IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

E-Healthcare Privacy data sharing with Fine-Grained Access Control

Miss. S. Saranya[1], V. Sandhiya[2], U. Rakshana Kumar[3]
Assistant Professor, Department of Computer Science and Engineering[1]
Research Student, Department of Computer Science and Engineering[2,3]
Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

Abstract: *The E-Healthcare Cloud system has shown that it can improve healthcare quality as well as individual quality of life. Unfortunately, concerns about security and privacy prevent it from being widely adopted and used. Several studies have been carried out in order to protect the privacy of electronic health record (EHR) data. We start with a two-layer encryption scheme. We create first-layer encryption to ensure efficient and fine-grained access control over EHR data, in which we create a highly specialised access policy for each data attribute in the EHR and encrypt them individually with high efficiency. To protect the privacy of role attributes and access policies used in the first-layer encryption, we construct the second-layer encryption systematically. We made a recommendation. User revocation is commonly supported in such schemes, as users' group memberships may change for a variety of reasons. Prior to now, the computational overhead for Auto user revocation. Binary key generation is included for file storage. We proposed enabling file encryption alongside proxy re encryption.*

Keywords: E-Healthcare.

I. INTRODUCTION

Electronic healthcare, which provides timely, accurate, and low-cost healthcare services, has demonstrated its potential to improve the quality of healthcare and people's lives. Many companies around the world have developed healthcare services, such as Google Fit, Apple Health Kit, and others. Meanwhile, with cloud computing's increasing maturity and benefits, the e-healthcare cloud system has piqued the interest of both academics and industry. IBM has already established its e-healthcare cloud centre, dubbed IBM Watson Health Cloud. Unfortunately, security and privacy concerns will impede widespread deployment and use of the e-healthcare cloud system. The fundamental reason is that once sensitive EHR data is outsourced to the cloud, data owners will lose control. Although cloud service providers promise to safeguard this information by installing anti-virus software, firewalls, and intrusion detection and prevention systems, they cannot prevent their employees from accessing it. For example, a veteran's affairs employee once took 26.5 million sensitive data items, including social security numbers and sensitive health information, without authorization. When sensitive data is misused, more serious problems arise. Insurance companies, for example, would refuse to insure individuals with serious health issues. As a result, it is critical to maintain the security and privacy of EHR data stored in the e-healthcare cloud system.

II. SYSTEM ANALYSIS EXISTING SYSTEM

First In particular, once a data user has been authorised, he has access to all data attributes in the EHR. For example, if a dentist is authorised to access a patient's EHR, he can also view the patient's information. Second, they are vulnerable to the inference attack. The frequency analysis attack, sorting attack, and cumulative attack are all part of the inference attack. The most well-known of these is the frequency analysis attack, which breaks traditional encryption algorithms. Existing schemes encrypt the EHR using traditional ciphertext policy attribute-based encryption, which inevitably exposes the access policy to the cloud. Third, they must devote a significant amount of time to secret generation for the repeated items. Each data attribute has its own set of roles. As we can see, the EHR contains a lot of repeated role attributes. Instead of generating ciphertext, conventional schemes can improve efficiency by nearly threefold in this example. Because data attributes in the EHR frequently contain a large number of repeated role attributes, we must propose schemes to reduce the computation cost associated with the repeated role attributes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Disadvantage

- Problems with data security and performance
- After response file access, the file can be accessed at any time.

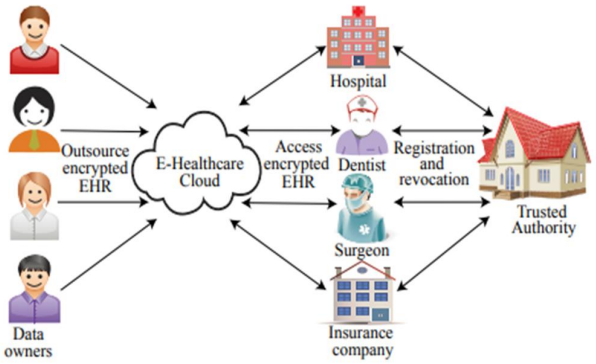
2.1 Proposed System

To ensure that access to EHR data is efficient and fine-grained. E Healthcare-Cloud allows the cloud to perform computationally intensive tasks on behalf of the data user while keeping sensitive information private. We also develop a blind data retrieving protocol to preserve the access pattern of data attributes in the EHR. We conduct extensive experiments and perform rigorous security analyses to validate the efficacy and efficiency of our proposed schemes. Our proposed scheme should limit the level of privacy protection to a certain degree. We measure the privacy disclosure of our scheme using the attacker's confidence in the success of an attack. We begin by demonstrating the two-layer encryption scheme. We suggested Because users may be subject to group membership, such schemes commonly support user revocation. For file storage, we include binary key generation. We proposed enabling proxy re encryption for file encryption.

