Inference Attack Resistant E-Healthcare Cloud System with Fine-Grained Access Control

Vidhya R[1], Vijaykumar C[2], Sumathi A[3]
[1,2,3]*Jayalakshmi Institute of Technology*

Abstract- **The e-healthcare cloud system has shown its potential to improve the quality of healthcare and individuals' quality of life. Unfortunately, security and privacy impede its widespread deployment and application. There are several research works focusing on preserving the privacy of the electronic healthcare record (EHR) data. We first propose a two-layer encryption scheme. To ensure an efficient and fine-grained access control over the EHR data, we design the first-layer encryption, where we devise a specialized access policy for each data attribute in the EHR, and encrypt them individually with high efficiency. To preserve the privacy of role attributes and access policies used in the first-layer encryption, we systematically construct the second-layer encryption We proposed User revocation is commonly supported in such schemes, as users may be subject to group membership changes for various reasons. Previously, the computational overhead for Auto user revocation. We include binary key generation for file storage. File encryption we proposed time enable proposed re encryption.**

I. INTRODUCTION

The electronic healthcare, providing timely, accurate, and low-cost healthcare services, has shown its potential to improve the quality of healthcare and individuals. When these sensitive data are abused, more serious problems will occur. For example, insurance companies would refuse to provide insurance to those who have serious health problems. To achieve the fine-grained access control, we need to define a specialized access policy for each data attribute in the EHR. Since different data attributes in the EHR usually share many role attributes in their access policies, for security concerns, we need to conceal the frequency of role attributes occurring in the HER. the first-layer encryption, the data owner conceals these access policy, and conducts the second-layer encryption. After that, the data owner outsources the encrypted EHR data, the encrypted first-layer access policy, and the second-layer access policy to the cloud. Finally, the data user conducts the first-layer decryption and obtains the authorized data attributes in the HER.

II. RELATED WORKS

First Specifically, once a data user is authorized, he can access all the data attributes in the EHR. For example, if a dentist is authorized to access a patient's EHR, then he can even access the patient's social Second, they suffer from the inference attack. The inference attack includes the frequency analysis attack, sorting attack, and cumulative attack. Among them, the most well known attack is the frequency analysis attack, which breaks the classical encryption algorithms. Existing schemes adopt the conventional ciphertext policy attribute-based encryption to encrypt the EHR, which inevitably expose the access policy to the cloud. Third, they have to spend a large amount of time on secret generation for the repeated items. Each data attribute has its own role attributes. As we can see, there are a lot of repeated role attributes in the EHR. In conventional schemes, instead of generating ciphertext. the efficiency can be improved for nearly three times in this example. Since the data attributes in the EHR often have a lot of repeated role attributes, we need to propose schemes to save the computation cost spent on the repeated role attributes.

III. THE PROPOSED SYSTEM

To ensure an efficient and fine-grained access control over the EHR data. e to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of data attributes in the EHR, we further construct a blind data retrieving protocol. We provide rigorous security analyses and con_duct extensive experiments to confirm the

effica_cy and efficiency of our proposed schemes. : Our proposed scheme should control the privacy protection to a specific level. We measure the privacy disclosure of our scheme by the attacker's confidence in the success of an attack. our proposed scheme, and show that the security and privacy goals have been achieved. We first prove that the two-layer encryption scheme. We proposed User revocation is commonly supported in such schemes, as users may be subject to group membership. We include binary key generation for file storage file encryption we proposed time enable proposed re encryption.

IV. THE EXISTING SYSTEM

1.System Model In our system model, four entities are involved, as shown in Fig. 2: they are the trusted authority, the data owners, the users, and the cloud. The trusted author_ity is responsible for user registration and revocation. The data owners are those who will outsource their EHR data to the cloud. To guarantee a fine-grained access control while preserving data privacy, the data owners encrypt their EHR data before outsourcing. To access this encrypted EHR data, the data user submits his role attributes to the cloud. Upon receiving the role attributes, the cloud retrieves the encrypted data and returns them to the data user.

2.SECURE CONSTRUCTIONSAs we can see, at the beginning, the data owner conducts the first-layer encryption on each data attribute in the EHR with the attribute based encryption algorithms. Then, to prevent the attacker from knowing the access policies used in the first-layer encryption, the data owner conceals these access policy, and conducts the second-layer encryption. After that, the data owner outsources the encrypted EHR data, the encrypted first-layer access policy, and the second-layer access policy to the cloud. Once the data user wants to retrieve data stored on the cloud, he submits his role attributes to the cloud, and the cloud will return the encrypted first-layer access policy. Upon receiving the ciphertext of the first-layer access policy, the data user performs the second-layer decryption, and retrieves his authorized data attributes from the cloud. With our design, the data retrieving process preserves the access pattern privacy

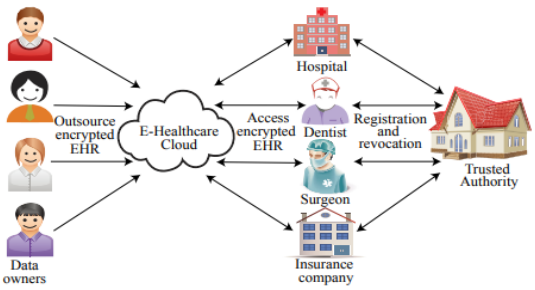
3.Proxy Re-Encryption (TimePRE)
Time-based Proxy Re-Encryption (TimePRE) scheme was proposed to allow a users' access right to expire automatically after a predetermined period of time. In this case, the data owner can be offline in the process of user revocations. The basic idea is to incorporate the concept of time into the combination of ABE and PRE. Specifically, each data is associated with an attribute-based access structure and an access time, and each user is identified by a set of attributes and a set of eligible time periods which denote the period of validity of the user's access right.

