Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 14, Issue. 2, No. 2: 2023
ISSN : **1906-9685**

SESPHAR CLOUD AND AI: SECURE HEALTH RECORD SHARING METHODOLOGY

Ms. S. Karthiga, M.Sc., B.Ed., Assistant Professor, Department of Computer Science Marudhar Kesari Jain College for Women, Tamilnadu karthiga@mkjc.in

Abstract

SESPHAR is a methodology designed to enable secure sharing of personal health records in the cloud and AI. SESPHAR addresses the challenges of data interoperability, functional integration, and security issues in health care clouds.It leverages innovative technologies, such as personal health record systems, to provide individuals with access to their medical records, self-management of diseases, and improved communication with healthcare providers. SESPHAR takes into consideration the confidentiality, integrity, and authenticity of personal health data stored in cloud storage. SESPHAR employs a key aggregate cryptosystem for access control revocation, ensuring that only authorized entities have access to the private health records within the cloud storage.

1.Introduction

Personal health records are systems designed to manage and store an individual's health information. These records offer various features, including the ability to view and input personal health data, exchange secure messages with healthcare providers, schedule appointments, and support clinical decisions. The goal of personal health records is to provide individuals with a comprehensive and accurate summary of their health and medical history, making this information accessible to authorized entities with the necessary electronic credentials (Chatterjee et al., 2013).SESPHAR recognizes the importance of personal health records in empowering individuals to take control of their healthcare and make informed decisions. ## The Need for Secure Sharing of Personal Health Records in the Cloud

The need for secure sharing of personal health records in the cloud arises due to several factors.

Securing Personal Health Records in the Cloud

Securing personal health records in the cloud is a critical aspect to protect the privacy and confidentiality of sensitive health information. This can be achieved through the implementation of robust security measures such as encryption and access control mechanisms.

Securing personal health records (PHRs) in the cloud is a critical aspect of ensuring the privacy and confidentiality of sensitive health information. The cloud offers numerous benefits for storing and accessing health records, such as increased accessibility and scalability, but it also introduces security challenges that need to be addressed. Here are some key considerations for securing personal health records in the cloud:

1. Encryption -

Data in Transit: Use secure communication protocols (e.g., HTTPS) to encrypt data while it is being transmitted between the user's device and the cloud server.

Data at Rest: Employ strong encryption mechanisms to protect health records stored on the cloud servers. This ensures that even if unauthorized access occurs, the data remains unreadable without the proper decryption keys.

2. Access Controls - Implement robust access control mechanisms to restrict access to personal health records. Only authorized individuals should have access to specific records based on their roles and responsibilities.

Use multi-factor authentication (MFA) to add an extra layer of security, requiring users to provide multiple forms of identification before accessing health records.

3. Authentication - Employ strong user authentication methods to verify the identity of individuals accessing the PHRs. This helps prevent unauthorized access to sensitive health information.

Regularly update and strengthen password policies to ensure that user credentials are secure.

4. Audit Trails: - Implement comprehensive audit trails to log and monitor all activities related to PHRs. This includes tracking who accessed the records, when they were accessed, and any modifications made. Regularly review these logs for any suspicious activities.

5. Data Backups

- Regularly backup health records to prevent data loss in case of accidental deletion, system failures, or cyber attacks. Ensure that backup data is also encrypted and stored securely.

6. Compliance with Regulations:

Familiarize yourself with and adhere to relevant data protection regulations and standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in the European Union.

7. Security Patching:

- Keep all software, including operating systems and applications, up-to-date with the latest security patches. Regularly update and patch the cloud infrastructure to address any vulnerabilities.

8. Security Training:

- Provide ongoing security training for employees and users to raise awareness about best practices, social engineering threats, and the importance of maintaining a secure environment.

9. Secure Development Practices:

- If you are developing a custom PHR application, follow secure coding practices to minimize vulnerabilities. Regularly conduct security assessments and code reviews.

10. Vendor Security:

- If using a third-party cloud service provider, ensure that they have robust security measures in place. Review and understand the provider's security policies, compliance certifications, and data protection practices.

