ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 143

2nd International Conference on Applied Mathematics, Modelling and Statistics Application (AMMSA 2018)

Safe Cloud Storage of Medical Information Based on Attribute Encryption

Boxiang Zhao, Liang Hu*, Yifan Zang, Yuxuan Liu, Xin Wen and Hongtu Li

College of Computer Science and Technology, Jilin University, Changchun, China

*Corresponding author

***Abstract*—Cloud computing has been developing at a rapid speed, playing an important role in many fields, especially in environments like hospitals which produce a lot of data every day and have specific users. Because the security of the information stored in the cloud cannot be guaranteed, we propose a safe cloud storage of medical information based on attribute encryption. This paper focuses on how to apply attribute-based encryption to hospitals' cloud storage environment, and to design the access process of different users in the cloud environment by using attribute encryption. Our goal is to build a scheme based on attribute encryption in which users with different demands can get the information they need in a safe and convenient way from the cloud server. In the scheme, sensitive information of a patient was encrypted locally based on attributes and then uploaded to the cloud server. We divided the users in the scheme into three kinds: the chief doctor, the doctor who is not in charge of the patient and the patient. Different users have a different way to get information stored in the cloud, and the decryption of the sensitive information is also different. For each step in the scheme, we carried out a security analysis to demonstrate the reliability, security and applicability of our scheme.**

Keywords—cloud storage; attribute-based encryption; medical information security

I. INTRODUCTION

A middle-sized hospital generates about 60 GB image data per day, which sets a great challenge to retrieve such amount of data even if its storage problem is assumed to be solvable. The fact is that the memory capacity of a hospital that can be used directly is limited. As a result, even though hospitals manage to expand their memory capacity every year, it still cannot meet its demand. To deal with this problem, hospital's image data is available for the clinician to view or retrieve online for only three days. After three days, these data will be transferred to a general server. Finally, these data will be stored in a hard disk after being stored in the server for three months. It will be very difficult and complex if you want to access these data after that.

In recent years, the rise of cloud computing arouses extensive interest in academic and industrial fields. As a new service pattern, cloud computing provides a platform to serve users according to their needs, such as data storage, software development, computing and so on. Data storage is one of the most popular cloud services. For agents like the hospital that need to generate a great deal of local-storage data (for instance patients' resource and image data), usage of cloud storage can perfectly deal with the problems like lack of local storage space or clearing at a high frequency.

Data in the cloud is exposed to the web environment, so the stored patient data may somehow be divulged, which would bring huge losses to the hospital and patients. Thus, the security problem of cloud computing draws more and more attention from the public. If the cloud server is insecure and the data stored in the cloud server is stored in plain text mode, it will be extremely easy for hackers to steal users' data after breaking through the security system of cloud service provider [1]. As a consequence, if we upload data to cloud server after we encrypt it, the data stored in the cloud server will be safe even if the cloud server is attacked.

We take the following case into consideration: a patient with coronary heart disease comes to internal medicine department to see a doctor and the doctor asks him to do some physical checkups (such as CT or B ultrasound) in the radiology department. After these checkups, doctors in radiology department encrypt the patient's image data and upload them to cloud server utilizing an attribute-based encryption algorithm with the access control policies in Figure 1. A few days later, the patient wants to copy his or her resources because he or she has to go to a better hospital. Physicians could download these data from the cloud server, decrypt and give the copy of checkups resources to the patient.

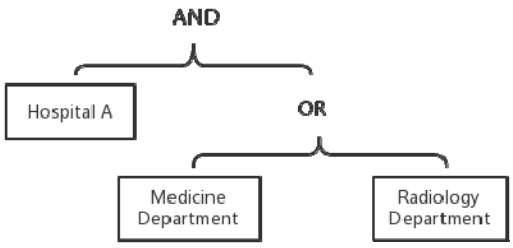

FIGURE I. ACCESS STRATEGY

In the situation mentioned above, when the patient's medical data is encrypted and uploaded to cloud server, only doctors in medicine or radiology department of hospital A have the right to download and view them, while others cannot view them even if they may obtain these resources in some improper ways.

The rest of the paper is organized as follows. Part 2 introduces some related work about attribute encryption and

security of cloud storage. Part 3 describes our safe cloud storage scheme. Part 4 proves the security of the scheme. Part 5 concludes the paper.

II. RELATED WORK

Sahai and Waters first proposed and achieved the concept of attribute-based encryption (ABE) [2], and Goyal et al. improved the scheme into key-policy ABE (KP-ABE) and ciphertext-based (CP-ABE) as two complementary forms of ABE [3]. The CP-ABE has a private attribute key which is associated with a set of attributes and its ciphertext is associated with an access policy, while the situation is reversed in KP-ABE.

