PP-CSA: A PRIVACY-PRESERVING CLOUD STORAGE AUDITING SCHEME FOR DATA SHARING

Ch. Rushyendra Mani[1], Sk. Mariem Siddikha[2]

[1]Assistant Professor, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

[2]PG Scholar, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

ABSTRACT

Data sharing is one important service provided by cloud storage. In order to share data conveniently and securely, Shen et al. proposed a cloud storage auditing scheme for data sharing, which uses the subitizable signature to hide sensitive information. However, it may cause unauthorized access to the data, since anyone can access the data stored on the cloud server. This article proposes a privacy-preserving cloud storage auditing (PP-CSA) scheme for data sharing, where only authorized users can access the data. Furthermore, PP-CSA adopts the Diffie–Hellman protocol to avoid the secure channel between the data owner and the sanitizer. Finally, the security analysis and the experimental results prove that the security and efficiency of PP-CSA can be accepted.

I. INTRODUCTION

Cloud storage services provide a relatively low cost, scalable, and convenient access for the 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 as 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, Shen et al. [11] constructed a cloud storage auditing scheme for data sharing with sensitive information hiding based on a sanitizable signature [12]. In the scheme [11], the medical doctor first blinds patient's sensitive information in the EHR, and generates auditing authenticators for the blinded EHR. Then, to unify the format of the blinded EHR and protect the hospital's private information, the EHR information system administrator who is the sanitizer sanitizes the blinded EHR. Meanwhile, the sanitizer transforms auditing authenticators without the medical doctor's private key and makes the cloud storage auditing be performed effectively.

Shen et al. scheme can protect the shared data's privacy. However, anyone can access the shared data, which will lead to 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 realize the sanitization operation. In Shen et al. 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, the establishment of 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 secure channel.

II. LITERATURE SURVEY

To verify the integrity of the outsourced data, several cloud storage auditing schemes have been proposed one after another. Ateniese et al. proposed provable data possession, which uses a random sampling strategy and homomorphic authenticator. Juels and Kaliski proposed proof of retrievability (PoR), which supports integrity auditing and recovery of the outsourced data. Subsequently, Shacham and Waters proposed a com- pact PoR based on BLS signature, which can support public integrity auditing. Furthermore, for cloud storage auditing, the security of the key is becoming increasingly important. Therefore, such as key exposure resilience and key escrow have been proposed successively in the cloud storage auditing.

After that, some cloud storage auditing schemes with privacy- preserving have been proposed. Wang et al. proposed a privacy-preserving public cloud storage auditing scheme, which can prevent the third-party auditor (TPA) from obtaining private data. Shen et al. proposed a lightweight cloud storage auditing scheme based on third party medium, which assists the DO to generate authenticators while protecting data privacy. Subsequently, Zhao et al. proposed a privacy-preserving cloud storage auditing scheme, which uses a security out-sourcing algorithm to assist the DO to generate authenticators. Anbuchelian et al. proposed a privacy-preserving cloud storage auditing scheme based on a secure encryption hash algorithm, which uses this hash algorithm to split and encrypt data. Han et al. proposed a lightweight privacy-preserving cloud storage auditing, which does not need bilinear pairing operations in the auditing phase. The above-mentioned schemes have complex certificate management problems because they are based on public key infrastructure. Then, Yu et al. proposed an identity-based cloud storage auditing scheme, which can prevent the auditor from accessing the DO's private data.

The data sharing is one important service provided by cloud storage. Wang et al. proposed a cloud storage auditing scheme for data sharing. In this scheme, the DO's identity privacy can be protected through a ring signature. However, cannot track the DO's real identity. Subsequently, Yang et al. proposed a cloud storage auditing scheme for data sharing, which can track the DO's identity. Fu et al. proposed a cloud storage auditing scheme, which used a homomorphic verifiable group signature to share data. Subsequently, other cloud storage auditing schemes for data sharing based on group signatures were successively proposed. Wu et al. proposed an efficient threshold privacy-preserving cloud storage auditing scheme. This scheme does not rely on group signatures or ring signatures, so the tag generation efficiency is more efficient. In the cloud storage auditing scheme of data sharing, the issue of user revocation has always been the focus of research. In 2018, Zhang et al. proposed a cloud storage auditing scheme for data sharing, which reduces the cost of revoking data users. Then, Chang and Wu proposed an efficient user revocation scheme with oblivious transfer and stateless lazy re-encryption. However, the DO's sensitive information can be accessed in the above-mentioned cloud storage auditing schemes for data sharing. In 2018, Shen et al. proposed a cloud storage auditing scheme for data sharing based on sanitizable signature, which can support the hiding of the DO's sensitive information. However, any users can access the sharing data in the scheme, which may cause the data abuse. Also, this scheme needs a secure channel between the DO and the sanitizer.

III. PROPOSED SYSTEM

Secure cloud storage auditing scheme 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 Diffie–Hellman protocol 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.

