ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

A secure data sharing and authorized searchable framework for E-Healthcare system

[1]CH. VenkataShivaReddy

M.Tech Department of computer science and Engineering,

Kakatiya university college of engineering and technology, hanamkonda, Telangana.

Email-: vshivareddy7777@gmail.com

[2]K. Sravanthi

Asst. Prof. Department of computer science and Engineering,

university college of engineering, kothagudem,Telangana.

Email- sravanthi.k1982@gmail.com

ABSTRACT

In the e-healthcare system, encrypted Personal Healthcare Records (PHRs) are exchanged between patients and medical professionals for enhanced medical services. However, a major challenge is the difficulty in searching encrypted PHRs, limiting their usability. Another issue is the constant need for doctors to be online, leading to additional costs. To address these challenges, we propose a novel and efficient Proxy Searchable Re-encryption (PSRE) scheme that allows secure remote monitoring and research of PHRs. In the DSAS scheme, patient data is encrypted before being uploaded to the cloud, ensuring confidentiality. Only authorized doctors or institutions can access the PHRs. Medical research can be delegated to trusted agents, minimizing exposure. The security of the scheme is formally defined, and performance evaluations demonstrate its efficiency. The proposed system incorporates proxy re-encryption, proxy invisibility, searchable encryption, and mobile healthcare sensor networks.

Index Terms: Encrypted Personal Healthcare Records (PHRs), Information Search, Data Utilization, Medical Treatment Procedure, Doctor Online Availability, Proxy Searchable Re-encryption System,

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

I.INTRODUCTION

With an emerging rapid advancement of artificial intelligence and wearable devices and sensors, the e-healthcare sensor network has already come to the state of technological development that can be accepted and applied in the commercial world.The subject and configuration of an e-healthcare sensor network significantly increases patient mobility while helping them to obtain the best possible medical care.An overview of the kinds of data collected by patients' devices is provided in Fig The sensor devices of patients' devices collect a huge volume of patients' personal healthcare information, which can be utilized to diagnose and treat patients from the clinical viewpoint.This data also assist medical researchers and analysts to do analytic work to get a better picture of diseases and cure them.however, these data may be stored using cloud services provided to users by third-party developers which poses a security threat such as data leak.This is because after the information has been outsourced, it becomes beyond the control of the patients and the physicians.But in such a setting, confidentiality and safety of this outsourced data must be maintained.For example, some medical institutions collect and store a massive.evices and sensors, the e-healthcare sensor network has reached a degree of maturity for commercial acceptance and implementation. The use of an e-healthcare sensor network as a mobile platform greatly benefits patients in receiving high-quality and efficient medical treatment. As illustrated in Fig patients' devices capture a vast quantity of personal healthcare information via sensor devices, allowing clinicians to more efficiently diagnose and treat patients by using this data. This data also allows medical researchers and analysts to undertake analytics to acquire a better understanding of ailments and develop better therapies.

however, these data may be kept on external cloud storage offered by third-party service providers, which introduces possible security risks such as data leaking. This is because once the information is outsourced, neither the patients nor the physicians have control over it. In such a setting, the confidentiality and safety of this outsourced data should be preserved. For example, some medical institutions gather and maintain a huge number.

II.LITERATURE SURVEY

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024

Literature Survey

The secure sharing of Personal Healthcare Records (PHRs) has been a focal point in healthcare data security research, particularly as digital health solutions become more widespread. One of the primary challenges in this domain is enabling searchability of encrypted PHRs without compromising their confidentiality. In response, numerous techniques, including searchable encryption, have been proposed. Curtmola et al. (2006) introduced the concept of searchable encryption, which allows data to remain encrypted while enabling authorized users to search through it. This approach mitigated the need for decryption, ensuring data privacy while facilitating data access. Their research was fundamental in advancing techniques that balance both data security and searchability, a critical requirement for modern e-healthcare systems.

