International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Privacy-Preserving Cloud Storage Auditing Scheme For DataSharing

Mrs. D. Srilatha Reddy
Computer Science and Engineering (JNTUH)
Sphoorthy Engineering College (JNTUH)
Hyderabad, India
Dyapa.sreelatha@gmail.com

G.Renuka
Computer Science and Engineering (JNTUH)
Sphoorthy Engineering College (JNTUH)
Hyderabad, India
19n81a0584renuka@gmail.com

A.Rishika
Computer science and Engineering (JNTUH)
Sphoorthy Engineering College (JNTUH)
Hyderabad, India
19n81a0568ar@gmail.com

Gattugari Sreekar
Computer Science and Engineering (JNTUH)
Sphoorthy Engineering College (JNTUH)
Hyderabad, India
19n81a05b5gatttugarisreekar@gmail.com

Abstract*—Cloud storage is one of the important storing service which helps in data sharing. To share the data conveniently and by providing high security , the previously proposed system has a cloud storage auditing scheme for data sharing, which uses a sanitizable signature(a variant of signatures that allow a single, and signer-defined, sanitizer to modify signed messages in a controlled way without invalidating the respective signature) to hide sensitive information which provides security for the data that is stored in the cloud storage but it needs a secure channel to provide that security for authorized access to the data and also any third party can have access to the data which may cause the data owner to lose their information. The System has some security issues related to unauthorized access to the data , where anyone can access the data. To prevent that, the newly proposed system Privacy-Preserving Cloud Storage Auditing(PP-CSA) scheme for sharing the data, where only some authorized users can have the access to the data. In addition to that, we don't need to have any secured channel between the data owner and the sanitizer, and the protocol that we use in PP-CSA is Diffie - Hellman. It is the protocol that gives a key-exchange protocol that enables two parties communicating over public channels to establish a mutual secret without it being transmitted over the Internet. Finally, more security and efficiency are provided by the PP-CSA.

Keywords: Cloud storage, Cryptography, Encryption and Decryption, Database Management , Uploading and Managing the files, Private key Management.

I. INTRODUCTION

CLOUD storage services provide relatively low-cost, scalable, and convenient access to stored data. Several organizations and clients outsource their data to the cloud server (CS) for storage. Therefore, cloud storage is widely used.But, it causes the data owner (DO) to lose direct control over its data, which may be corrupted owing to software/hardware failures or human causes.So, several cloud storage auditing schemes have been proposed.

After being stored in the CS, the DO's data can be shared with other users through some applications such as AWS, Dropbox, or iCloud, and so on. However, these data usually contain DO's privacy. For example, medical data, such as the electronic health record (EHR), may contain the patient's name, contact information, and other private information. If these data are stored in plaintext, the DO's privacy will be exposed. Therefore, under the premise of data integrity, how to protect the DO's privacy for data sharing is worth to be studied.

Usually, the DO can encrypt the shared data.However, it will cause the problem of secure key distribution. To avoid key distribution we have constructed an out-storage auditing scheme for data sharing with sensitive information hiding based on a private key. In the scheme , the data is blinded as it has sensitive information using encryption and decryption techniques. And then the blinded data is sent to the authorized user. By using the private key sent by the DO to the user of that data (file), the user can get the access to the information in that file. However , establishing a secure channel requires additional operations, and in some cases, it is even hard to establish a secure channel. Therefore, it is necessary to study a privacy-preserving cloud storage auditing (PP-CSA) scheme for authorized data sharing without a secure channel.

This scheme can protect the shared data's privacy. However, anyone can access the shared data, which will lead to

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

unauthorized access to the data and further damage to the interests of the DO. In addition, to sanitize the auditing authenticator, the sanitizer should get the secret value sent by the DO, which is the key to realizing the sanitization operation. In this scheme, it needs a secure channel between the DO and the sanitizer to sanitize the auditing authenticator, where the DO sends the secret value to the sanitizer. However, establishing a secure channel requires additional operations, and in some cases, it is even hard to establish a secure channel. Therefore, it is necessary to study a privacy-preserving cloud storage auditing (PP-CSA) scheme for authorized data sharing without a secure channel.

Contributions: This article studies secure cloud storage auditing schemes for data sharing and the following is the summary of the contributions.

1) We propose a PP-CSA scheme for data sharing, where only the authorized user can access the data.

2) We use the AES encryption algorithm when the DO sends auditing authenticators to the sanitizer. And there is no need to establish a secure channel between the DO and the sanitizer in PP-CSA.

