in random oracle model, which gives positive result. Without using any trusted third party, this protocol supports both, multiple owners as well as multiple clouds [7].

2.2 PORs: Proofs of Retrievability for Large Files

Ari Juels Burton, S. Kaliski Jr.

This paper, proposed a mechanism which enables backup service to generate concise proof so that authenticated user can retrieve a target file. This concept is similar to proof of knowledge (POK), but it is produced to manage larger files in semi trusted environment. The use of cryptographic technique, helps to ensure, integrity and privacy of the retrieved file. The important goal of POR is, verifier doesn't have to download and check the file for integrity and privacy purpose. It shows whether file is retrievable or not within certain time [3].

2.3 HAIL: A High Availability and Integrity layer per cloud storage

Kevin D. Bowers, Ari Juels , Alina Opera.

This paper introduces the concept of HAIL: A High Availability and Integrity layer per cloud storage, where, for distributed system, a set of servers allows to check that stored file is intact and retrievable. HAIL cryptographically verifies files and reactively reallocates the shared files. This paper shows how HAIL improves files security using tools like PORs [5].

2.4 Cooperative Provable Data Possession for Integrity verification in multi cloud storage

Yan Zhu, Hongxin Hu, Gail-joon ahn and Mengyang Yu.

Provable Data Possession (PDP) is a technique, designed for distributed data storage to support service scalability and data migration, when client's data has been stored on various clouds. Here PDP is introduced based on homomorphic verifier response and index hierarchy which supports dynamic scalability on multiple clouds [1].

2.5 Secure and Efficient Privacy Preserving Public Auditing Scheme for cloud Storage

Dr. G. K. Kamalam , B.Neka , E.Jamunadevi

To maintain integrity and privacy of the data stored on cloud, effective and secure security methods are highly recommended. Thus paper provides privacy preserving public auditing protocols that supports public auditing and privacy of data. It also focuses on improvement of security mechanism of cloud storage service [8].

2.6 Provable Data Possession at Untrusted Stores

Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song

To verify the data without retrieving the original file, this paper provides constant amount of metadata to verify the proof. It minimizes the network communication by transmitting constant amount of data [4].

2.7 Privacy Preserving Public Auditing Using TPA for Secure Cloud Storage.

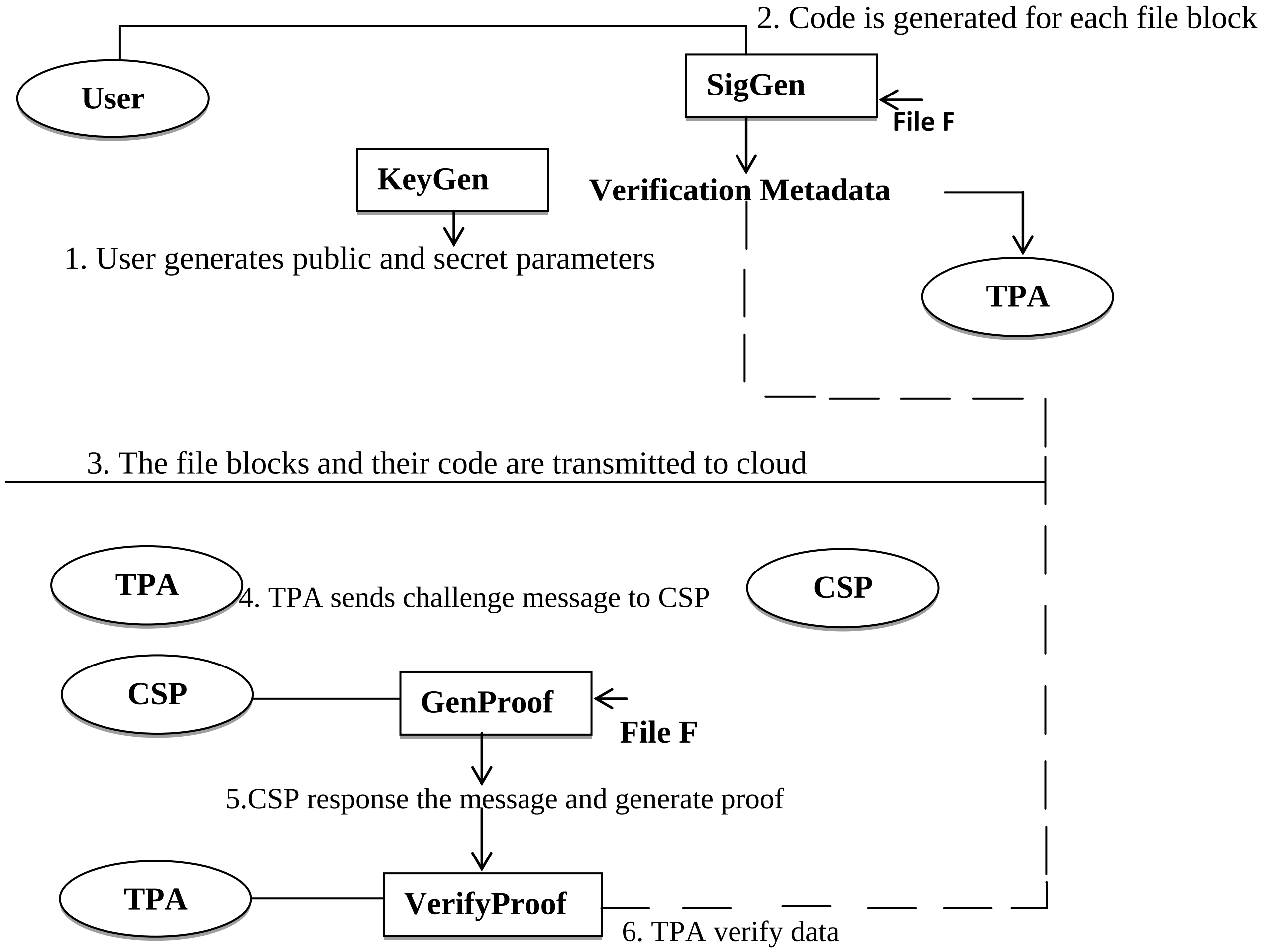
Jyoti R. Bolannavas.

