International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 4, pp 302-306, April-2025

https://doi.org/10.47001/IRJIET/2025.904042

MediSheild: Revolutionizing Health Data Privacy and Smart Record Retrieval

[1]Om Suryawanshi, [2]Adnan Tamboli, [3]Ganesh Kute, [4]Prof. Diksha Yedke, [5]Prof. Prachi Patil

[1,2,3]Student, Department of Information Technology, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India

[4,5]Asst. Professor, Department of Information Technology, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India

Abstract **- In medical management, more and more information technologies are applied to improve work efficiency. For example, the hospital information management system is used to carry out a patient's basic information and medical management, the wrist one-dimensional QR Code is employed to quickly read or input a patient's identity (ID) and so on. Information technology brings convenience while at the same time there are certain secure drawbacks in several typical scenarios because of immature technology or management vulnerability, such as, the reports transparency leaks user privacy, access to view the medical privacy record is not strictly controlled, infusion confirmation is without technical authentication, patient wrist ID is easy to be forged, payment is not convenient and so on. The security issues are further analyzed as follows. Healthcare applications are considered as promising fields for wireless sensor networks, where patients can be monitored using wireless medical networks (WMNs). Current WMN healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing, as a few examples. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. The main contribution of this paper is to distribute patient's data securely in data servers and performing the cryptosystems to perform statistical analysis on the patient data without compromising the patient's privacy.**

Keywords: QR Code, Healthcare, Wireless Medical Network, Data Security.

I. INTRODUCTION

Rapid technological convergence of Internet of Things (IoT), wireless body-area networks (WBANs) and cloud computing has caused e-healthcare (electronic-healthcare) to emerge as a promising information-intensive industrial application domain that has significant potential to improve the quality of medical care. Therefore, how to achieve medical data collection, transmission, processing and presentation has become a critical issue in e-healthcare applications, in which a variety of wireless sensor nodes and terminal devices play important roles in network data aggregation and communications. Furthermore, the evolution of m-health (mobile-health) technology has made it possible for people to gather information concerning their health status easily, anytime and anywhere using smart mobile devices.

However, these medical data consist of personal private information that should not be susceptible to eavesdropping or malicious tampering during transmission. Therefore, the privacy protection and secure transmission of e-/m-healthcare (electronic-/mobile-healthcare) data has drawn more attention from many researchers. A secure and reliable e-/m-healthcare framework to defend against hostile attacks and threats is highlighted for available applications of the informational healthcare industry. Moreover, a challenge remains concerning how to effectively process the ever-growing volume of healthcare data and protect data privacy but maintain low sensor network overhead. Due to the resource-strained characteristics (such as limited power) of mobile devices and sensors, the tradeoff between efficiency and privacy or security must be further balanced for the commercial promotion of e-/m-healthcare. Therefore, a meaningful concern of this paper is the design of a feasible, efficient and privacy-guaranteed e-/m-healthcare information system employing wireless sensor networks.

Most current e-/m-healthcare systems require doctors (or system administrators) to participate in medical information processing, which brings two problems: low effectiveness caused by manual operations and privacy breaches due to doctors' acquaintance with users' private data. A medical expert system that can automatically analyze users' scrambled private data but minimize doctors' participation can address these two problems, particularly for the application of general physical examinations. Even with perfect access control mechanisms, frequent human intervention will always cause a higher risk of privacy disclosure in e-/m-healthcare. As a

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 4, pp 302-306, April-2025

https://doi.org/10.47001/IRJIET/2025.904042

major component of e-/m-healthcare systems, the development of a medical expert system is another focus of this paper.

II. LITERATURE REVIEW

1. **Smart Card-Based Healthcare Information Security System**
   Authors: B. Kim, S. Choi
   Published in:IEEE Transactions on Industrial Informatics, 2020
   Summary:
   This paper presents a smart card-based system for securing medical information at hospitals. It highlights how smart cards can store digital certificates and encrypted health records.
   Relevance to Project:
   Inspired the authentication module using smart card technology for secure login and identity verification.

2. **Secure Mobile Healthcare System Using QR Code and Public Key Infrastructure**
   Authors: M. Zhang, H. Wang
   Published in: Journal of Medical Systems, 2021
   Summary:
   Introduces a method of encrypting sensitive health data using QR codes embedded with public key cryptographic signatures to ensure privacy during mobile data sharing.
   Relevance to Project:
   Helped design our encrypted QR code generation and verification flow.

