
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

DSAS A SECURE DATA SHARING AND AUTHORIZED SEARCHABLE FRAMEWORK FOR E-HEALTH CARE SYSTEM

[1]SMT.S ARUNA, [2]SALADI ASRITHA DEVI

[1](Assistant Professor), MCA, Swarnandhra College

[234]MCA, scholar, Swarnandhra College

ABSTRACT

Encouraging patients to share encrypted personal healthcare records (PHRs) with physicians or medical research organizations allows e-healthcare systems to provide high-quality medical services to more and more people. Nevertheless, a significant concern is that encrypted PHRs hinder efficient information search, leading to a reduction in data utilization. The fact that all physicians (or at least some of them) may not have the means to be online constantly throughout patient care is another problem. In this study, we provide a novel proxy searchable re-encryption method that is both secure and practical. This scheme enables medical service providers to easily and securely conduct research and monitoring of patient health records remotely. Our DSAS scheme has three main features: (1) all patient healthcare records are encrypted before being uploaded to the cloud, guaranteeing that the data remains private and secure; (2) access to the data is restricted to authorized doctors or research institutions; (3) the owner, who is the doctor in charge, can use the cloud to assign medical research and usage to the user, who is the doctor in agent, or a specific research institution, thus reducing the amount of data exposed to the cloud. Our approach is secure, and we define the meaning of security. Evaluation of performance indicates that our system is efficient.

1.INTRODUCTION

Securely exchanging encrypted Personal Healthcare Records (PHRs) with healthcare providers and research organizations allows an expanding number of people to benefit from high-quality medical services in the area of e-healthcare systems. However, a significant challenge arises from

the encryption itself, as it hampers the effective search and utilization of information within these encrypted records. This limitation leads to a reduction in the overall usability and accessibility of valuable healthcare data.

Moreover, the traditional medical treatment process often demands that doctors remain online constantly, which can be impractical and costly for many healthcare professionals, especially under certain circumstances such as travel or emergencies. This requirement for continuous online presence poses a barrier to seamless and efficient healthcare service delivery, highlighting the need for innovative solutions that can address these challenges effectively.

In response to these critical issues, this paper presents a novel and secure Proxy Searchable Re-encryption Scheme (DSAS) designed specifically for e-healthcare systems. DSAS aims to enable medical service providers to monitor and conduct research on remote PHRs securely and efficiently. Encrypting patient health records (PHRs) before uploading them to a cloud server is one of the key elements of DSAS that guarantees the highest level of privacy and confidentiality for PHRs.

To further improve data security and prevent unwanted access, DSAS limits access to PHRs to only approved physicians or research institutes. The DSAS cloud server also makes it easy for the chief medical officer (Alice) to delegate medical research and utilization duties to other doctors (Bob) or even to certain research organizations.This delegation mechanism not only streamlines the medical workflow but also minimizes the exposure of sensitive information to the cloud server, bolstering overall data protection. To validate the effectiveness and security of DSAS, we provide a formalized security definition and conduct rigorous security proofs to demonstrate the scheme's robustness against various potential threats and attacks. Finally, comprehensive performance evaluations are conducted to showcase the efficiency and practicality of DSAS in real-world e-healthcare settings, highlighting its potential to significantly enhance the security, accessibility, and usability of encrypted PHRs for medical practitioners and researchers alike.

2.LITERATURE SURVEY

- **E-Healthcare System Using Searchable Encryption**

Authors: Yang et al.

Description: Suggests a solution for electronic healthcare that uses searchable encryption to protect cloud-based sensitive patient information. The system enables encrypted data searches controlled by patients, ensuring privacy and security.

- **Public-Key Encryption with Keyword Search (PEKS)**

Authors: Boneh et al., Abdalla et al., Baek et al.

Description: Introduces PEKS for securely searching encrypted data, further refined by subsequent works to handle large volumes of patient records efficiently.

- **Proxy Re-Encryption (PRE) Technology**

Authors: Blaze et al.

Description: Utilizes PRE technology to securely store and share medical data in e-healthcare systems, preventing collusion and enhancing overall data security.

- **Identity-Based Proxy Re-Encryption (IB-PRE)**

Authors: Green and Ateniese

Description: Extends PRE to identity-based scenarios, enhancing security measures against specific attacks and improving data access control.