Hasan et al. first considered the security and privacy issues of a provenance system, but they did not give any solutions on how to build a secure provenance system [4]. Lu et al. proposed a provenance system which efficiently achieves user privacy and data confidentiality using group signature [5]. However, it is built in the inefficient composite order groups, and it does not support expressive access control. Based on Lu`s work, Chow et al. built a cloud storage system which supports dynamic users and data provenance [6]. But the system can only have one-attribute access policies and the number of data users allowed by the system is limited.

Li et al. proposed a framework for access control to personal health records (PHR) within cloud computing environment using attribute-based encryption (ABE) [7]. Through ABE, every patient`s PHR data is encrypted. The framework shows how the patients control their own data and reduce the complexity of the keys management.

Zhao et al. created the first identity-based public verification scheme [8]. However, identity-based encryption does not suit the condition that a hospital contains many doctors with the same priority.

To ensure the remotely stored data integrity under different systems, the concept of public auditability was proposed in [9], [10], [11], and [12]. The public auditability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. But in [9], [10], and [11] `s schemes, there are not any privacy protection of users` data which means the data might be revealed to the auditors.

Wang et al. created a fair remote retrieval (FRR) model to enable an independent third party to secure the private medical information [13]. However, in the paper, Wang mainly talked about how to achieve the retrievability and integrity of the medical information and the model can`t provide secure data when there is an attack that a malicious server could modify user`s data and forge authenticated value.

The cloud storage solutions presented by the authors above are mostly used for general cloud computing. There are still many details to be discussed if it is used in specific areas, especially in the medical field which involves three kinds of users including the chief doctor, the doctor who is not in charge and the patient. How to design a scheme to determine who can access the sensitive information stored in the cloud and how much information they can access needs to be further discussed.

So far, no one has given a detailed and complete scheme of cloud storage in the medical field or in hospital.

III. OUR SCHEME

A. The Setting of the Attribute Set Is Shown in Figure II.

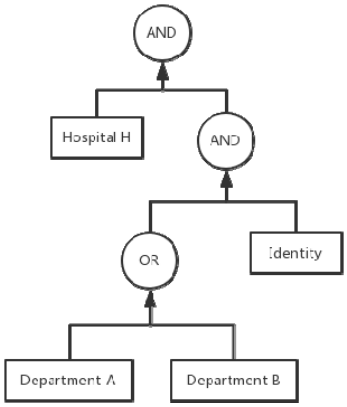

FIGURE II. THE SETTING OF ATTRIBUTE SET

B. Overview of the Scheme

The process is shown in Figure 3.

