Secure Transfer of EHR in Cloud Storage using AES

Drisya, Manjusha M S

Department of Computer Science and Engineering, MDIT, Kozhikode,India

---***---

Abstract - *In some common cloud storage systems such as the Electronic Health Records (EHRs) system, the cloud file might contain some sensitive information. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now. In order to address this problem, propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding and an highly secured encryption scheme has been used in it . In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file. As a result, scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. Proposed scheme also makes to transfer EHR in a secure way to be used by another ones. Meanwhile, the proposed scheme is based on AES cryptography.*

Key Words: *Electronic Health Records (EHRs), Sensitive information, Data integrity, Auditing, Sanitizer, Encrypting , AES , Cryptography.*

1.INTRODUCTION

Data sharing as one of the most common features in cloud storage, allows a number of users to share their data with others. However, these shared data stored in the cloud might contain some sensitive information. For instance, the Electronic Health Records (EHRs) [9] stored and shared in the cloud usually contain patients sensitive information (patients name, telephone number and ID number, etc.) and the hospitals sensitive information (hospitals name, etc.). If these EHRs are directly uploaded to the cloud to be shared for research purposes, the sensitive information of patient and hospital will be inevitably exposed to the cloud and the researchers.

A potential method of solving this problem is to encrypt the whole shared file before sending it to the cloud, and then generate the signatures used to verify the integrity of this encrypted file, finally upload this encrypted file and its corresponding signatures to the cloud. This method can realize the sensitive information hiding since only the data owner can decrypt this file. However, it will make the whole shared file unable to be used by others. So introduces a new concept of sharing of EHR files by AES encryption scheme and securely transfer to other systems.

1.1 Problem Statement

The data owner can decrypt this file. However, it will make the whole shared file unable to be used by others. For example, encrypting the EHRs of infectious disease patients can protect the privacy of patient and hospital, but these encrypted EHRs cannot be effectively utilized by researchers any more. Distributing the decryption key to the researchers seems to be a possible solution to the above problem. However, it is infeasible to adopt this method in real scenarios due to the following reasons. Firstly, distributing decryption key needs secure channels, which is hard to be satisfied in some instances. Furthermore, it seems very difficult for a user to know which researchers will use his/her EHRs in the near future when he/she upload s the EHRs to the cloud. As a result ,it is impracticall to hide sensitive information by encrypting the whole shared file. Transferring of EHR securely in cloud, downloading of EHR by patients from cloud. Unfortunately ,this problem has also remained unexplored in previous researches.

1.2 Scope of Work

Propose a concept data integrity auditing with sensitive information hiding for secure cloud storage. In such a scheme, the sensitive information can be protected and the other information can be published. It makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is protected. While the remote data integrity auditing is still able to be efficiently executed. Design a practical scheme with sensitive information hiding for secure cloud storage by using AES encryption scheme. In detailed scheme, firstly, the user blinds the data blocks corresponding to the personal sensitive information of the original file by using AES encryption, and then sends them to a sanitizer. A sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file it is also done by using AES encryption scheme. Design a practical scheme with sensitive information hiding for secure cloud storage by using AES encryption scheme and the transferring of HER securely in cloud and the downloading of HER of patients securely in cloud.

2. RELATED WORK

Data stored in the cloud can be retrieved and the integrity of these data can be ensured. Based on pseudorandom function and BLS signature, Shacham and Waters [4] proposed a private remote data integrity auditing scheme and a public remote data integrity auditing scheme.

In order to protect the data privacy, Wang et al. [5] proposed a privacy-preserving remote data integrity auditing scheme with the employment of a random masking technique. Solomon et al. [6] utilized a different random masking technique to further construct a remote data integrity auditing scheme supporting data privacy protection. This scheme achieves better efficiency compared with the scheme in [5]. To reduce the computation burden of signature generation on the user side, Guan et al. [7] designed a remote data integrity auditing scheme based on the indistinguishability obfuscation technique. Shen et al. [8] introduced a Third Party Medium (TPM) to design a light-weight remote data integrity auditing scheme. In this scheme, the TPM helps user generate signatures on the condition that data privacy can be protected.

In order to support data dynamics, Ateniese et al.[10] firstly proposed a partially dynamic PDP scheme. Erway et al. [11] used a skip list to construct a fully data dynamic auditing scheme. Wang et al. [12] proposed another remotedata integrity auditing scheme supporting full data dynamics by utilizing Merkle Hash Tree. To reduce the damage of users' key exposure, Yu et al. [13–15] proposed key-exposure resilient remote data integrity auditing schemes based on key update technique [16].

