International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 255-261 www.ijaem.net ISSN: 2395-5252

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

Kanagarajan M 1, MR. Nagarajan, A.P, M.C.A.2
1.IIMCA, Sri Muthukumaran Institute of Technology, Mangadu
2.Professor, MCA, Sri Muthukumaran Institute of Technology, Mangadu

Date of Submission: 01-09-2022 Date of Acceptance: 10-09-2022

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.**

Index Terms—E-healthcare cloud, electronic healthcare record (EHR), inference attack, fine-grained access control, two-layer encryption.

I. INTRODUCTION

1.1 About the project

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 EHR. the first-layer encryption, the data owner conceals this is 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 EHR.

1.2 EXISTING SYSTEM

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.

Disadvantage.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 255-261 www.ijaem.net ISSN: 2395-5252

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

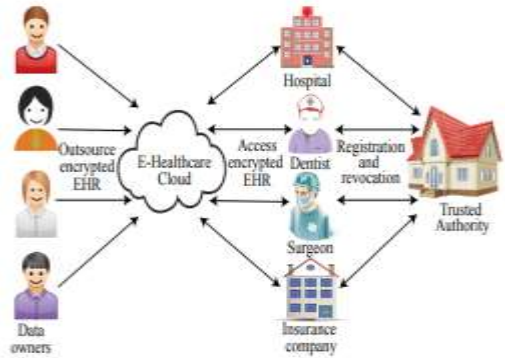
1.3 PROPOSED SYSTEM

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 conduct extensive experiments to confirm the efficacy 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. Specialist**

Advantage

- our proposed scheme, and show that the security and privacy goals have been achieved. We first prove that the two-layer encryption scheme is secure.
- We provide rigorous security analyses and conduct extensive experiments to confirm the efficacy and efficiency of our proposed scheme.
- Uses attributes of the users to provide access to data. Time-based Proxy Re- Encryption specifies time for every attribute of a user which is termed as access time of the attribute.
- The key problems of this approach include establishing access control for the encrypted data and revoking the access rights from users when they are no longer authorized to access the encrypted data

System architecture



Modules

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 authority 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. The data user further decrypts the ciphertexts, and obtains the authorized data attributes in the EHR with his role attributes.

2.SECURE CONSTRUCTIONS

As 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 this 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

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 255-261 www.ijaem.net ISSN: 2395-5252

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. When the data attributes share many repeated role attributes in an EHR data, though we need to update the secret shares for some role attributes, , conventional schemes have to update the secret share for all the role attributes of all the affected data attributes.

Algorithm

The proxy re-encryption was not explicitly used, the system mimics a proxy re-encryption (PRE) algorithm scheme from the point of view of the data owner and user. Re-Encryption of original cipher text is done with the help of semi-trusted third party (proxy server). Here, encrypted data which is already done by the owner provided to the proxy server, proxy server will re-encrypt that file without knowing the plain text and user can decrypt without sharing his/ her secret key to the proxy server.

1.4 Technical Challenges

To design an efficient and inference attack-resistant e-healthcare cloud system with fine-grained access control, there are three key challenges.

1) 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 EHR. Therefore, how to ensure an efficient and correct encryption on the data attributes while preserving the statistical data of the role attributes is a challenging problem.
2) To improve the efficiency of the whole system, the cloud is expected to execute computationally intensive works on behalf of the data users. Thus, how to prevent the cloud from deducing sensitive data, while achieving the above functionality is very important.
3) Since the cloud possesses all the EHR data and is responsible for returning accessed data, how to ensure the cloud correctly and efficiently returns the data attributes without knowing which data attributes are actually returned is also a challenging problem.

1.5 Our Approach and Key Contributions

In this paper, for the first time, we design an inference attack-resistant e-healthcare cloud system with fine-grained access control. We first propose a two-layer encryption scheme. In the first-layer encryption, we propose to define a specialized access policy for each data attribute in the EHR, generate a secret share for every distinct role attribute, and reconstruct the secret to encrypt each data attribute, which ensures a fine-grained access control, saves much encryption time, and conceals the frequency of role attributes occurring in the EHR. In the second-layer encryption, we propose to preserve the privacy of role attributes and access policies used in the first-layer encryption. Specifically, we merge the first-layer access policies, add noise to the merged access policy, and encrypt the first-layer access policies under the noisy and merged access policy. Additionally, to take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern(access frequency) of the data attributes in the EHR, we construct a blind data retrieving protocol. Furthermore, we show that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations, which confirm the efficacy and efficiency of our schemes.

Our main contributions are summarized as follows:

- To the best of our knowledge, this is the first attempt to address the inference attack problem in the e-healthcare cloud system with fine-grained access control. Compared with the existing solutions, our scheme not only ensures novel functionalities, but also achieves higher efficiency on encryption, decryption, and role attribute revocation.
- We systematically construct a two-layer encryption scheme. The first-layer encryption ensures the fine-grained access control, saves much encryption time, and conceals the frequency of role attributes occurring in the EHR. The

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 255-261 www.ijaem.net ISSN: 2395-5252

second layer encryption enables the cloud to execute computationally intensive works on behalf of the data user, while preserving the privacy of access policies used in the first-layer encryption.