3) We give the security analysis, which proves that PP-CSA is a secure cloud storage auditing scheme with authorized access. Moreover, the experiment results show that PP- CSA achieves desirable efficiency.

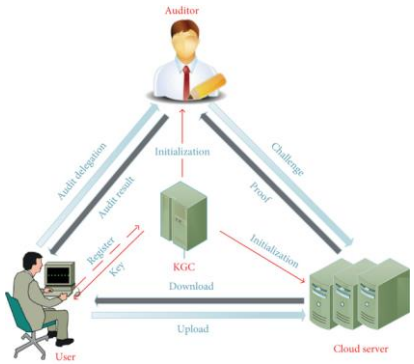


Fig.1: Cloud Auditing Scheme

To maintain privacy and provide security, no details of DO or User are leaked in case of misusing of that information. And also the sensitive information in the files is hidden well enough that only DO knows the data and the User who hot access.

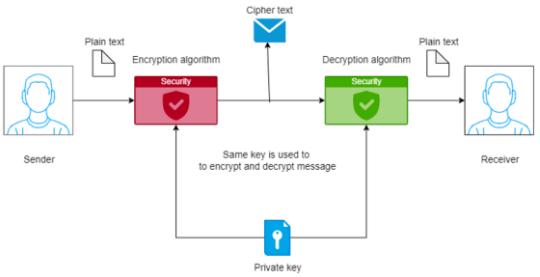


Fig.2: Encryption and Decryption

I. Related Work

To verify the integrity of the outsourced data, several cloud storage auditing schemes have been proposed one after another.

A. Cloud Auditing Scheme

As we use cloud services a lot and one of the main services that cloud provides is storing and managing the data, and also providing security to that data.Data sharing is one important service provided by cloud storage. Hence, we proposed a system to provide secure data sharing.

So, we proposed a system where the integrity of the auditing scheme is more accurate and effective.Furthermore, for cloud storage auditing, the security of the key is becoming increasingly important.

After that, some cloud storage auditing schemes with privacy-preserving have been proposed. We proposed a privacy-preserving public cloud storage auditing scheme, which can prevent the third-party auditor (TPA) from obtaining private data.Hence, we proposed a lightweight cloud storage auditing scheme based on a third-party medium, which assists the DO to generate authenticators while protecting data privacy.

In this scheme, the User's identity privacy can be protected through a ring signature. However, cannot track the User's real identity. They only need to provide simple information about them as required for login.

B. Encryption and Decryption

We proposed a privacy-preserving cloud storage auditing scheme, which uses a security out-sourcing algorithm to assist the DO to generate authenticators. And also included a secure

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

encryption hash algorithm, which uses this hash algorithm to split and encrypt data. The above-mentioned schemes have complex certificate management problems because they are based on public key infrastructure.

Encryption and Decryption of the files and data that is being uploaded by the DO in the cloud will be managed by the encryption and decryption algorithms.The encrypted file is uploaded to the cloud, and using the private key the user can have access to the information in the file.

This scheme relies on the private key generation by the KGC and also the cloud auditing scheme for data sharing.This scheme is really efficient and effective for data sharing with our involving any third-party auditors who can sometimes be a threat to our details and information.

III.SYSTEM MODEL AND SECURITY GOALS

A. SystemModel

The system model of PP-CSA has six different entities: the DO, the sanitizer, the user, the CS, the TPA, and the key generation center (KGC), as shown in Fig. 1.

1) DO: It is the owner of the data and authorizes the sanitizer to determine which user can access its data.

2) Sanitiser: It sanitizes the DO's data, and then transforms the corresponding authenticators. Subsequently, it sends the sanitized data and authenticators to the CS. Furthermore, it is also responsible for authorizing users to access the DO's data.

3) User: It mainly refers to the research institutions that need to access the DO's data.

4) CS: It provides enormous storage space for the DO, and verifies whether the user is authorized.

5) TPA: It is a public verifier that performs the auditing honestly and returns the auditing results to the DO.

The DO blinds the sensitive information in the data and generates authenticators. Finally, the DO sends blinded data and authenticators to the sanitizer. After receiving it, the sanitizer sanitizes the data and transfers the corresponding authenticators. Afterward, the sanitized data and corresponding authenticators are uploaded to the CS for storage and sharing. When the user needs to use the data, a sharing request is sent to the sanitizer. The sanitizer generates authorization based on the DO's warrant and sends it to the CS together with the sharing request. After passing the verification of the CS, the user can access the data.