The data sharing is an important application in cloud storage scenarios. To protect the identity privacy of user, Wang et al. [17] designed a privacy-preserving shared data integrity auditing scheme by modifying the ring signature for secure cloud storage. Yang et al. [18] constructed an efficient shared data integrity auditing scheme, which not only supports the identity privacy but only achieves the identity traceability of users. Fu et al. [19] designed a privacy-aware shared data integrity auditing scheme by exploiting a homomorphic verifiable group signature. In order to support efficient user revocation, Wang et al. [20] proposed a shared data integrity auditing scheme with user revocation by using the proxy re-signature.

3. SYSTEM DESIGN

This section briefly describes the detailing scheme of the existing system and the modified system i.e.. is the proposed system.

3.1 Existing System:

The system model involves five kinds of different entities: the cloud, the user,the sanitizer, the Private Key Generator(PKG)and the Third Party Auditor (TPA), as shown in Fig 3.5.. (1)Cloud: The cloud provides enormous data storage space to the user. Through the cloud storage service, users can upload their data to the cloud and share their data with others. (2) User: The user is a member of an organization, which has a large number of les to be stored in the cloud. (3)Sanitizer: The sanitizer is in charge of sanitizing the data blocks corresponding to the sensitive information (personal sensitive information and the organizations sensitive information) in the le, transforming these data blocks signatures into valid ones for the sanitized le, and uploading the sanitized le and its corresponding signatures to the cloud. (4) PKG: The PKG is trusted by other entities. It is responsible for generating system public parameters and the private key for the user according to his identity ID. (5) TPA: The TPA is a public verifier. It is in charge of verifying the integrity of the data stored in the cloud on behalf of users. The system design is shown as:

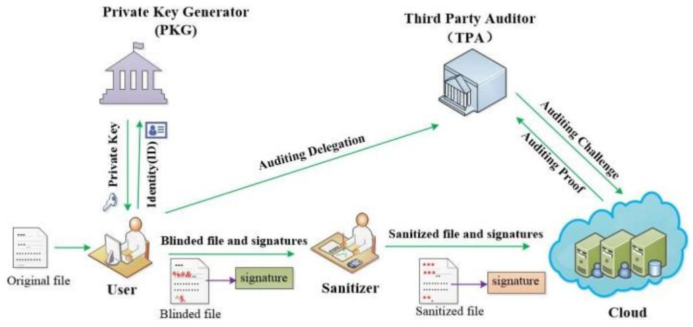


Fig -3.1: Existing System.

3.2 Proposed System

Finally, the user sends the blinded file. When the above messages from user are valid, the sanitizer firstly sanitizes the blinded data blocks into a uniform format and also sanitizes the data blocks corresponding to the organizations sensitive information to protect the privacy of organization. Finally, the sanitizer uploads the sanitized file and the corresponding signatures to the cloud. When the data integrity auditing task is performed, the cloud generates an auditing proof according to the challenge from the TPA. The TPA can verify the integrity of the sanitized file stored the cloud by checking whether this auditing proof is correct or not. The details will be described in the following subsection. The proposed scheme also provide the secure transfer of EHR in cloud i.e. the doctor from one hospital is allowed to send the EHR to the doctor i.e referred in the other hospital in a proper secure manner. Only the authorized doctor will get thecorrespondingEHRfromtheotherdoctorandthepatientsinformationwillbe highly secured in it. In this scheme patients also can download their own EHR from the cloud without being exposed to attackers. EHR can be securely transferred to the preferred doctor through thus cloud. Only the doctor interaction is only there and no external interactions. Patient can securely download their EHR file. Downloading is done through proper security.

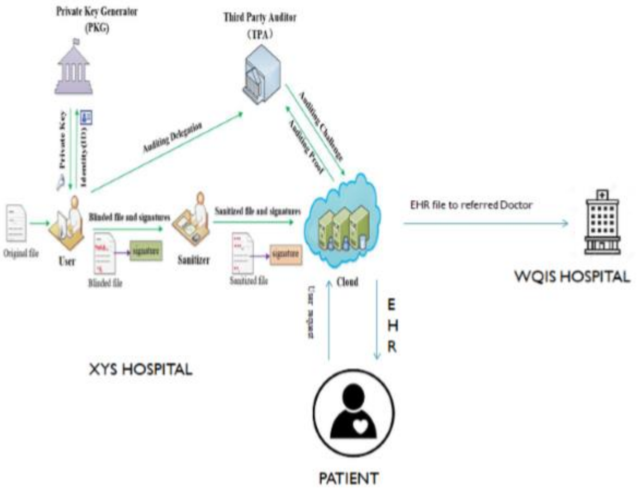


Fig -3.2: Proposed System

4. IMPLEMENTATION

EHR can be securely transferred to the preferred doctor through thus cloud. Only the doctor interaction is only there and no external interactions. Patient can securely download their EHR file. Downloading is done through proper security. This method not only realizes the remote data integrity auditing, but also supports the data sharing on the condition that sensitive information is protected in cloud storage. To the best of our knowledge, this is the first scheme with the above functions. Besides, our scheme is AES cryptography. We give the security analysis of the proposed scheme, and also justify the performance by concrete implementations. The result shows that the proposed scheme achieves desirable security and efficiency.