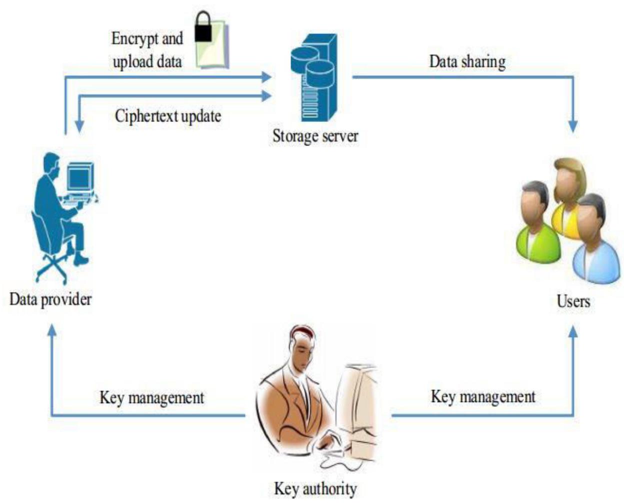

Fig: Architecture of the proposed methodology

SYSTEM MODEL

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

2) SANITIZER: It sanitizes the DO's data, and then transforms the corresponding authenticators. Subsequently, it sends the sanitized data and authenticators to the CS. Further- more, 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.

6) KGC: It is a fully trusted authority and responsible for generating system public parameters. Meanwhile, the KGC generates a private key for the DO.

In this model, the DO first sends the ID to the KGC for registration, the KGC distributes private key for the DO. Then, 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 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.

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) AUTHORIZATION ACCESS: Only the authorized user can access the DO's data.

VI. CONCLUSION

This article proposed a PP-CSA scheme for data sharing, which effectively supports the sensitive information hiding. In PP-CSA, only the authorized 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.

V. REFERENCES

[1] C. Sivapragash, S. R. Thilaga, and S. S. Kumar, "Advanced cloud comput- ing in smart power grid," in Proc. IET Chennai 3rd Int. Sustain. Energy Intell. Syst., 2014, pp. 356–361.

[2] C. Sivapragash, S. Padmanaban, H. Eklas, J. B. Holmnielsen, and R. Hemalatha, "Location-based optimized service selection for data man- agement with cloud computing in smart grids," Energies, vol. 12, no. 23, 2019, Art. no. 4517.

[3] S. Kumar and C. Sivapragash, "Time orient traffic estimation approach to improve performance of smart grids," J. Comput. Theor. Nanosci., vol. 13, no. 8, pp. 5037–5045, 2016.

[4] D. G. Chandra and R. S. Bhadoria, "Role of G-cloud in citizen centric governance," in Proc. IEEE Int. Conf. Parallel Distrib. Grid Comput., 2012, pp. 44–48.

[5] 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.

[6] K. S. Jadon, R. S. Bhadoria, and G. S. Tomar, "A review on costing issues in big data analytics," in Proc. Int. Conf. Comput. Intell. Commun. Netw., 2015, pp. 727–730.

[7] 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.

[8] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[9] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[10] K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Secur., vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[11] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 2, pp. 331–346, Feb. 2018.

[12] G. Ateniese, D. H. Chou, B. De Medeiros, and G. Tsudik, "Sanitizable signatures," in Proc. Eur. Symp. Res. Comput. Secur, 2005, pp. 159–177.

[13] H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryptol., vol. 26, no. 3, pp. 442–483, 2013.

[14] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, 2004.

[15] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1362–1375, Jun. 2016.

[16] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 8, pp. 1931–1940, Aug. 2017.

[17] Y. Xu, S. Sun, J. Cui, and H. Zhong, "Intrusion-resilient public cloud au- diting scheme with authenticator update," Inf. Sci., vol. 512, pp. 616–628, 2020.

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

[19] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," IEEE Syst. J., vol. 12, no. 1,

pp. 64–73, Mar. 2018.

[20] D. He, N. Kumar, S. Zeadally, and H. Wang, "Certificateless provable data possession scheme for cloud-based smart grid data management systems," IEEE Trans. Ind.

Informat., vol. 14, no. 3, pp. 1232–1241, Mar. 2018.

[21] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," IEEE Trans. Services Comput., to be published, doi: 10.1109/TSC.2018.2789893.

[22] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[23] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third-party medium," J. Netw. Comput. Appl., vol. 82, pp. 56–64, 2017.

[24] P. Zhao, J. Yu, and H. Zhang, "Secure outsourcing algorithm for signature generation in privacy-preserving public cloud storage auditing," J. Inf. Sci. Eng., vol. 35, no. 3, pp. 635–650, 2019.

[25] S. Anbuchelian, C. Sowmya, and C. Ramesh, "Efficient and secure auditing scheme for privacy preserving data storage in cloud," Cluster Comput., vol. 22, no. 4, pp. 9767–9775, 2019.

[26] J. Han, Y. Li, and W. Chen, "A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities," Comput. Standards Interfaces, vol. 62, pp. 84–97, 2019.

AUTHOR'S PROFILE

CH. RUSHYENDRA MANI is currently working as Assistant Professor in Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.

SK. MARIEM SIDDIKHA is pursuing MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.