WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Design Of A Secure Data Sharing & Authorized Search for e-Health

Arjumand Afroze [1], Deevela Nishitha [2], Sana Ali [3]

Department of IT, Stanley College of Engineering & Technology for Women,Hyderabad,India.
Email: arjumanddafroze@gmail.com
nishithadeevela@gmail.com
saaaanaali@gmail.com

ABSTRACT :

Our e-healthcare system, DSAS, addresses the challenges of encrypted personal healthcare records (PHRs) hindering effective information search and the need for constant online presence of doctors. DSAS is a secure proxy searchable re-encryption scheme that enables remote and secure monitoring and research of PHRs. It ensures privacy by encrypting records before uploading to the cloud server, with access granted only to authorized healthcare providers or research institutions. Attending doctors can delegate tasks to assisting doctors or research institutions, minimizing information exposure. Our scheme is secure and efficient, as confirmed by performance evaluations.

Keywords: Secure Data Sharing, Authorized data sharing, DSAS, Cloud Computing, Secure e-healthcare System, Searchable Framework, SHA - 256 Algorithm, RSA Algorithm, AES Algorithm

INTRODUCTION:

The progress in artificial intelligence and wearable technology has driven the expansion of e-healthcare sensor networks to a larger scale, transforming the way patient care is delivered. These networks, functioning as mobile platforms, allow for the gathering of detailed personal healthcare records (PHRs) using sensor devices that patients wear. This information gives healthcare professionals the ability to provide more accurate diagnoses and treatments, as well as aiding in medical research and analysis for improved understanding and care. Nevertheless, the storage of PHRs on external cloud services raises worries regarding the security and confidentiality of data. It is crucial to encrypt PHRs on the cloud to ensure privacy and prevent unauthorized access.

Aim & Objectives

The main objective of this project is to create and put into operation a reliable and effective e-healthcare system that utilizes wearable devices and sensors in a sensor network to gather personal healthcare records (PHRs) from patients. The goal of this system is to facilitate precise diagnoses and treatments by healthcare professionals. The project is centered on addressing security issues linked to storing PHRs on external cloud services by utilizing encryption methods like searchable encryption and proxy re-encryption. These strategies guarantee the privacy and authenticity of patient information while enabling efficient data access and secure sharing of access privileges.

1.2 Algorithms

I. **SHA-256 (Secure Hash Algorithm 256-bit):** SHA-256 is commonly utilized to encrypt confidential information like patient details, medical histories, and passwords. It produces a 256-bit encrypted code that is extremely difficult to tamper with and ensures strong security measures.
II. **AES (Advanced Encryption Standard):** AES is a symmetric encryption algorithm widely adopted for securing data in transit and at rest. It offers strong encryption and efficient performance, making it suitable for encrypting sensitive healthcare data.
III. **RSA (Rivest-Shamir-Adleman):** RSA is a widely used asymmetric encryption algorithm for secure communication, digital signatures, and key exchange. It utilizes public and private key pairs, enabling secure data transmission and authentication in e-healthcare systems.

Literature Survey :

a. Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud", Jun. 2018.
Authors: T. Bhatia, A. K. Verma, and G. Sharma
The main goal of the project is to securely share personal healthcare records on mobile devices by implementing certificateless proxy re-encryption in the cloud. This method combines certificateless cryptography and proxy re-encryption to protect the privacy and security of healthcare data, specifically

addressing concerns regarding secure data sharing on cloud platforms.

b. A Survey on Security and Privacy in Electronic Healthcare Systems" in 2023

Authors: B. S.Manoj and N. S. Prasad

The text examines the security and privacy issues in Electronic Healthcare Systems (EHS), emphasizing risks such as unauthorized entry and data leaks. It suggests remedies such as encryption and access restrictions, although it lacks concrete data and consideration of non-technical aspects, calling on stakeholders to incorporate practical examples to strengthen EHS security.

c. Secure Data Sharing in Healthcare: A Review of Techniques and Approaches" in 2024

Authors: M. R. Islam and M. A. Hossain

The research paper discusses the secure sharing of data in the healthcare sector, focusing on access control, encryption methods, and cloud computing technologies. It emphasizes the advantages of enhanced security and privacy while also acknowledging the difficulties and regulatory requirements involved. The paper offers healthcare providers valuable information for developing successful approaches to safeguard patient data and improve healthcare outcomes.