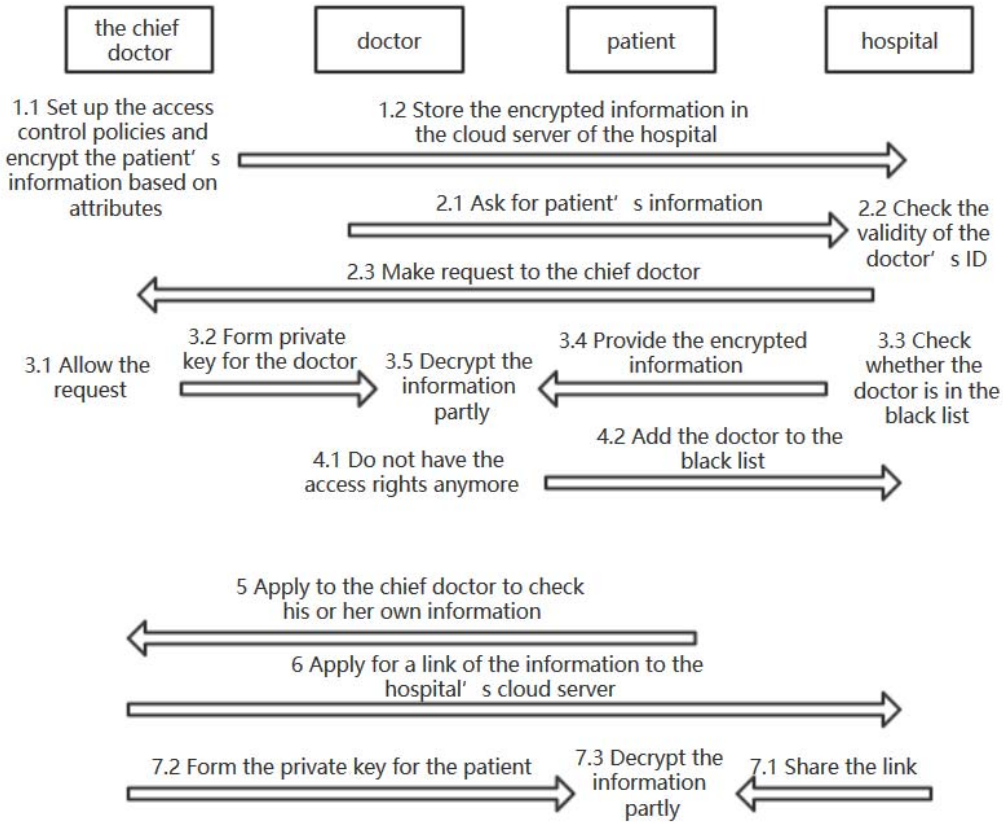

FIGURE III. DOCTOR AND PATIENT GET THE INFORMATION

After examining a patient, the chief doctor sets up the access control policies AC of the advice E, patient's data D (CT image, B ultrasound image and other data) and personal information I. Then he or she encrypts this information based on attribute-based encryption and finally uploads the ciphertext C to the cloud server.

$$C=Encrypt_{ABE}(E, D, I, AC);$$

1) The chief doctor C-DOC checks the files:

a) The validity V of the chief doctor's ID will be checked by the cloud server.

$$V_{C\text{-}DOC}=Check(ID_{C\text{-}DOC}, Blacklist);$$

b) Certificate Authority CA forms the private key PK based on the chief doctor's attributes A (e.g. hospital, department, name.....). Then the chief doctor could decrypt all the information including doctor's advice, patient's data, personal information.....

$$PK_{C\text{-}DOC}=Keygen(A_{C\text{-}DOC});$$

$$if\ (V_{C\text{-}DOC})\ M=Decrypt(PK_{C\text{-}DOC}, C);$$

c) If a chief doctor is no longer eligible to access the information, then the cloud server will add the chief doctor to the blacklist and reject his or her access.

$$if\ (!V_{C\text{-}DOC})\ Blacklist=Add(ID_{C\text{-}DOC});$$

2) Other doctors check the files: (in case doctors who have similar cases can learn from each other)

a) If a doctor DOC makes a request to the cloud server to access the information of a patient of another doctor, the validity of this doctor's ID will be checked by the hospital's cloud server. If it is valid, then the request will be sent to the chief doctor.

$$V_{DOC}=Check(ID_{DOC}, Blacklist);$$

$$Request=Send(V_{DOC}, ID_{C\text{-}DOC});$$

b) If the chief doctor approves this doctor's request of checking the files, then a private key will be formed by the certificate authority based on the doctor's attributes (hospital, department, name.....). The cloud server checks whether this doctor is on the blacklist, if not, the cloud server will provide the patient's information to this doctor, who could partly decrypt the information (doctor's advice, patient's data) later through a private key.

$$PK_{DOC}=Keygen\ (A_{DOC});$$

$$if\ (V_{DOC})\ M=Decrypt\ (PK_{DOC}, C);$$

c) If this doctor doesn't have the access right to these information, the server will add him or her to the blacklist and reject his or her requests.

$$if\ (!V_{DOC})\ Blacklist=Add\ (ID_{DOC});$$

3) Patients check the files: (in case the patient has to transfer to another hospital and the relevant image data and information have to be brought to the new one)

a) A patient P asks the chief doctor for his or her own information (CT image, B ultrasound image and other data).

$$Request=Send\ (1, ID_{C\text{-}DOC});$$

b) The chief doctor applies for a link of the file F with a valid period T to the hospital's cloud server. The certificate authority forms the private key for the patient based on his or her attributes (hospital, department, name.....).

$$Link=New\ (F, T);$$

$$PK_{P}=Keygen\ (A_{P});$$

c) The chief doctor shares the information link to the patient and then the patient could partly decrypt the information through a private key.

$$M=Decrypt\ (PK_{P}, C);$$

IV. SCHEME ANALYSIS

In the section above, we have described 3 cloud storage schemes using attribute-based encryption. In this section, we will carry out detailed safety analysis of these three schemes.

First of all, the chief doctor needs to record the patient's personal information, data and doctors' advice. After the doctor setting the strategy of access control, the sensitive information will be uploaded to the cloud after encryption which is safe during the uploading. Owing to the encryption, even if they are intercepted, the safety is still guaranteed.

