WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Framework for Secure Data Access and Searchability for E-Healthcare System

Arjun. P*[1], Akilan. S. K*[2], Manikantan. S*[3], Mr. Rajesh. A*[4]

*[1]UG Student, Dept. of CSBS, E.G.S Pillay Engineering College, Nagapattinam, Tamil Nadu, India
*[2]UG Student, Dept. of CSBS, E.G.S Pillay Engineering College, Nagapattinam, Tamil Nadu, India
*[3]UG Student, Dept. of CSBS, E.G.S Pillay Engineering College, Nagapattinam, Tamil Nadu, India
*[4]Assistant Professor, Dept. of CSBS, E.G.S Pillay Engineering College, Nagapattinam, Tamil Nadu, India
DOI: https://doi.org/10.55248/gengpi.5.0224.0533

ABSTRACT

A growing number of patients in the e-healthcare system receive excellent medical treatment by encrypting their personal health records (PHRs) and sharing them with physicians or medical research organizations. One significant problem, though, is that the encrypted PHRs hinder efficient information searching, which lowers data utilization. The fact that the medical treatment procedure necessitates a doctor's constant online presence presents another problem; not all doctors can afford to be absent under specific conditions. In this work, we develop a novel secure and useful proxy searchable re-encryption technique that enables medical service providers to securely and effectively do remote patient health record monitoring and study. By means of our program, (1) Before being uploaded to the cloud, the medical records of the patients that the devices acquire are encrypted; (2) The PHRs are only accessible to approved medical professionals or research facilities; (3) To minimize information exposure to the cloud server, Alice, the doctor-in-charge, can assign medical research and utilization to Bob, the doctor-in-agent, or to a specific research institution via the cloud server. We demonstrate the security of our scheme and define the meaning of security. Lastly, performance evaluation demonstrates our scheme's effectiveness.

KEYWORDS: Re-encryption, secure data transmission, searchable encryption.

I. INTRODUCTION

The development of technology and sensors and the rapid advancement of human consciousness have pushed sensor networks for electronic medical applications to the level where data letters can be effectively sent and received. The network is a mobile platform called electronic medical sensor network, which collects important personal health information from sensor devices embedded in patient equipment to provide good and good treatment to patients. Doctors can use this information to better diagnose and treat patients' needs, while clinical researchers and analysts can use analytics to gain deeper insights into diseases. However, storing this data in cloud storage provided by third-party service providers can increase the risk of data leaks and security breaches because neither doctors nor patients can control the information once the data is separated. To solve this problem, the privacy and security of external data must be protected.

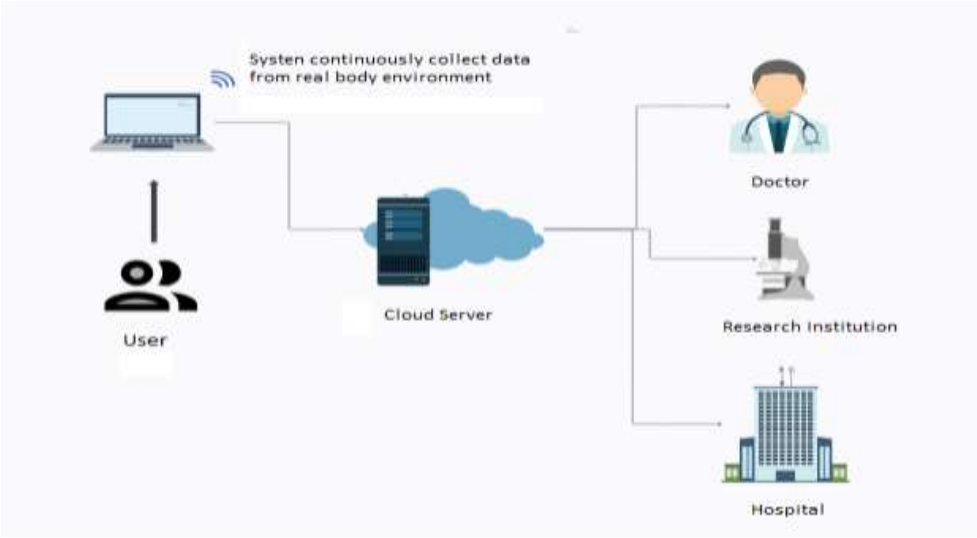

Fig 1: ARCHITECTURE

Hospitals often allow agencies such as the Centers for Disease Control and Prevention (CDC) to access patient medical records stored on cloud servers in efforts to prevent and prevent disease, but this has raised concerns about the disclosure of patient information. Encrypting PHRs stored on cloud platforms is important to prevent data leakage. Searchable encryption technology allows encrypted PHRs to be uploaded to a cloud server, allowing doctors or researchers to use a trapdoor to enable encrypted keyword searches without going directly to free or keyword records.