- **Proxy-Invisible Conditional Proxy Re-Encryption (CPRE)**

Authors: Seo et al.

Description: Proposes a proxy-invisible CPRE scheme to enhance security measures in e-healthcare systems, focusing on mitigating potential vulnerabilities.

- **Addressing PKG Despotism and Key Escrow**

Authors: He et al.

Description: Highlights solutions for PKG despotism and key escrow issues in proxy re-encryption schemes, ensuring better privacy and data security.

- **Fuzzy Conditional Proxy Re-Encryption (FCPRE)**

Authors: Fang et al.

Description: Introduces FCPRE, enhancing security measures in proxy re-encryption systems by incorporating fuzzy logic and conditional access controls.

- **Proxy Re-Encryption with Keyword Search (PRES)**

Authors: Shao et al.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

Description: Enables patients to securely delegate search capabilities using PRES, although some schemes may pose risks like unrestricted access.

- **Conditional Proxy Re-Encryption (CPRE) for Access Control**

Authors: Weng et al.

Description: Proposes CPRE for limiting access based on specific conditions, ensuring data security without compromising privacy in e-healthcare systems.

- **Ongoing Research in CPRE and Privacy Preservation**

Description: Ongoing research efforts focus on improving CPRE schemes without compromising privacy, with a particular emphasis on enhancing security measures in e-healthcare networks.

This literature survey provides an overview of advanced security mechanisms and encryption techniques applied in e-healthcare systems to protect sensitive medical data, ensuring privacy, data integrity, and access control.

3. EXISTING SYSTEM

To safeguard private healthcare information stored in the cloud, Yang et al. suggested an electronic healthcare system that makes use of searchable encryption. The cloud server may search patients' encrypted data using this system. Prior to its refinement by Abdalla et al. and Baek et al., public-key encryption with keyword search (PEKS) was developed by Boneh et al. Additionally, more sophisticated searching algorithms were created to effectively manage a huge number of patient data.

Another approach to safely storing and sharing medical data in e-healthcare systems is the proxy re-encryption (PRE) technique developed by Blaze et al. It makes data more secure and stops people from working together. To further strengthen protection against specific assaults, Green and Ateniese expanded this concept to identity-based proxy re-encryption.To improve safety, Seo et al. suggested a proxy-invisible CPRE method. Concerns about key escrow and PKG tyranny in proxy re-encryption were discussed by him and others.

Additional security was added by Fang et al. with the use of fuzzy conditional proxy re-encryption. The delegation and access control features of PRE have found their way into mobile healthcare networks.
Patients may safely delegate search skills using Proxy Re-Encryption with Keyword

Search (PRES), developed by Shao et al. Unrestricted access is one security concern that certain PRE systems provide. Weng et al. proposed conditional proxy re-encryption to limit access based on specific conditions, ensuring data security without leaking sensitive information. Ongoing research focuses on improving CPRE schemes without compromising privacy.

The operations performed in the described e-healthcare system include:

Encryption: Prior to being uploaded to the cloud server, the encrypted versions of patients' healthcare records are stored on the devices. This protects the privacy and secrecy of patients' medical records.

- **Access Control**: The encrypted protected health records kept on the cloud server can only be accessed by authorized medical professionals or research organization. This restricts access to sensitive medical data and prevents unauthorized parties from viewing the information.
- **Delegation**: Through the cloud server, the chief medical officer (Alice) may assign responsibilities for medical research and utilization to other doctors (Bob) or to certain research institutes. This delegation mechanism allows for efficient collaboration and workflow management among healthcare professionals.
- **Searchable Encryption**: The system employs searchable encryption techniques, allowing authorized users to perform encrypted keyword searches on the cloud-stored data. This enables efficient information retrieval without compromising data privacy.
- **Proxy Re-Encryption (PRE):** Proxy re-encryption technology is utilized to securely transform encrypted data between doctors, facilitating data sharing and delegation while maintaining data security and privacy.

Disadvantages:

- The system is not implemented a conditional proxy re-encryption searchable method to provide more security on datasets.
- The system is not implemented Hashing techniques on each datasets for more secure and safe data transaction.