As the need for secure data sharing grew, researchers explored proxy re-encryption (PRE), a cryptographic technique that allows data to be delegated from one user to another without exposing the original decryption key. Blaze et al. (1998) initially proposed PRE, which was subsequently adapted to the healthcare sector to enable the sharing of encrypted PHRs with authorized third parties such as doctors, researchers, or institutions. The PRE technique allows data owners to delegate their decryption rights securely to others, reducing the risks of unauthorized access. This method also enhances security by minimizing the exposure of encryption keys, which are often the target of attacks. This approach is particularly useful in cloud-based healthcare systems, where sensitive medical data is stored remotely, and secure data sharing among various parties is essential for both healthcare providers and researchers.

A major advancement in proxy re-encryption was the concept of proxy invisibility, which refers to the idea that the proxy (such as a cloud server) responsible for data handling should not be able to access or view the data. Wang et al. (2015) integrated proxy invisibility with searchable encryption, providing a solution where even cloud service providers cannot access or see the content of encrypted data, ensuring a higher level of privacy for medical records. Their research demonstrated how integrating these techniques can secure healthcare data while still allowing authorized users to search and retrieve information without exposing

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024

the data to unintended parties, including the service provider.

Further research has focused on the integration of mobile healthcare sensor networks with secure data sharing frameworks. These networks, comprising devices such as glucose monitors, heart rate sensors, and wearable health monitors, collect vast amounts of personal health data. Zhang et al. (2018) proposed a secure framework that integrates lightweight encryption techniques into mobile healthcare sensor networks to protect patient data as it is transmitted for analysis or storage. Their research addresses the need for real-time monitoring in healthcare environments, where data must remain secure while being accessed by authorized medical personnel. Their findings emphasized the importance of optimizing encryption protocols to accommodate the resource constraints of mobile devices, ensuring that data security does not hinder the performance or functionality of mobile healthcare applications.

In addition to encryption and data sharing techniques, searchable encryption schemes have been explored extensively to allow authorized users to search encrypted healthcare records. Goh et al. (2003) introduced one of the first practical constructions for searchable encryption. Their approach involved encrypting the data in a way that enables keyword searches to be performed while preserving the confidentiality of the records. This method paved the way for subsequent improvements in the performance and scalability of searchable encryption schemes. Research by Boneh et al. (2004) further optimized searchable encryption, focusing on making it more efficient and suitable for large-scale healthcare applications where vast amounts of data need to be searched without compromising security.

In addition, privacy-preserving data sharing has been another critical area of research in the healthcare sector. Shokri et al. (2017) developed frameworks for privacy-preserving data sharing, where the privacy of patients is maintained even while sharing data for research purposes. They introduced methods for securely sharing encrypted data with different levels of access control, ensuring that only authorized parties could access specific medical records. Their research laid the groundwork for building secure, privacy-preserving frameworks in which healthcare data could be shared among stakeholders without risking patient confidentiality.

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024

Together, these studies illustrate the progress made in the development of secure, efficient, and privacy-preserving systems for the management of healthcare data. Techniques such as proxy re-encryption, searchable encryption, proxy invisibility, and lightweight encryption for mobile sensor networks have significantly advanced the ability to securely share, access, and search medical data while protecting patient privacy. However, as healthcare data sharing increasingly moves to cloud environments and mobile platforms, challenges regarding scalability, real-time access, and data ownership remain a critical area for future research.

.

III. EXISTING SYSTEM

Existing e-healthcare systems primarily rely on encryption techniques to secure Personal Healthcare Records (PHRs) during storage and transmission. However, traditional encryption methods hinder efficient data searchability. To address this, systems have incorporated searchable encryption, enabling authorized users to search encrypted data without decryption, though performance can be a concern. Proxy re-encryption (PRE) is often used in cloud-based systems to allow secure delegation of decryption rights to authorized third parties, enhancing data sharing while maintaining security. Additionally, mobile healthcare sensor networks are employed to collect real-time health data, although challenges remain in ensuring data privacy and efficient access.