Using the private key, a secure channel is created between the DO and the user, and the sanitizer is the third man for both the DO and user to share the secret key to the user for the file that they want to access.The sanitizer accepts the request if the user and shares the secret key through the mail he is registered with and then the user uses the secret key to decrypt the data.

If any modifications are done by the user then through TPA,m the DO can know about the modifications. The hashcode technique is used to check whether any modifications are done to the file or not.Once the hashcode is changed then, we can understand that the file is modified. This whole process is under the control of TPA.

B. Security Goals

1. *Correctness:*

a) Auditing correctness: If the data stored in the CS is complete, the generated proof can be verified by the TPA.

b) Authorization correctness: If the user's authorization is correct, the authorization can be verified by the CS.

2. Sensitive information hiding: The DO's sensitive information will not be exposed to anyone and the sensitive information of the DO's data will not be exposed to CS and users.

3. Auditing soundness: If the CS does not truly store the DO's data, it cannot pass the TPA's verification.

4. Authorisation access: Only the authorized user can access the DO's data.

5. Key Management: The keys are managed by the sanitizer to decrypt the data of the file that DO upload and is blinded using the AES algorithm.

IV. ALGORITHM

We have used the AES algorithm to encrypt and decrypt the data.
Using the private key, the user can decrypt the data.

The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of

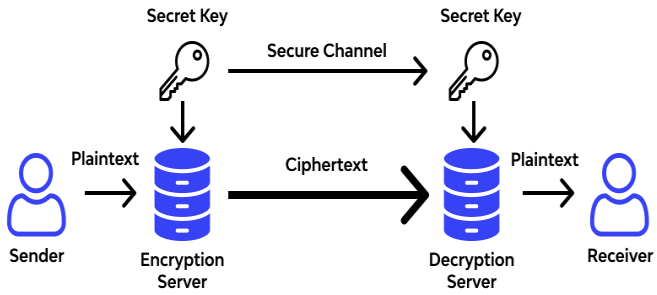
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

128, 192, and 256 bits. Since the AES algorithm is considered secure, it is the worldwide standard.

The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.

Safety aside, AES encryption is very appealing to those who work with it. Why? Because the encryption process of AES is relatively easy to understand. This allows for easy implementation, as well as really fast encryption and decryption times.
In addition, AES requires less memory than many other types of encryption (like DES), which makes it a true winner when it comes to choosing your preferred encryption method.
Finally, when an action requires an extra layer of safety, you can combine AES with various security protocols like WPA2 or even other types of encryption like SSL.

AES Algorithm Working



V. CONCLUSION

This article proposed a PP-CSA scheme for data sharing, which effectively supports sensitive information hiding. In PP-CSA, only the authorised user can access the file stored in the CS to protect the interests of the DO. Security analysis and experimental results show that the PP-CSA is secure and efficient.

REFERENCES

1. K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012

2. R. S. Bhadoria, “Security Architecture for cloud computing, Handbook of Research on Securing Cloud-Based Databases With Biometric Applications. Hershey, PA, USA: IGI Global, 2015.

3. R. Ding, Y. Xu, J. Cui, and H. Zhong, “A public auditing protocol for a cloud storage system with intrusion-resilience,” IEEE Syst. J., vol. 14, no. 1, pp. 633–644, Mar. 2020.

4. S.-C. Chang and J.-L. Wu, “A privacy-preserving cloud-based data management system with efficient revocation scheme,” Int. J. Comput. Sci.Eng., vol. 20, no. 2, pp. 190–199, 2019.

5. Neil Richards, "Why Privacy Matters", New York, NY, United States of America: Oxford University Press, 2022.

6. Bruce Schneier, "Applied Cryptography", Second Edition, John Wiley & Sons, Inc,1996.

7. Ray Rafaels, "Cloud Computing: From Beginning to End", CreateSpace Independent Publishing Platform, 2015.

8. Ricardo Puttini, Thomas Erl, and Zaigham Mahmood,"Cloud Computing: Concepts, Technology and Architecture", Pearson Publishing,2013

9. Parves Kamal, "Security of Password Hashing in Cloud", Department of Information Systems Assurance, St. Cloud State University, St. Cloud, MN, USA,2019.

10. Frank Rubin, Foreword by Randall K. Nichols, "Secret Key cryptography", Manning Publications,2022.