To check the data integrity on cloud storage, public auditing is done using the concept of TPA. It purpose secure cloud storage system which supports privacy preserving public auditing. Here TPA can perform audit for multiple users simultaneously [6].

3. PROPOSED SYSTEM

To properly monitor confidentiality and integrity of the stored data in proposed system, TPA will be fully automated. To achieve a privacy-preserving public auditing system, TPA integrates the data using public key based Asymmetric Key encryption technique. For data transmission security, the use of ELGAMAL algorithm is used for data encryption in cloud computing. Data before transmission will be encrypted, hence even if the data is stolen; there is no corresponding key which will restore that encrypted data. Only the authorized user knows the key, others like, cloud servers or TPAs do not know the key. Also, for the purpose of the properties of encryption, the cloud can directly work on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. For data integrity checking by TPA, data owner apply hashing using modified SHA 256 algorithm and send secret hash key to TPA for data verification. User's privacy is protected because user's files are encrypted as well as hashed in cloud storage.

4. SYSTEM FLOW


2. Code is generated for each file block
User
SigGen
File F
KeyGen
Verification Metadata
1. User generates public and secret parameters
TPA
3. The file blocks and their code are transmitted to cloud
TPA
4. TPA sends challenge message to CSP
CSP
CSP
GenProof
File F
5.CSP response the message and generate proof
TPA
VerifyProof
6. TPA verify data

Account Registration

The account registration function shall allow users to create secure account. The account will track user's name password, mobile no and email-address. Each user will be provided his/her own space on cloud.

Account login

The account login function shall allow account members to enter their username and password. Once verified user will be able to access account history, their data on server and update their account information.

Encrypt

The encrypt function shall offer users, the ability to encrypt their data before storing it on cloud storage. The owner will generate secret hash key and secret tag key.

Tag Generation

The tag generation function shall offer the users the ability to generate a tag for the encrypted data stored on the cloud and pass it on the TPA.

Decrypt /Download

The decrypt function shall offer the users the ability to decrypt their data while retrieving it from the cloud.

User Login

The user login function shall give users the store address, telephone numbers, email address, and its location.

TPA Login

TPA Login function shall offer the user to login with his user name and password and verify the data integrity with the help of the secret tag key send by the owner.

Share file

The share file function shall give authorized user access to the data store on cloud server.

Account Logout

The account logout function shall allow account members to exit their account for security purposes.

5. CONCLUSION AND FUTURE SCOPE

In this paper, a privacy preserving public auditing system for data storage security in cloud computing is proposed. Public auditability is to allow Third party auditor to verify the correctness of the cloud data whenever required without retrieving a copy of the whole original data or introducing additional online burden to the cloud user. It protects the data privacy against the auditors as well by combining the cryptography method such as RSA and ELGAMAL. The goal of this encryption scheme is to ensure confidentiality of data in communication and storage process. By moving the computing loads of auditing from the auditor to the server, Third Party Storage Auditing Service incurs less communication cost and less computation cost of the auditor which greatly enhances the auditing performance and can be applied to large scale cloud storage systems. These encryption schemes are not supported everywhere and there characteristics must be taken into account while using them.

6. ACKNOWLEDGMENTS

Foremost, I would like to express my sincere gratitude to the Head of Department (Computer Science and Technology) and my guide Prof. Sumedh Pundkar for his valuable guidance and continuous support during this paper; his patience, motivation, enthusiasm and immense knowledge. Their direction and mentoring helped us to successfully work on this paper. My sincere gratitude to Dr. Sanjay Pawar, Principal (UMIT) for his valuable encouragement and insightful comments.

7. REFERENCES

[1] Zhu,Y.,Hu, H.,Ahn, G.,Yu, M.: Cooperative provable data possession for integrity verification in multi-cloud storage. IEEE Trans. Parallel Distrib. Syst. 23(12) 2231–2244 (2012)

[2] Yan Zhua,b, Hongxin Huc, Gail-Joon Ahnc, Stephen S. Yauc. ―Efficient audit service outsourcing for data integrity in clouds‖. In ―The Journal of Systems and Software 85 (2012) 1083– 1095

[3] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability forlarge files," in *Proc. 14th ACM Conf. Comput. Commun.Secur*, 2007,pp. 584–597.

[4] G.Ateniese et al., ―Provable Data Possession at Untrusted Stores,‖ Proc. ACM CCS ‗07, Oct. 2007, pp. 598–609.

[5] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability andintegrity layer for cloud storage," in *Proc. 16th ACM Conf. ComputCommun. Secur.*, 2009, pp. 187–198.

[6] Jyoti R Bolannavar, "privacy preserving public auditing using TPA for secure cloud storage.", International Journal of Scientific Engineering and research

[7] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*,vol. 24, no. 9, pp. 1717–1726, Sep. 2013

[8] Dr. G.K. Kamalam, B. Neka, E. Jamunadevi, "Secure and Efficient Privacy Preserving Public auditing scheme for cloud Storage", International Journal of Computer Network and Security,2015