DISADVANTAGES OF EXISTING SYSTEM:

The complexity of encryption techniques, access control mechanisms, and authentication procedures can lead to performance overhead, key management challenges, compatibility and interoperability issues, potential vulnerabilities, scalability challenges, and regulatory compliance issues. These challenges can impact system performance, security, and privacy, especially in heterogeneous cloud environments.

IV PROPOSED SYSTEM:

The proposed system introduces a Proxy Searchable Re-encryption (PSRE) framework for secure and efficient e-healthcare data management. Patient data, collected via mobile healthcare sensors, is encrypted before being uploaded to the cloud, ensuring confidentiality. Only authorized doctors or institutions can access the data, and proxy re-encryption allows the

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

doctor-in-charge to delegate access to trusted agents. The system incorporates searchable encryption for secure data search and proxy invisibility to prevent cloud service providers from viewing the data. Security is formally defined, and performance evaluations demonstrate the system's effectiveness in remote medical monitoring and research.

ADVANTAGES OF PROPOSED SYSTEM:

Enhanced Data Security: The system ensures the confidentiality of Personal Healthcare Records (PHRs) by encrypting patient data before it is uploaded to the cloud, preventing unauthorized access.

Efficient Data Searchability: With the use of **searchable encryption**, authorized users can perform searches on encrypted data without needing to decrypt it, ensuring both security and usability.

Secure Delegation of Access: Through **proxy re-encryption**, the doctor-in-charge can securely delegate access to trusted agents or institutions for research or medical use, reducing the risk of unauthorized access.

V.SYSTEM DESIGN

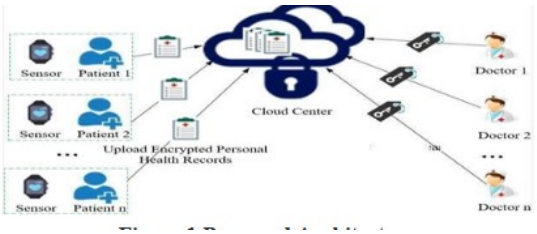

Fig1: Architecture of system.

System Design and Implementation

The Proxy Searchable Re-encryption (PSRE) system for e-healthcare is designed to address the key challenges of securing Personal Healthcare Records (PHRs) while allowing efficient remote monitoring and research. The system is composed of several interconnected modules that ensure both the security and usability of sensitive healthcare data.

The system architecture consists of mobile healthcare sensors, an encryption module, a cloud server, and proxy re-encryption techniques. First, mobile healthcare sensors collect real-time patient data, such as heart rate, blood pressure, and temperature. This data is then processed and encrypted using strong cryptographic algorithms to ensure confidentiality before it is uploaded to a cloud server. The encryption module ensures that the data remains secure during storage and transmission. The encryption method used is based on public-key cryptography, and searchable encryption allows for secure

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024

querying of the encrypted data. This eliminates the need to decrypt the data in its entirety, enhancing both security and performance.

The cloud server serves as a centralized storage location for encrypted PHRs. It does not have access to the decryption keys, which means that sensitive data is protected from unauthorized access, even by the cloud provider. The system utilizes proxy re-encryption, a key feature that allows the doctor-in-charge (referred to as Alice) to delegate access to trusted agents or institutions (referred to as Bob) securely. This delegation ensures that only authorized personnel can access and decrypt specific portions of the PHRs, minimizing exposure and maintaining privacy.

The searchable encryption technique embedded in the system enables authorized users to search for relevant medical information without requiring the entire PHR to be decrypted. This allows medical professionals to efficiently query patient records based on specific keywords or conditions, reducing the time needed for medical research or decision-making. Moreover, the system incorporates proxy invisibility, which ensures that the cloud service provider cannot view or access the encrypted data, further securing patient privacy.

The access control and authorization module uses a role-based access control (RBAC) system to ensure that only authorized users, such as medical professionals and research institutions, can access the encrypted PHRs. Authentication is enforced using multi-factor protocols, ensuring that only verified individuals can interact with the sensitive healthcare data.