CDC Leverages Innovative Encryption for Clinical Care and Data Recovery Encrypted PHRs, but doctors' expectations can easily become problematic. Intermediary Re-Encryption (PRE) aims to solve this problem by allowing trusted intermediaries to securely transmit doctors' secrets. However, existing PRE methods have limitations. Intermediaries have great power to alter the encrypted message, regardless of the password used, and there is a risk of conflict if unscrupulous parties' band together to compromise the administrator's identity. This affects the security of the system, and should limit the operation of the name server to increase security and protect the confidentiality of patient information. More importantly, while advances in electronic healthcare provide significant benefits to patient care and medical research, ensuring the privacy and security of medical records is also crucial. This includes using strong encryption, improving the encryption process, and restricting access to sensitive information to reduce risk and protect patient privacy in the digital age.

II. RELATED WORKS

As cloud computing advances quickly, more and more patients are prepared to transfer their PHRs to cloud servers in order to take advantage of the convenient services offered. These PHRs are often kept in encrypted form on the cloud to safeguard data security and private user information. However, when the user tries to access files containing some intriguing keywords, data encryption gets in the way of efficient data useIn order to safeguard sensitive healthcare files on cloud storage and allow cloud servers to search on the encrypted data under patient control, Yang et al. presented a secure, searchable, and privacy-preserving e-health system based on searchable encryption. Boneh et al. introduced the idea of public-key encryption with keyword search (PEKS) and provided the first PEKS implementation for an e-healthcare system operating in a public key environment. Later, the consistency notion was proposed and the PEKS concept was reviewed by Abdalla et al.

The e-healthcare system has more expressive searching systems, and searching schemes are suggested to optimize data storage and retrieval in the multi-user environment in order to store a large number of PHRs from several users. In addition to searchable encryption, the Blaze et al. proposed proxy re-encryption (PRE) technique was also used in the e-healthcare system to store and exchange medical data. Recently, proxy re-encryption has been used extensively to enable ciphertext transformation in cloud storage services, making it a very promising cloud computing option. A unidirectional approach was developed in 2005 by Ateniese et al. who also showed how to stop the proxy from working with delegators to reveal the delegator's secret key.

Green and his colleagues introduced a non-transferable proxy re-encryption method that addresses both the PKG tyranny and key escrow issues. Fuzzy conditional proxy re-encryption was presented by Fang et al., along with a concrete construction based on the "set overlap" distance metric. In order to allow a data owner to grant permission for a healthcare analyst to access their data, PRE was implemented in a mobile healthcare social network.

III. PROPOSED SYSTEM

We propose a secure method for data exchange and authorized searching within an e-healthcare framework. In this system, patients consistently collect Personal Health Records (PHRs) through sensors in physical environments. The encrypted PHRs are then submitted to their designated treating physician

for medical purposes. In certain scenarios, Doctor A may wish to share specific PHRs with Doctor B without disclosing the entirety of the records. To obtain access authorization, Doctor A generates a re-encryption key using their private key and Doctor B's public key.

All Directions: There's a more noteworthy predominance of unidirectional mediator re-encryption than multi-directional middle person re-encryption, the appoint] may exchange assents to an outside party, expanding the security hazard. The un directionality of the e Healthcare framework is hence a pivotal highlight. Unnoticeable intermediary in case a malicious client within the secured e-medical care system is able to recognize a re-scrambled cipher text from a interesting cipher content, it'll make a security hazard.

Condition disclosure: Private information is typically included in the condition of the conditional proxy re-encryption scheme. If the condition is made public, the system will be severely harmed. It goes without saying that the intermediary server will receive fewer sensitive data if the intermediary condition is concealed, making the e-medical care framework safer.

Searchable framework: Creating an effective and searchable framework for an e-healthcare system involves a meticulous approach to data organization and accessibility. The foundation lies in a well-defined data model, encompassing patient records, medical history, and related entities with clear interrelationships. The chosen database system should support robust indexing and searching mechanisms, ensuring swift data retrieval. Security measures must be paramount, incorporating user authentication, authorization protocols, and compliance with healthcare privacy regulations.