Advantages

- Our main advantage is that we can securely store and access data in the cloud.
- If the server is interrupted or an internal staff member makes a mistake, the E-Healthcare document may be vulnerable. our proposed scheme, and demonstrate that the security and privacy objectives were met.
- The serious security and protection concerns are just one of the issues impeding the framework's widespread adoption.

III. SYSTEM ARCHITECTURE



3.1 Modules Description

A. Data Owner

There are n numbers of data owners in this module. Before performing any operations, the owner should register. And the details of the registered owner are saved in the Owner module. After successfully registering, he must login with his authorised user name and password.

Data Owner, based on user characteristics, develops different access control strategies, encrypts uploaded files with the appropriate encryption method, and then sends them to the cloud server.

In this module, we perform the following tasks:

1. Register
2. Login
3. Upload File

The data owner receives a one-time key from the cloud server. That key is used in the upload process. When the Data Owner's Session Time is up, the Key will automatically expire. Data owners should define the access policy for each data

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

attribute in the EHR so that data users can access the data. In this module, there are n numbers of data owner are present. Owner should register before doing some operations. And register Owner details are stored in Owner module. After registration successful he has to login by using authorized user name and password.
Cloud Server Provide one Time Key to Data Owner. That Key Used for upload Process. After Data owner Session Time Finished the Key will automatically expired.

1. View File
2. Logout

The access policy for each data attribute in the EHR should be specified by the data owner so that the data user can only access and decrypt his authorised data attribute.

User

The user is the receiver of ciphertexts who has access to the outsourced data. If the user is the intended receiver as defined by the data owners or data disseminators, he is able to decrypt the initial and re-encrypted ciphertexts. This module contains n data users. Before performing any operations, the Data User must first register. And only the Trusted authority has access to register user details. After a successful registration, the trusted authority must grant permission to the data user. The user must then login with an authorised user name and password. The User can define their roles in this module, such as Surgeon, Insurance, and so on.

E-Healthcare Cloud System

In this module, we create the following features:

1. Login
2. View All File Information
3. Update User and Owner
4. View All Data Owner
5. View All User details with status of Blocked or accepted.

Trusted Authority

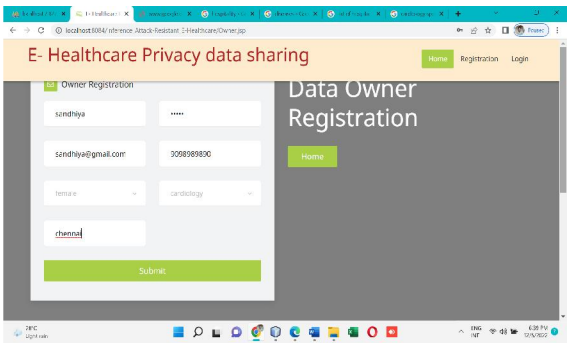
The central authority (CA) is a fully trusted authority that manages and distributes public/secret keys in the system, including generating system parameters to initialize. the system and generating private keys and attribute keys with users' identity and attributes. Furthermore, it serves as a trusted time agent, publishing time tokens at predefined intervals.