3.1 PROPOSED SYSTEM

In the proposed system,the following contributions have been developed :

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

- **Uni-Directional**: To prevent the delegatee from increasing privacy exposure by passing permissions to a third party, unidirectional proxy re-encryption is preferable to multi-directional proxy re-encryption.
- Therefore, e-healthcare systems must have unidirectionality.
- Condition-Hiding: Conditional proxy re-encryption schemes often include conditions that conceal private information. The system will suffer significant damage in the event that the problem is made public. The e-healthcare system is naturally more safe if the proxy condition is masked, since the proxy server will get less critical information.
- Collusion-Resistance: Since collusion-resistance is an inherent quality of trustworthy properties, it cannot be ensured that a dishonest proxy would not collaborate with the delegatee to export the private key of the delegator, since this would have catastrophic effects on the e-healthcare system. For security reasons, it is believed that the proxy server, which is often used for permitted work, is untrustworthy. Therefore, a secure e-healthcare system must have collusion-resistance.

Advantages:

● Data security: Prior to being sent to the server in the cloud, the data gathered from the patients' sensor devices is encrypted. Since the cloud server cannot decipher the encrypted PHRs, data privacy and confidentiality are guaranteed.

Conditional authorization: Under the conditional permission, if the in-charge doctor (Owner) is not present, another doctor (User) may be assigned the work via a cloud server. This way, the cloud server doesn't have to decrypt the patient health records, which minimizes the exposure of information.

Condition-hiding: The privacy of patients' protected health records (PHRs) is protected by our approach in two ways: first, by encrypting the data, and second, by keeping the condition's identity hidden in the re-encryption key.

4. OUTPUT SCREENS

Home Page

ISSN2321-2152

www.ijmece .com

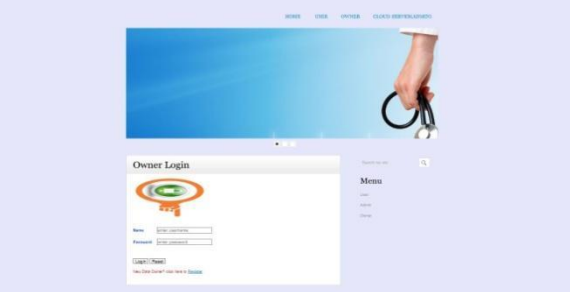
Vol 12, Issue 2, 2024

Home page of our application

User Login Page

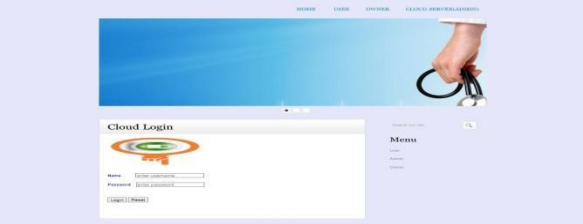
User need login with his name and password