By implementing these measures, organizations can enhance the security of personal health records in the cloud and build trust among users regarding the confidentiality and integrity of their health information. Regularly reassess and update security measures to stay ahead of evolving threats and technology.

2.The Role of AI in Personal Health Records

AI plays a significant role in enhancing the capabilities of personal health record systems.

It can assist in analyzing and interpreting large amounts of health data, identifying patterns and trends, offering personalized recommendations for treatment plans, and aiding in clinical decision making. Furthermore, AI can contribute to the security of personal health records by employing machine learning algorithms to detect and prevent potential security breaches or unauthorized access attempts in real time.

Artificial Intelligence (AI) plays a significant and evolving role in managing and utilizing Personal Health Records (PHRs). Here are several ways in which AI contributes to the enhancement of PHRs:

Methodology for Secure Sharing of Personal Health Records

The SESPHAR methodology provides a comprehensive approach to secure sharing of personal health records in the cloud (Personal Health Record Using Cloud computing Technology, 2020).

It incorporates access control mechanisms, encryption techniques, and key aggregate cryptosystem for revocation of access control.

The methodology also includes the use of secure communication protocols and cryptographic techniques to ensure the confidentiality, integrity, and authenticity of the shared health records. By leveraging the PHR security model and adapting it to the cloud environment, SESPHAR enables authorized persons to securely store and share personal health records stored in the cloud computing environment.

3.SESPHAR: A Comprehensive Overview

SESPHAR is a comprehensive framework that addresses the challenges and concerns associated with secure sharing of personal health records in the cloud. The framework utilizes scalable features of cloud computing to support the storage and sharing of PHR data. It adopts a patient-centric approach, focusing on ensuring the confidentiality, integrity, and authenticity of personal health records.

Impact of SESPHAR on Health Data Management

The secure sharing of personal health records significantly transforms health data management by fostering seamless accessibility and interoperability. This approach enhances care coordination, empowers patients, and facilitates efficient, informed decision-making among healthcare providers. It promotes a patient-centric model, allowing individuals greater control over their health information for more personalized care. Additionally, the streamlined administrative processes and data-driven insights derived from shared records contribute to operational efficiency and evidence-based healthcare practices. However, stringent privacy and security measures are crucial to maintain trust and compliance with regulations. Overall, the secure sharing of personal health records is pivotal for advancing healthcare by integrating technology, improving patient outcomes, and shaping a more interconnected and efficient healthcare ecosystem.

Future Prospects of SESPHAR

The future of secure sharing of personal health records holds great potential for transforming healthcare. As interoperability improves, individuals will have seamless access to their health data, empowering them to actively engage in their care. This shift toward data-driven healthcare will facilitate better care coordination, support tele health services, and enable predictive analytics for early intervention and preventive care.

Advanced cyber security measures will be essential to ensure the privacy and integrity of shared health information. As regulatory frameworks evolve, the integration of wearable devices and IoT data will further enhance the depth and real-time nature of personal health records, contributing to more personalized and efficient healthcare solutions.

Conclusion

In conclusion, the secure sharing of personal health records holds promising implications for the future of healthcare. The seamless exchange of health information is poised to enhance patient engagement, care coordination, and tele health services, ultimately leading to more personalized and effective healthcare delivery. The integration of advanced technologies, such as predictive analytics and wearable devices, has the potential to revolutionize preventive care and contribute valuable insights to medical research. However, to fully realize these benefits, ongoing attention to robust cyber security measures, evolving regulatory frameworks, and addressing privacy concerns is imperative. As the healthcare landscape continues to embrace data-driven solutions, the secure sharing of personal health records stands as a cornerstone for a more interconnected and patient-centric healthcare ecosystem.

References

1. Chatterjee, S., LeRouge, C., & Tremblay, M C. (2013, January 1). Educating Students in Healthcare Information Technology: IS Community Barriers, Challenges, and Paths Forward. https://scite.ai/reports/10.17705/1cais.03301
2. Personal Health Record Using Cloudcomputing Technology. (2020, March 23). https://scite.ai/reports/10.37506/ijphrd.v11i3.832
3. Privacy Preserving Approaches in E-Health Clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.
4. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017.
5. J. Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI: 10.1109/MC.2013.225.