IV. OUTPUT RESULTS

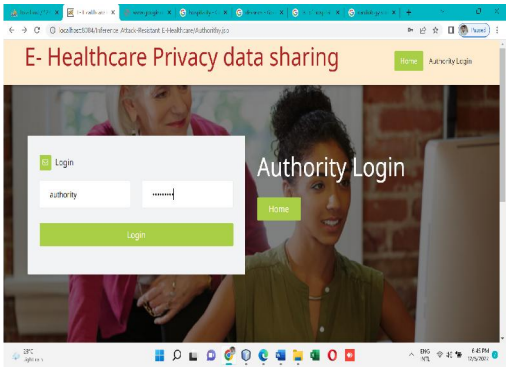
Home Page

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

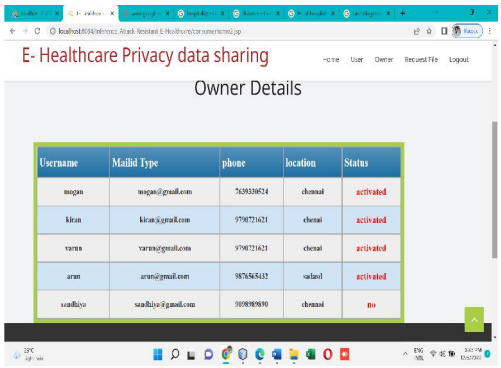
Owner Registration



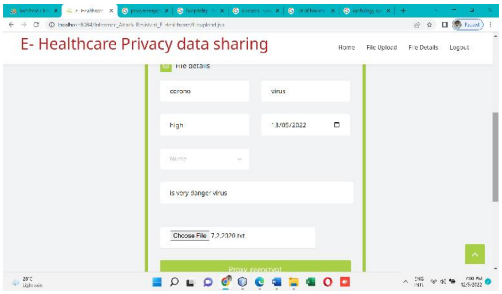
Authority Login



Authority verified owner details

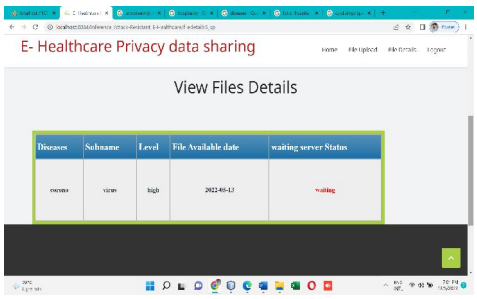


Data Owner file uplood

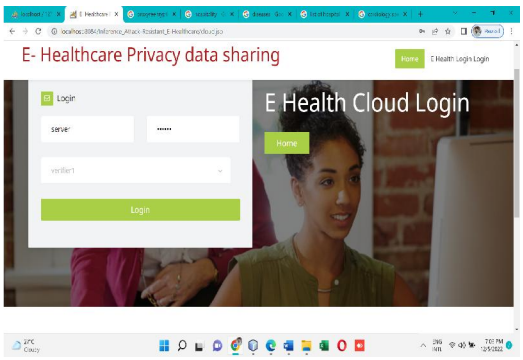


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

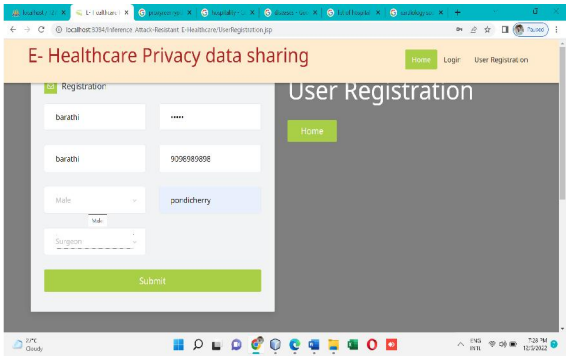
Waiting for approved E health cloud



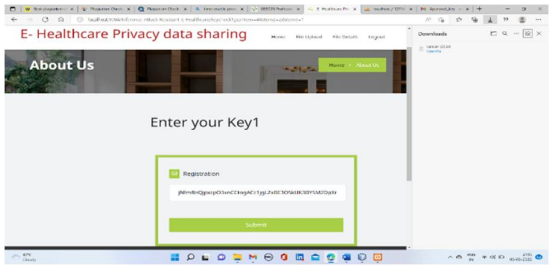
E health cloud login



User registration



File key to download



V. CONCLUSION

We create a fine-grained access control e-healthcare cloud system that is resistant to inference attacks. We begin by suggesting a Time proxy re encryption scheme. We propose that a specialised access policy be defined for each data

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

attribute in the EHR, a secret share be generated for each distinct role attribute, and the secret be reconfigured to encrypt each data attribute. We develop a blind data retrieving protocol based on the Paillier encryption to preserve the access pattern of data attributes in the EHR. provides a re-encryption module as well as time privileges for accessing a specific file . This will allow each user's access right to take effect after a predetermined period of time, and will allow the CSP to automatically re-encrypt cypher texts based on its own time. To deal with user revocation, Time based PRE was implemented to provide access. because we embed randomness there. Furthermore, the inference attack described in our paper is launched by observing the role attributes, access policy, and access pattern (access frequency). We can prevent attackers from performing inference attacks by using our constructions. We intend to build a secure and privacy-preserving e-health cloud system that 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.