Owner Login Page



Owner need to login with his username and password

Cloud/Admin Login Page



Admin need to login with his credentials

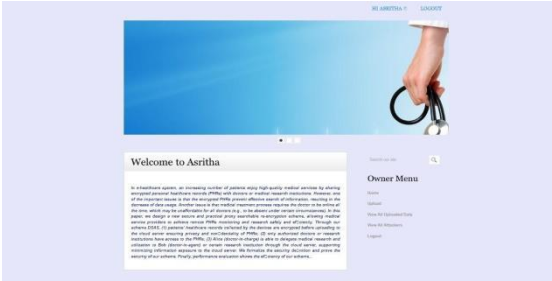
User Dashboard

After successful user login he is entered into his dashboard

User Operation

1.User accessing particular patient details

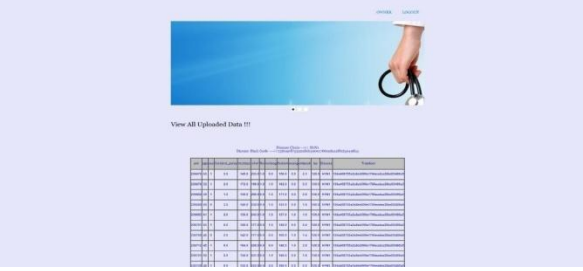
Owner Dashboard



Owner Operations

1.Owner can upload a File

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

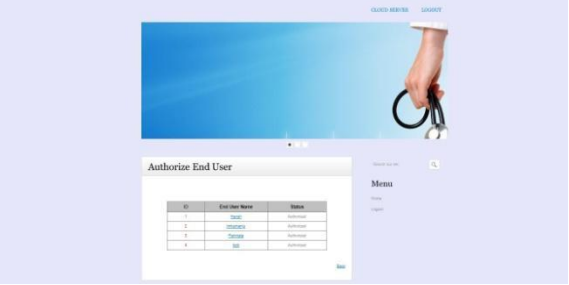


2.Owner can view apploaded file information

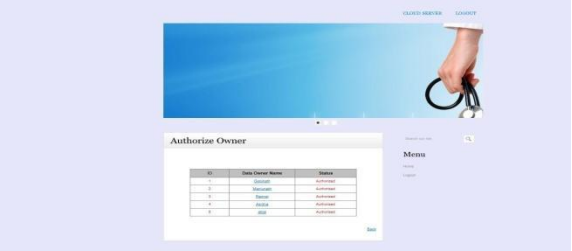
3.Owner can view all attackers

Cloud/Admin Dashboard

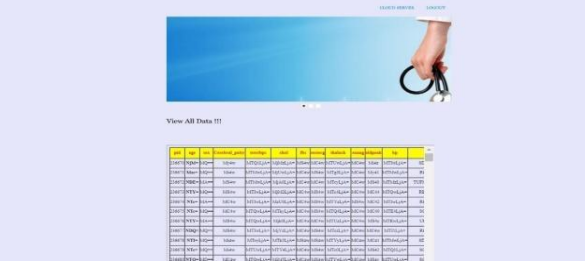
Cloud Operations:



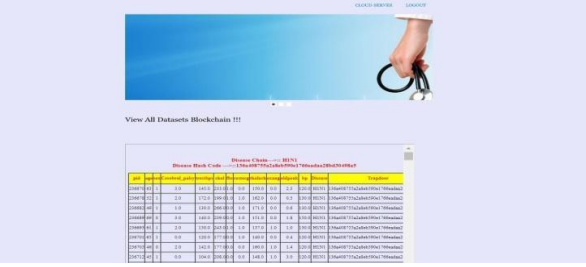
1.Admin can view and autherize User



2.Admin can view and authorize Owner also



3.Admin can only view the patient info in encrypted form

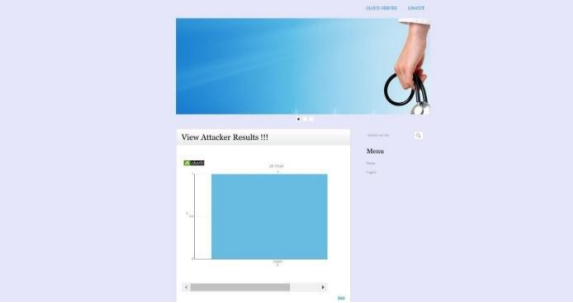


4.Admin can view the decrypted patient info inDataBlockChain

5.Admin can view all attackers information

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

6.Admin canview disease results



7.Admin can view attackers result

5. CONCLUSION

Overall, the e-healthcare domain's approved searching architecture and system for safe data exchange show a strong commitment to protecting data privacy, integrity, and access control. Medical records and other sensitive patient data are encrypted before storage and transmission in the database using industry-standard algorithms like RSA and AES. Datasets may be efficiently uploaded to the system, and all patient information is protected before storage. On top of that, the search feature allows authorized users to get pertinent patient data using certain keywords without compromising data privacy or confidentiality. The system's architecture and execution as a whole demonstrate a thorough strategy for protecting patient information and encouraging safe data exchange in electronic health records.

6.REFERENCES

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, ``Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005,pp. 205_222. [2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1_30, 2006. [3] J. Baek, R. Safavi-Naini, and W. Susilo, ``Public key encryption with keyword search revisited," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA),2008, pp. 1249_1259. [4] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud com-puting," Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520,Mar. 2020. [5] T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personal healthcare records using certi_cateless proxy re-encryption in cloud,"Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. e3309,

ISSN2321-2152

www.ijmece .com

Vol 12, Issue 2, 2024

Jun. 2018. [6] 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