4.1. Implementing using Advanced Encryption Standard

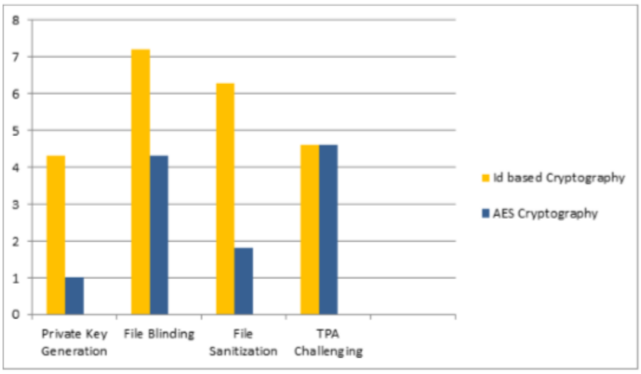
In this system AES encryption is done in the user side and the sanitizer side. The user blinds the sensitive information using the AES encryption and to ensure that the personal sensitive information of the le is not exposed to the sanitizer, and all of the sensitive information of the le is not exposed to the cloud and the shared users and by then it is been sent to the sanitizer. The sanitizer sanitizes the hospitals sensitive information and also .Firstly ,after the data blocks corresponding to the patients sensitive information are blinded, the contents of these data blocks might become messy code. The sanitizer can unify the format by using wildcard store place the contents of these data blocks. In addition, the sanitizer also can sanitize the data blocks corresponding to the hospitals sensitive information such as hospitals name by using wildcards, which protects the privacy of the hospital. Secondly ,the sanitizer can facilitate the information management. It can sanitize the EHRs in bulk , and uploads these sanitized EHRs to the cloud a taxed time. Thirdly, when the medical doctor needs the EHR,thesanitizerastheadministratorofEHRinformationsystemcandownload the blinded EHR from the EHR information system and sends it to the medical doctor. The medical doctor can recover the original EHR from the blinded one.

5. RESULT AND DISCUSSIONS

In this section, rst give the functionality comparison among our scheme and several related schemes, and the computation overhead. And then discuss the communication overhead and the computation complexity of our scheme.

5.1 Performance of different process

To effectively evaluate the performance in different processes, set the number of data blocks to be 100 and the number of sanitized data blocks to be 5 in our experiment. As shown in Fig.5.1 , private key generation and private key verification spend nearly the same time. The time of signature verification and that of sensitive information sanitization respectively same. So concluding that in these processes, the signature verification spends the longest time and the sensitive information sanitization spends the shortest time.



Pie Chart -5.1:Performance of different process

5.2. Computation Complexity

Analyze the computation complexity of the different entities in different phases. The computation complexity of different entities in this scheme respectively depends on the number c of challenged blocks, the total number n of data blocks, the number d1 of data blocks corresponding to the personal sensitive information and the number d2 of data blocks corresponding to the organizations sensitive information. See that the computation complexities of data blinding and signature generation for the user are O(d1) and O(n) respectively. On the sanitizer side ,the computation complexity of data sanitization is O(d1 + d2). The computation overheads of challenge generation and proof verification are both O(c) on the TPA side. The computation complexity of proof generation for the cloud is O(c).

6. CONCLUSIONS

Proposed an auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In scheme, the file stored in the cloud canbesharedandusedbyothersontheconditionthatthesensitiv einformationof the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency.

Better clinical decision by integrating the patients details into hospitals cloud. So the medical doctor can verify the case in details and examining it. Getting the details of the previous case can make it in a better one. So a grouping of EHR with similar cases are done.

7.FUTURE WORK

This system can be implemented in hospitals for further reference for details of the diagnosing as the personal information can be sanitized and the privacy can be protected.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, Jan 2012.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07, 2007, pp. 598–609.

[3] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07, 2007, pp. 584–597.

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

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud stor- age," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.

[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," *Comput. Electr. Eng.*, vol. 40, no. 5, pp. 1703–1713, Jul. 2014.

[7] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in *Computer Security – ESORICS 2015*. Cham: Springer International Publishing, 2015, pp. 203–223.

[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud audit- ing scheme for group users via the third party medium," *Journal of Network and Computer Applications*, vol. 82, pp. 56–64, 2017.

[9] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud audit- ing scheme for group users via the third party medium," *Journal of Network and Computer Applications*, vol. 82, pp. 56–64, 2017.

[10] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proceedings of the 4th international conference on Security and privacy in communication netowrks*, 2008, pp. 1–10