3. **A Survey on Privacy and Security in Wireless Healthcare Applications**
   Authors: Y. Lin, P. Lin
   Published in: ACM Computing Surveys, 2019
   Summary:
   A comprehensive review of vulnerabilities in wireless healthcare networks and suggestions for privacy-preserving techniques.
   Relevance to Project:
   Highlighted the need for encryption and secure transmission methods in wireless healthcare, validating the problem we aim to solve.

4. **Privacy-Preserving Data Transmission in Wireless Body Area Networks**
   Authors: R. Rahmani, M. Granados
   Published in: IEEE Sensors Journal, 2018
   Summary:
   Focuses on encryption and anonymization techniques in wireless networks used in patient monitoring devices.
   Relevance to Project:
   Guided the secure transmission mechanism over wireless links used in the project.

5. **Enhancing Medical Data Security Using Hybrid Cryptography Techniques**
   Authors: A. Shaikh, N. Sutar
   Published in: International Journal of Computer Applications (IJCA), 2020
   Summary:
   Proposes a hybrid approach using symmetric (AES) and asymmetric (RSA) cryptography for securing EHR systems.
   Relevance to Project:
   Inspired the dual encryption logic used before encoding data into QR codes.

III. SYSTEM DESIGN

The system is simplified and represented in the figure. This schematic representation of the architecture shows the processes, services and related activities that happen in the entire system. This is a consolidated representation of what happens at what point of time in which device in the system. The project Privacy Protection for Wireless Medical Data for Applying QR Code to Secure Medical Management introduces a novel and innovative system that aims to address the shortcomings of the existing healthcare data management systems. The proposed system is designed to enhance the security, privacy, and overall efficiency of managing medical data in a wireless environment.

In the proposed research work to design and implement a system which work with healthcare services. This research work aims to propose a unified trust computing scheme for giving most relevant, efficient and trustworthy healthcare service provider to the requesting patent. Trustworthiness of the healthcare service/provider will be evaluated based on various attributes like QR Code, unique patient id to secure patients record in healthcare environment.

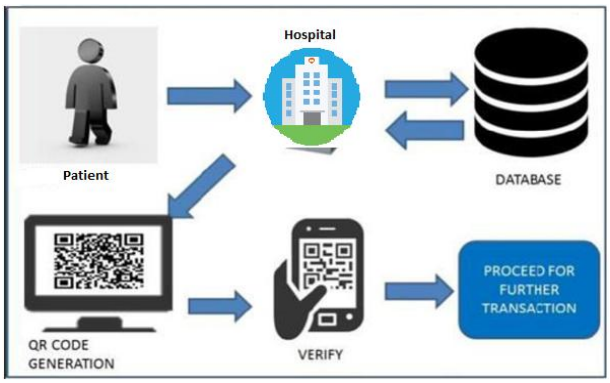

Figure 1: System Architecture Diagram

IV. MATHEMATICAL MODELLING

Mathematical Model
Let S be the Whole system which consists:
S= {IP, Pro, OP}.
Where,

A. IP is the input of the system.
B. Pro is the procedure applied to the system to process the given input.
C. OP is the output of the system.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 4, pp 302-306, April-2025

https://doi.org/10.47001/IRJIET/2025.904042

A. Input:
IP = {P, DR, QR}.
Where,

1. P is Patient.
2. DR is Doctor.
3. OR is used for patient record monitoring.

B. Process
PRO= {RE, NT, INFO, REC}
RE- During Registration Patient and doctor Stored Dataset.
RE={RE1, RE2, RE3,…REn}
QR– This QR code store the database of patient.
QR={QR1,QR2,QR3,….QRn}
INFO is the patient information.

NT- Notification sends by user

C. Output:
OP={NT,QR}

V. ALGORITHM DETAILS

A. AES ALGORITHM

A symmetric block cipher algorithm with a block/chunk size of 128 bits is the AES Encryption algorithm, also referred to as the Rijndael algorithm. These distinct blocks are converted using keys that are 128, 192, and 256 bits long. It then connects these blocks to create the ciphertext after encrypting each one separately. Example: It uses 256-bit encryption, which is regarded as being more sophisticated and secure. The one-to-one message is safely sent and received using 256-bit AES encryption on Facebook and WhatsApp.