- We design a blind data retrieving protocol, which preserves the access pattern of data attributes in the EHR, and achieves high efficiency.
- We provide rigorous security analyses and conduct extensive experiments to confirm the efficacy and efficiency of our proposed schemes.

The rest of this paper is organized as follows. Section 2 presents the preliminaries. Section 3 formulates the problem. Section 4 demonstrates the secure constructions. Section 5 presents the security and privacy analysis. Section 6 demonstrates the efficiency of our proposed scheme. Section 7 reviews the related works. In Section 8, we conclude the paper.

II. CLOUD COMPUTING:

Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software are located and how it all works doesn't matter to you, the user—it's just somewhere up in the nebulous "cloud" that the Internet represents.

2.1DATA SECURITY

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centres that provide diverse services over the network or the Internet to satisfy user's requirements

Cloud computing can be considered as a new computing archetype that can provide services on demand at a minimal cost. The three well-known and commonly used service models in the cloud paradigm are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with the related data is deployed by a cloud service provider, and users can use it through the web browsers. In PaaS, a service provider facilitates services to the users with a set of software programs that can solve the specific tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities.

2.2CLOUD SERVICES

Cloud computing will enable services to be consumed easily on demand. Cloud computing has the characteristics such as on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk. These merits of cloud computing have attracted substantial interests from both the industrial world and the academic research world. Cloud computing technology is currently changing the way to do business in the world. Data security has consistently been a major issue in IT. Data security becomes particularly serious in the cloud computing environment, because data are scattered in different machines and storage devices including servers, PCs, and various mobile devices such as wireless sensor networks and smart phones. Data security in the cloud computing is more complicated than data security in the traditional information systems.

To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy. The trustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology. Latif et al. discussed the assessment of cloud computing risks

2.3Data Confidentiality: Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 255-261 www.ijaem.net ISSN: 2395-5252

Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization.

2.4 Hybrid Technique

A hybrid technique is proposed for data confidentiality and integrity [33], which uses both key sharing and authentication techniques. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. RSA public key algorithm can be used for secure distribution of the keys between the user and cloud service providers.

2.5 Data Availability

Data availability means the following: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

2.6 Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively [43]. Privacy has the following elements.

(i) When: a subject may be more concerned about the current or future information being revealed than information from the past.

(ii) How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

(iii) Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

III. PRIVACY PRESERVING ELECTRONIC HEALTHCARE SYSTEMS

The security and privacy problems in e-healthcare systems have attracted much interest. Benaloh et al. [10] proposed an efficient system that enables data owners to perform searches over their EHR data, and share partial access rights with other users. To achieve a data owner-centric access control over EHR in the multi-owner cloud system, Li et al. [11] proposed to adopt the multi-authority attribute-based encryption to encrypt each owner's EHR. In [12], Sun et al. designed a secure electronic health record system based on anonymous credentials, a pseudorandom number generator, and the proof of knowledge. Based on the noninteractive proof system, Guo et al. proposed a privacy preserving attribute-based authentication system in mobile health networks [27], and a verifiable and privacy-preserving monitoring scheme for the e-healthcare cloud system [28]. Zhou et al. [13] further proposed a white-box traceable and revocable multiauthority attribute-based encryption (TR-MABE) to achieve a multilevel privacy preservation for EHR data.

These works suffer from two main limitations. First, they only support the 'black or white' access control policy. Second, they suffer from the inference attack. Different from these works, we seek to design an inference attack-resistant e-healthcare cloud system with fine-grained access control.

1.6 Attribute-based Encryption

The Attribute-based Encryption (ABE) was first introduced by Sahai and Waters [29]. In the ABE, a user is authorized to decrypt a cipher-text only if his role attributes satisfy the corresponding access policy. Goyal et al. [30] first designed the Key-Policy Attribute Based Encryption (KP-ABE), where a ciphertext is labelled with a set of role attributes, and the corresponding private key is associated with an access policy. Later, Bethencourt et al. [31] introduced the CiphertextPolicy Attribute-Based Encryption (CP-ABE), where the private key is associated with role attributes and the cipher-text is associated with an access policy. In [25], Waters presented the efficient, expressive, and secure CP-ABE systems, where they embed a LSSS matrix into the public parameters.

Since the conventional ABE-based schemes will inevitably expose the role attributes and access policies to the public, they suffer from the inference attack. 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.

1.7 Inference Attack

The recent papers [14], [32] focus on the inference attack against encrypted databases. They demonstrate that by adopting techniques including frequency analysis and sorting attack, the inference attack can break most of existing encrypted databases. In these two papers, the data is assumed to be numerical, and encrypted with the property-preserving encryption schemes(the order preserving encryption, the deterministic encryption, etc.).

Different from these researches, we aim to protect the E-Healthcare data with fine-grained access

control, the data can be either numerical or string value. To achieve this, we devise our own two-layer encryption scheme, the ciphertext is neither order-preserving nor deterministic, 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.

IV. 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 EHR, 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 EHR, 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.

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 e-Print 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