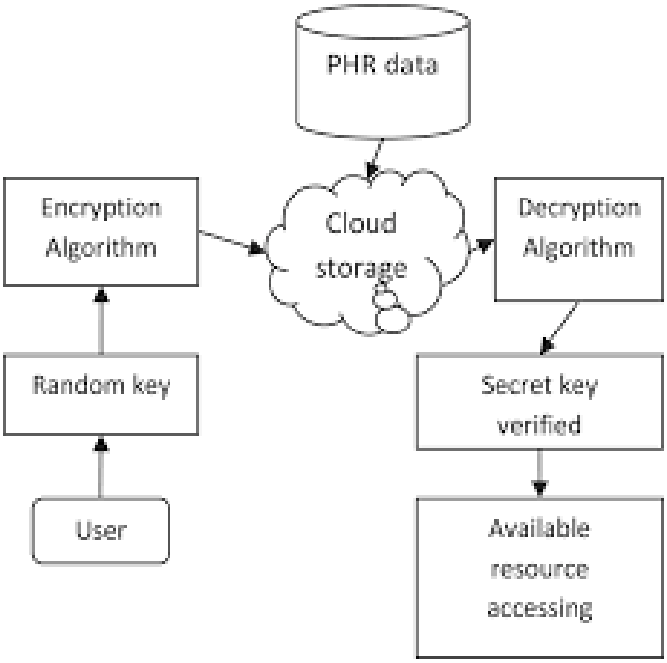

Fig 2: FLOWCHART OF PROPOSED SOLUTION

Agreement and Disagreement: It is impossible to guarantee collusion-resistance when an unscrupulous proxy works with the delegate to export the delegate gator's private key, which would be terrible for the e-healthcare system due to the intrinsic nature of trustworthy property Consequently, the need for a secure e-healthcare system with collusion resistance arises.

IV. IMPLEMENTATION

4.1 PATIENT

The first component is the Patient module, where a new patient registers by providing their details on a registration form. The patient is not allowed to utilize the system once they have enrolled. The patient cannot access the system until the cloud server verifies their identity; this serves as an additional security measure to keep out unauthorized users. The personal healthcare records (PHRs) of patients are managed by this module, which also grants access to the data the patient has provided. PHRs are collected from several devices, encrypted, and uploaded to a secure cloud server. Blood pressure, temperature, and blood group should all be entered by the patient into the patient module. Each patient Every patient has a distinct patient ID in order to reduce duplication.

4.2 DOCTOR

We create the Doctor's section in this module, where a new physician registers by filling out a registration form with their information. Similar to the previous module, the doctor is unable to log in to the system after registering. The doctor can only log in to the system if the cloud server authorizes them;

this was done to increase system security. The PHRs of patients are accessible to authorized doctors through the doctor module. They can safely look for patients using it, and the PHRs' anonymity is guaranteed

4.3 DATA COLLECTION AND ENCRYPTION

This part is responsible for compiling PHRs from various patients and encrypting them before uploading them to the cloud server. It also maintains the availability, confidentiality, and integrity of PHRs by following security guidelines.

4.4 DATA RETRIEVAL PHASE

The information gathering component is in charge of responding to requests from licensed physicians for their medical records. The pertinent data is obtained by the doctor module from the cloud server, decrypted, and returned. They can only access the data if a particular decryption key is available; otherwise, they are unable to access the data. The file will not be shared by all entities according to the key.

4.5 CONDITION AUTHORIZATION

The main feature of the project offers an effective and safe proxy searchable reencryption technique for remote PHR monitoring and inquiry. In order to limit the amount of information that is exposed to the cloud server, Alice, the doctor-in-charge, will assign Bob, the doctor-in-agent, responsibility for medical research and use.

4.6 CLOUD SERVER

The doctor and patient modules are connected through the cloud server module.