Steps:

1. byte substitution: In order to replace the 16 input bytes, a fixed table (S-box) provided in the design is looked up. A matrix with four rows and four columns rep-resents the outcome.
2. shift rows: There are two ways to execute the shift row [4]. The fourth row is rotated three times if the parity is 1, and the second row is rotated by one [5]. These condrow rotates by one and the third row by two if the parity is 0. Similar to how it happens during encryption, the rows of the state matrix are cycled through during decryption.
3. mix columns: With the use of a static matrix, the MixColumns() function multiplies a specified ”state” matrix. The AES encryption mechanism makes use of the MixColumns() function. Using a static matrix and a provided “state,” the Mix-Columns() function multiplies the columns of the static matrix.
4. add round key: Using the AES key schedule, Key Expansion round keys are obtained from the cypher key. For each round plus one, AES needs a distinct 128-bitround key block. Round one major addition: Add RoundKey - each byte of the state is combined with a byte of the round key using bit wisexor.

B. MD5 ALGORITHM

A string of any length can be hashed using the cryptographic hash method MD5 (MessageDigestMethod5), which produces a128-bit digest. The digests are shown as 32-bit hexadecimal values. This technique was created in 1991 by Ronald Rivest to enable the verification of digital signatures.

As a checksum, MD5 can be used to ensure data integrity and protect it from accidental corruption. It has been discovered that this historically popular cryptographic has h function has numerous serious flaws.

A high-end consumer graphics card can decrypt complex8-character passwords encrypted by MD5 in 5 hours using brute force assaults. The findings were nearly instantaneous for straight forward passwords made up only of lowercase letters or numbers.