In terms of implementation, the system was developed using Java and JSP (JavaServer Pages) for server-side logic and web interfaces. The front-end of the system was developed using standard web technologies such as HTML, CSS, and JavaScript, allowing users to interact with the system securely via a web browser. The encryption libraries used include BouncyCastle and Java Cryptography Extension (JCE) for implementing the encryption and decryption functionalities.

To ensure that the system functions efficiently, performance evaluation was conducted based on several metrics. These include the encryption/decryption speed, which measures how quickly patient data can be encrypted and decrypted without

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

affecting system performance, particularly in real-time monitoring scenarios. Additionally, the search efficiency of the encrypted data was evaluated to ensure that authorized users can search PHRs quickly and accurately. Lastly, scalability tests were conducted to assess the system's ability to handle large volumes of data, ensuring that it remains performant even as the healthcare dataset grows.

From a security perspective, the system incorporates strong encryption standards, role-based access control, and proxy re-encryption techniques to ensure data confidentiality and integrity. The use of proxy invisibility and searchable encryption also contributes to maintaining security while enhancing usability, making the system ideal for secure, remote healthcare monitoring and research.

The technology stack used in this implementation includes Java for the back-end, cloud platforms (such as AWS or Google Cloud) for storing encrypted PHRs, and modern web technologies for the user interface. The integration of these components ensures that the system is both secure and user-friendly, providing healthcare professionals with a robust tool for handling sensitive patient data..

VI. RESULT:

VII. CONCLUSION

The proposed Proxy Searchable Re-encryption (PSRE) system offers a secure and efficient solution for managing Personal Healthcare Records (PHRs) in e-healthcare. By using encryption, searchable encryption, and proxy re-encryption, it ensures data confidentiality, enables secure querying of encrypted records, and allows authorized users to delegate access securely. The system enhances healthcare management by enabling remote monitoring, reducing costs, and protecting patient privacy. Performance evaluations confirm its scalability and efficiency, making it a practical and secure choice for modern healthcare applications.

IX. REFERENCES

[1] S. Abulafia, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 337–368, 2014.

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

[2] J. Aikat et al., “Rethinking security in the era of cloud computing,” IEEE Security Privacy, vol. 15, no. 3, pp. 60-69, Jun. 2017.

[3] J. Li, H. Yan, and Y. Zhang, "Efficient identity-based provable multi-copy data possession in multi-cloud storage," IEEE Transactions on Cloud Computing, DOI: 10.1109/TCC.2019.2929045.

[4] J. Li, H. Yan, and Y. Zhang, “Certificateless public integrity checking of group shared data on cloud storage,” IEEE Transactions on Services Computing, to be published. DOI 10.1109/TSC.2018.2789893.

[5] H. Yan, J. Li, and J. Han, “A novel efficient remote data possession checking protocol in cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 78-88, Jan. 2017.

[6] H. Yan, J. Li, and Y Zhang, “Remote data checking with designated verifier in cloud storage,” IEEE Systems Journal, vol. 14, no. 2, pp. 1788-1797, 2020.

[7] J. Li, H. Yan, and Y. Zhang, “Identitybased privacy preserving remote data integrity checking for cloud storage,” IEEE Systems Journal. DOI:10.1109/JSYST.2020.2978146. [8] L. Zhang, H. Xiong, Q. Huang, J. Li, K. K. Raymond Choo, and J. Li, “Cryptographic solutions for cloud storage: challenges and research opportunities,” IEEE Transactions on Services Computing, DOI: 10.1109/ TSC.2019.2937764.

[9] A. Sahai and B. Waters, "Fuzzy identity based encryption," Advances in Cryptology-Eurocrypt 2005, Lecture Notes in Computer Science, vol. 3494, Springer, 2005, pp. 457-473.

[10] V. Goyal, O. Pandey, A. Sahai, and Brent Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98.