4.Revoking Role Attributes In conventional schemes, when a data owner wants to revoke several role attributes, say A′, the data owner needs to update the secret for role attributes in A′, and re-generate secret shares and ciphertexts for all the role attributes involved in the affected data attributes. We observe that, when the data attributes share very few repeated role attributes in an EHR data, then we only need to update secret shares for very few role attributes.

Disadvantages of Existing System

1. The first attempt to address the inference attack problem in the e-healthcare cloud system with fine grained access control.
2. Existing schemes adopt the conventional ciphertext policy attribute-based encryption to encrypt the EHR, which inevitably expose the access policy to the cloud.
3. the data attributes while preserving the statistical data of the role attributes is a challenging problem.

V. SYSTEM ARCHITECTURES



VI. RESEARCH METHODOLOGIES

Waterfall Model: The Waterfall Model is a linear sequential flow. In which progress is seen as flowing steadily downwards (like a waterfall) through the phases of software implementation. This means that any phase in the development process begins only if the previous phase is complete. The waterfall approach does not define the process to go back to the previous phase to handle changes in requirement.

Waterfall Model Phases

Waterfall Model contains the main phases similarly to other process models, you can read this article for more information about phases definitions.

When to use Waterfall Model?

Due to the nature of the waterfall model, it is hard to get back to the previous phase once completed. Although, this is can be very rigid in some software projects which need some flexibility, while, this model can be essential or the most suitable model for other software projects' contexts.

The usage of the waterfall model can fall under the projects which do not focus on changing the requirements, for example:

1. Projects initiated from a request for proposal (RFP), the customer has a very clear documented requirements
2. Mission Critical projects, for example, in a Space shuttle
3. Embedded systems.

VII. CONCLUSION

we design an inference attack resistant e-healthcare cloud system with fine grained access control. We first propose a Time proxy re encryption scheme. We propose to define a specialized access policy for each data attribute in the HER, generate a secret share for every distinct role attribute, and reconstruct the secret to encrypt each data attribute. To preserve the access pattern of the data attributes in the HER, we construct a blind data retrieving protocol based on the Paillier encryption. Provides the encryption module for the re-encryption and also time privileges for accessing particular file. This will enable each user's access right to be effective in a pre-determined period of time, and enable the CSP to re-encrypt cipher texts automatically, based on its own time. In order to deal with user revocation, Time based PRE was implemented to provide access. Since we embed randomness there. Additionally, the inference attack described in our paper is launched by observing the role attributes, access policy, and access pattern (access frequency). With our constructions, we can prevent the attackers from achieving the inference attacks. We aim to systematically construct a secure and privacy preserving e-health cloud system, so that it is immune to the inference attack and runs efficiently.

VIII. SOFTWARE REQUIREMENTS

Operating system	:	Windows XP/7.
Coding Language	:	Java .
Front end	:	Html/css
Back end	:	J2se,J2ee.
Database	:	Mysql.
Tools	:	NetBeans IDE 7.2.1

HARDWARE REQUIREMENTS:

System	:	Pentoium IV 2.4 GHz.
Hard disk	:	40 GB.
Floopy driver	:	1.44 Mb.
Monitor	:	15 VGA colour.
Mouse	:	DELL.
Ram	:	512 Mb.

IX. REFERENCES

[1] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227– 238, 2013.

[2] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, pp. 1–10, 2015.

[3] W. Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, "Secure distributed keyword search in multiple clouds," in Proc. IEEE/ACM IWQOS'14. Hongkong: IEEE/ACM, May 2014, pp. 370–379.

[4] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014). Atlanta, USA: IEEE, jun 2014, pp. 276–286.

[5] D. Nascimento and M. Correia, "Shuttle: Intrusion recovery for paas," in Proc. IEEE Distributed Computing Systems (ICDCS'15), Ohio, USA, Jun.

2015, pp. 10–20. [6] At risk of exposure -in the push for electronic medical records, concern is growing about how well privacy can be safeguarded. [Online]. Available: http://articles.latimes.com/2006/ jun/26/health/heprivacy26

[7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 103–114.

[8] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Security and Privacy in Communication Networks. Springer, 2010, pp. 89–106.

[9] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "Hcpp: Cryptography based secure ehr system for patient privacy and emergency healthcare," in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 373–382.

[10] J. Zhou, Z. Cao, X. Dong, and X. Lin, "Tr-mabe: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," in INFOCOM, 2015 Proceedings IEEE. Hong Kong: IEEE, 2015, pp. 2398–2406.

[11] M. Naveed, S. Kamara, and C. V. Wright, "Inference attacks on property-preserving encrypted databases," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 644–655.

[12] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Technion-Israel Institute of technology, Faculty of computer science, 1996.

[13] Z. Liu, Z. Cao, and D. S. Wong, "Efficient generation of linear secret sharing scheme matrices from threshold access trees," IACR Cryptology ePrint Archive, 2010. [Online]. Available: http://eprint.iacr.org/2010/374

[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in cryptologyEUROCRYPT99. Springer, 1999, pp. 223–238.

[15] B. Wang, W. Song, W. Lou, and Y. T. Hou, "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee," in INFOCOM, 2015 Proceedings IEEE. Hong Kong: IEEE, 2015, pp. 2092–2110.

[16] W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," IEEE Transactions on Computers, 2015. [20] L. Zhang, T