If the chief doctor wants to download patient's sensitive information, he or she only needs to apply for downloading these data from the cloud server. Under the circumstances that the chief doctor's ID is valid, the cloud server will transmit the encrypted information. The certification authority then generates the private key for the chief doctor after identification. This step does not include the transmitting of clear text which makes sure that the sensitive information will not be divulged.

For one patient, if other doctors want to access his or her sensitive information, three steps below in this scheme ensure the safety of the cloud storage.

When the doctor wants to access one patient's information, the cloud server will check the validity of his or her ID. If the ID is invalid, the server will deny the access which is the foundation for safety. After that, the cloud server will inform the chief doctor who makes the decision whether the access is allowed. Meanwhile, the server checks whether the doctor is in the blacklist. Only meet the conditions at the same time can the doctor access the patient's data. During these steps, multiple authentication and confirmation ensure the rationality of the access. Next, certification authority checks the identity attribute of the doctor, even if someone breaks the first two barriers and gets the sensitive data, they cannot satisfy the decryption requirements and cannot decrypt the information. Finally, the satisfied doctor is able to get the data with the private key generated by certification authority based on his identity attribute.

For those who are qualified or once qualified to access the sensitive data stored in the cloud, the server will carry out regular checks to ensure that those who are not qualified can no longer access the data. If the identity gets changed which cause the change of some access rights, the server will add them to the blacklist in order to avoid them to access the data.

When the patients need their own data, they need to apply to the chief doctor who will apply a sharing link from the cloud server. This step requires the doctor's certification of the patient. For each generated link, a valid time will be set. Patients can only access the sensitive information of themselves within the stipulated time. Due to the time limit, it can ensure that sensitive information will be accessed by the certain person in certain time. At the same time, because of the data is encrypted, the patient requires the private key from the certification authority to decrypt the data. Those who get the link in illegal ways cannot pass the identification and decrypt the data.

V. CONCLUSIONS

In this paper, we proposed a reliable working scheme of medical information stored in cloud storage. And we proved that the medical information`s security can be guaranteed in cloud storage through our scheme by attribute-based encryption. The analysis of our scheme stated its efficiency.

REFERENCES

[1] Chow, R., Golle, P., Jakobsson, M., Shi, E., taddon, J., Masuoka, R., Molina, J., 2009. Controlling data in the cloud: outsourcing computation

without outsourcing control. In: Proceedings of the ACM Workshop on Cloud Computing Security. pp. 85–90.

[2] Sahai A, Waters B. Fuzzy Identity-Based Encryption[C]// International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2005:457-473.

[3] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// ACM Conference on Computer and Communications Security. ACM, 2006:89-98.

[4] Hasan R, Sion R, Winslett M. Introducing secure provenance:problems and challenges[C]// ACM Workshop on Storage Security and Survivability, Storagess 2007, Alexandria, Va, Usa, October. DBLP, 2007:13-18.

[5] Lu R, Lin X, Liang X, et al. Secure provenance:the essential of bread and butter of data forensics in cloud computing[C]// ACM Symposium on Information, Computer and Communications Security, ASIACCS 2010, Beijing, China, April. DBLP, 2010:282-292.

[6] Chow S S M, Chu C K, Huang X, et al. Dynamic secure cloud storage with provenance[C]// Cryptography and Security. Springer-Verlag, 2012:442-464.

[7] Li M, Yu S, Ren K, et al. Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings[C]// International Conference on Security and Privacy in Communication Systems. Springer Berlin Heidelberg, 2010:89-106.

[8] Zhao J, Xu C, Li F, et al. Identity-Based Public Verification with Privacy-Preserving for Data Storage Security in Cloud Computing[J]. Ieice Trans Fundamentals, 2013, 96(12):2709-2716.

[9] Ateniese G, Burns R, Curtmola R, et al. Provable data possession at untrusted stores[C]// ACM Conference on Computer and Communications Security. ACM, 2007:598-609.

[10] Wang Q, Wang C, Li J, et al. Enabling public verifiability and data dynamics for storage security in cloud computing[C]// European Conference on Research in Computer Security. Springer-Verlag, 2009:355-370.

[11] Shacham H, Waters B. Compact Proofs of Retrievability[C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2008:90-107.

[12] Juels A, Kaliski B S. Pors:proofs of retrievability for large files[C]// ACM Conference on Computer and Communications Security. ACM, 2007:584-597.

[13] Wang H, Wu Q, Qin B, Josep DF. FRR: fair remote retrieval of outsourced private medical records in electronic health networks. Journal of Biomedical Informatics 2014; 50:226–233.