VI. RESULTS

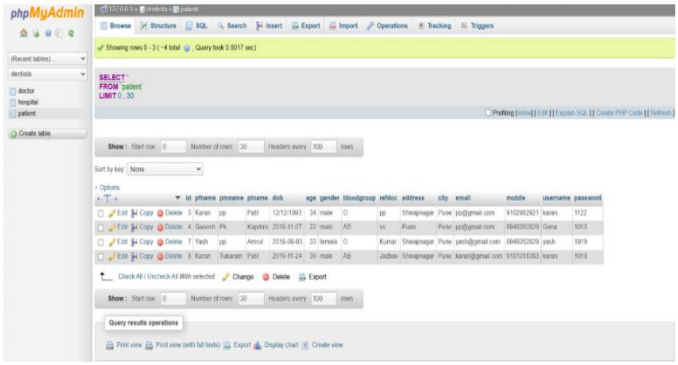

Figure 2: Database

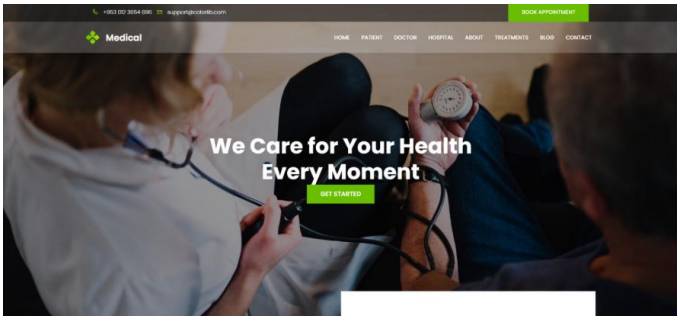

Figure 3: Home Page

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 4, pp 302-306, April-2025

https://doi.org/10.47001/IRJIET/2025.904042

Figure 4: Doctor Login Page

Figure 5: Patient Login Page

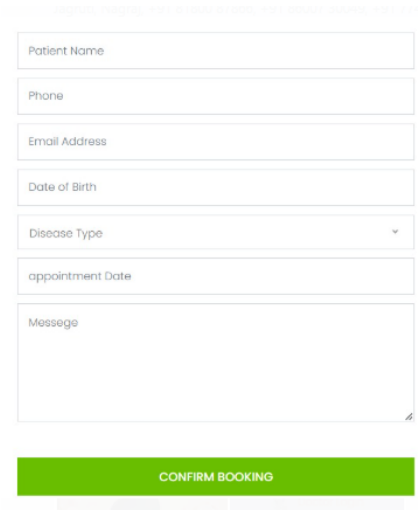

Figure 6: Appointment Booking Page

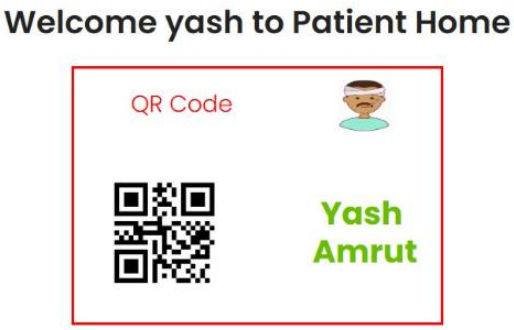

Figure 7: QR code

VII. CONCLUSION

The project successfully demonstrates a secure and efficient system for managing and accessing sensitive medical data using **Smart Card-based authentication** and **QR Code encryption**. By integrating technologies like **Java, JSP, HTML/CSS**, and **MySQL**, the system ensures secure wireless transmission, fast authentication, and privacy preservation in healthcare environments.

This solution addresses key concerns such as data breaches, unauthorized access, and inefficient medical record retrieval — particularly useful in hospitals, clinics, emergency scenarios, and rural healthcare setups.

The system was rigorously tested and proved to be reliable, user-friendly, and adaptable for real-world deployment.

REFERENCES

[1] A.Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam, "Toward Energy-Efficient and Trustworthy eHealth Monitoring System," China Commun., vol.12, no. 1, pp. 46-65, Jan. 2015.

[2] M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform," The Scientific World J., vol. 2015, Article ID 937914, 13 pages, http://dx.doi.org/10.1155/2015/937914, 2015.

[3] Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu. "A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing," in Proc. of 33rd IEEE INFOCOM, 2014, pp. 2130-2138.

[4] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," in Proc. of 35th IEEE Symp. on Security and Privacy, 2014, pp. 524-539.

[5] C. Bekara and M. Laurent-Maknavicius, "A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," in Proc. of 3rd IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), 2007, pp. 59-59.

[6] P. T. Sivasankar and M. Ramakrishnan, "Active key management scheme to avoid clone attack in wireless sensor network," in Proc. of 4th Int. Conf. on Computing, Communications and Networking Technologies (ICCCNT'13), 2013, pp. 1-4.

[7] A.Marcos, J. Simplicio, H. I. Leonardo, M. B. Bruno, C. M. B. C. Tereza, and M. N¨aslund, "Secour Health: A Delay-Tolerant Security Framework for Mobile Health Data Collection," IEEE J. Biomedical and Health Informatics (IEEE Trans. INF TECHNOL B), vol. 19, no. 2, pp. 761-772, Mar. 2015.

ISSN (online): 2581-3048
Volume 9, Issue 4, pp 302-306, April-2025
https://doi.org/10.47001/IRJIET/2025.904042

[8] R. X. Lu, X. D. Lin, and X. M. (Sherman) Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE Trans. Parall. distr., vol. 24, no. 3, pp. 614-624, Mar. 2013.

[9] A.Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," in Proc. of Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), 2007, pp. 209-214.

[10] A.C.F. Chan, "Symmetric-Key Homomorphic Encryption for Encrypted Data Processing," in Proc. of 2009 IEEE International Conference on Communications (ICC '09), 2009, pp.1-5.

[11] C. C. Zhao, Y. T. Yang, and Z. C. Li, "The Homomorphic Properties of McEliece Public-Key Cryptosystem," in Proc. of 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES'12), 2012, pp.39-42.

[12] J. Reid, I. Cheong, M. Henrickson, and J. Smith, "A novel use of RBAC to protect privacy in distributed health care information systems," in Proc. of 8th Australasian Conf. on Information Security and Privacy, 2014, pp. 403-415.

[13] J. Mirkovic, H. Bryhni, and C. Ruland, "Secure solution for mobile access to patient's health care record," in Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Serv., 2011, pp. 296-303.

AUTHORS BIOGRAPHY

Om Suryawanshi, Student, Department of Information Technology, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India.

Adnan Tamboli, Student, Department of Information Technology, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India.

Ganesh Kute, Student, Department of Information Technology, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India.

Prof. Diksha Yedke, Asst. Professor, Department of Information Technology, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India.

Prof. Prachi Patil, Asst. Professor, Department of Information Technology, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India.

Citation of this Article:

Om Suryawanshi, Adnan Tamboli, Ganesh Kute, Prof. Diksha Yedke, & Prof. Prachi Patil. (2025). MediSheild: Revolutionizing Health Data Privacy and Smart Record Retrieval. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(4), 302-306. Article DOI https://doi.org/10.47001/IRJIET/2025.904042

****