System Requirements :

H/W System Configuration:-

Processor	-	Pentium –IV
RAM	-	4 GB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

Software Requirements:

Operating System	-	Windows XP
Coding Language	-	Java/J2EE(JSP,Servlet)
Front End	-	J2EE
Back End	-	MySQL

System Analysis & Design :

4.1 Modules

Alice Module:

I. In this module, there are n numbers of users are present.
II. User should register before doing some operations.
III. After registering successfully he has to wait for admin to authorize him and after admin authorized him he can login by using authorized user name and password.
IV. When Login successfully done, he will do some operations like Register and Login, Upload datasets, View All Uploaded Datasets, View All Attackers.

Bob Module:

I. In this module, there are n numbers of users are present.
II. User should register before doing some operations.
III. After registration successful he has to wait for admin to authorize him and after admin authorized him. And he can login by using authorized user name and password.
IV. Login successful he will do some operations like Register and Login, Search and Decrypt Patient Details.

Cloud Server Module:

I. In this module, the Admin has to login by using valid user name and password.
II. After login successful he can do some operations such as Login, View and Authorize User, View and Authorize Owner, View All Datasets, View All Datasets Block chain, View All Attackers, View Disease Results, View Attacker Results.

4.2 Architecture:

A secure e-healthcare framework involves several key elements:

1. User Authentication and Authorization: Secure login procedures and role-based access determine permissions for users like doctors and patients.
2. Data Encryption: Protects information during transmission and storage, preventing breaches of sensitive health data.
3. Role-Based Access Control: Restricts users to accessing only information relevant to their roles.
4. Secure Communication Protocols: HTTPS safeguards data transmission within the system.

5. Audit Logs: Detailed logs of user activities and data access help monitor and investigate suspicious actions.
6. Tokenization: Substitutes sensitive data with non-sensitive tokens for added security.
7. Consent Management: Allows patients to manage consent for data sharing, ensuring compliance with privacy regulations.
8. Data Segmentation: Limits shared information to necessary details, reducing risk.
9. Regular Security Audits: Identify and address vulnerabilities to maintain system confidentiality and integrity.
10. These measures collectively ensure secure and authorized data sharing while enabling efficient and controlled search capabilities in e-healthcare.

Conclusion & Future Scope:

In conclusion, our proposed e-healthcare system addresses current challenges in healthcare information management through a robust, secure framework leveraging cloud computing for scalability and accessibility. Essential functionalities like search, indexing, and backups enhance data processing efficiency, while encryption, authentication, and authorization safeguard sensitive data. The cloud infrastructure and secure centralized database ensure reliable access to patient records, fostering user trust and supporting collaborative decision-making.

The future outlook for secure data sharing and authorized searchable frameworks in e-healthcare is promising. Enhanced data security through blockchain, interoperability standards, AI and Machine Learning for advanced analytics, IoT integration for continuous monitoring, and telemedicine for remote care all drive innovation. Patient-centric solutions empower individuals, regulatory compliance ensures legal data handling, and collaborative research accelerates medical advancements. Ethical considerations and user-friendly designs further enhance adoption, promising significant improvements in healthcare delivery and patient outcomes.

REFERENCES :

1. 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.
2. H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authen-tication as an intelligent process," IEEE Trans. Commun., vol. 67, no. 3,pp. 2260_2273, Mar. 2019.
3. J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserv- ing high order bi-Lanczos in cloud-fog computing for industrial appli-cations," IEEE Trans. Ind. Informat., early access, May 28, 2020, doi:10.1109/TII.2020.2998086.
4. L. Fang, J. Wang, C. Ge, and Y. Ren, ``Fuzzy conditional proxy re-encryption," Sci. China Inf. Sci., vol. 56, no. 5, pp. 1_13, May 2013.
5. 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 fog comput-ing and cloud computing," IEEE Trans. Ind. Informat., vol. 14, no. 10, pp. 4519_4528, Oct. 2018.
6. D. He, M. Ma, S. Zeadally, N.Kumar, and K. Liang, ``Certi_cateless public key authenticated encryption with keyword search for industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3618_3627, Aug. 2018