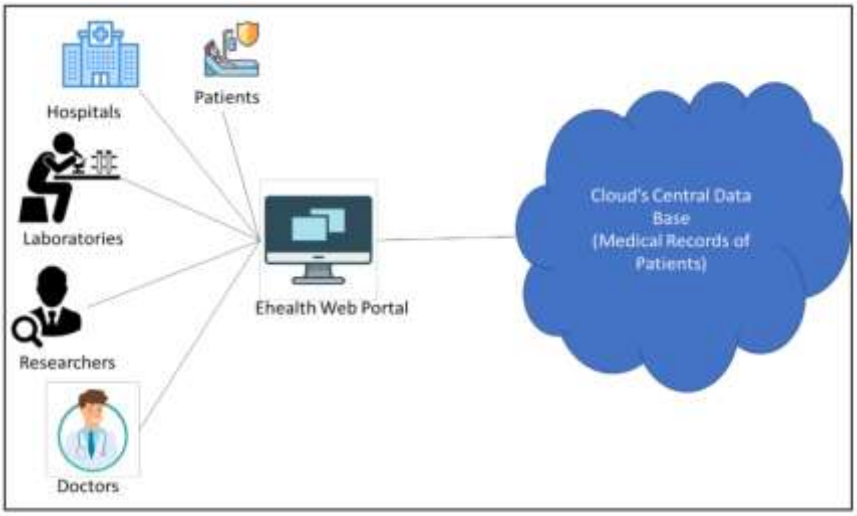

Fig 3: CLOUD SERVER

V. FUTURISTIC WORK

5.1 SCALABILITY

The current system solution is suitable for small-scale installations. Enhancing the system's scalability to support large-scale e-healthcare systems with a huge volume of patients and medical data may be the focus of future work.

5.2 PRIVACY PROTECTION

Even though the system provides excellent security and privacy, there is always room for improvement. Subsequent investigations may focus on developing stronger privacy-protection tactics to guarantee that patients' private medical records are protected even in the case of a breach or attack.

5.3 INTEGRATION WITH EMERGING TECHNOLOGIES

The system may be integrated with cutting-edge technologies like blockchain, artificial intelligence, and the internet of things to enhance functionality and security. While AI can accomplish the same, block chain, for instance, may be utilized to create a decentralized, impenetrable database for storing PHRs.

VI. CONCLUSION

We presented a proxy-invisible condition-hiding proxy re-encryption technique that enables keyword search and can be applied to secure data delegation and interchange in e-healthcare systems. By providing a re-encryption key, a doctor named Bob (the delegate) can obtain a conditional authorization under our novel method from a doctor named Alice (the delegator). Safe delegation can be enabled by the cloud server using the re-encryption key to perform cipher text transformation, allowing Bob to access the PHRs that were initially encrypted with Alice's public key. Without being aware of the word or the underlying issue, the cloud server may scan encrypted PHRs on the doctor's behalf. Specifically, we achieved proxy-invisibility within the system. The system also has a feature called collusion-resistance, which means that even if one dishonest cloud server conspires with Bob, the delegate, Alice's private key will still be safe. We demonstrated security with a thorough proof, and a performance analysis demonstrates the effectiveness and usefulness of our suggested system.

VII. REFERENCE

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy reencryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1_30, 2006.

[2] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," Concurrency Compute., Pact. Exper., vol. 32, no. 5, p. e5520, Mar. 2020.

[3] I. F. Blake, G. Seroussi, and N. Smart, ``Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series (317)), vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666.

[4] H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authentication as an intelligent process," IEEE Trans. Commun., vol. 67, no. 3, pp. 2260_2273, Mar. 2019

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ``Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptograph.Techn.Berlin, Germany: Springer, 2004, pp. 506_522

[6] Q. Huang, L. Wang, and Y. Yang, ``Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities," Secure. Commun.Netw., vol. 2017, pp. 1_12, Aug. 2017.

[7] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserving high-order bi-Lanczos in cloud-fog computing for industrial applications," IEEE Trans. Ind. Informat., early access, May 28, 2020, doi: 10.1109/TII.2020.2998086

[8] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, ``Secure data storage and searching for industrial IoT by integrating Library. [Online]. Available: http://crypto. stanford.edu/pbcTTGT

[9] L. Fang, W. Susilo, C. Ge, and J. Wang, ``Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search,'' Theor.Comput. Sci., vol. 462, pp. 3958, Nov. 2012.

[10] L. Fang, J. Wang, C. Ge, and Y. Ren, ``Fuzzy conditional proxy re-encryption,'' Sci. China Inf. Sci., vol. 56, no. 5, pp. 113, May 2013.

[11] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserving high order bi Lanczos in cloud-fog computing for industrial applications,'' IEEE Trans. Ind. Informat, early access, May 28, 2020, doi:10.1109/TII.2020.2998086.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy re-encryption schemes with applications to secure distributed storage,'' ACMTrans. Inf. Syst. Secur., vol. 9, no. 1, pp. 130, 2006.

[13] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy reencryption for e-healthcare data sharing in mobile cloud computing,'' Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520, Mar. 2020.

[14] M. Blaze, G. Bleumer, and M. Strauss, ``Divertible protocols and atomic proxy cryptography,'' in Advances in Cryptology-EUROCRYPT. Berlin, Germany: Springer, 1998, pp. 127144.

[15] T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personal healthcare records using certicateless proxy re-encryption in cloud,''Trans. Emerg.Telecommun.Technol., vol. 29, no. 6, p. e3309, Jun. 2018.