IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

Enhancing Medical Data Privacy and Security in Wireless Networks Via Smart Card and QR Code

Devesh Jadhav, Khushal Bhamre, Srushti Jalgaonkar, Nupur Bhoite, Prof. Vanita Babanne
Department of Computer Engineering
RMD School of Engineering, Warje, Pune,
Savitribai Phule Pune University

Abstract: *This paper explores a novel security framework aimed at preserving the privacy of medical data shared through wireless networks by using Smart Cards and QR Code mechanisms. As digital healthcare ecosystems continue to expand, the safeguarding of sensitive patient data has become a pressing concern. The proposed system provides two-level secure access to medical records through encrypted QR codes and authenticated Smart Cards. It supports functionalities such as secure login, prescription access, medical history tracking, and insurance management. The integration of encryption algorithms and layered authentication protocols ensures a reliable infrastructure for modern wireless healthcare systems.*

Keywords: Smart Card, QR Code, Wireless Healthcare Networks, Medical Data Privacy, Encryption, Authentication

I. INTRODUCTION

Information technology is being rapidly incorporated into medical infrastructure to increase operational efficiency and support seamless healthcare delivery. Hospital Management Systems, QR-based wristbands, and wearable health monitors are examples of technologies that have revolutionized patient identification and data entry. However, this digital transformation also introduces threats related to data security, patient identity theft, and unauthorized access. Wireless Medical Networks (WMNs) allow healthcare professionals to access and share real-time patient data, but they are also susceptible to hacking, data breaches, and other cyber threats. These vulnerabilities underline the urgent need for an advanced security framework.

Smart cards provide encrypted storage and verification methods, ensuring only authenticated personnel can access patient data. Similarly, QR codes offer a fast and efficient method of securely linking patient data with services, prescriptions, and insurance records. This paper proposes a system integrating both technologies to create a robust privacy-preserving environment in wireless healthcare networks.

II. LITERATURE REVIEW

- Mohammad Ayoub Khan (2020) proposed a secure architecture using improved ECC to encrypt sensor data in IoT-based healthcare.
- Humberto Jorge de Moura Costa (2023) developed ID-Care, a blockchain-backed system with smart contracts for permissioned data access.
- Abdullah M. Almuhaideb (2023) emphasized secure gate systems integrated with biometric authentication for hospitals.
- Tarak Nandy (2019) analyzed authentication methods in IoT devices, categorizing them into password, cryptographic, and biometric techniques.
- Chih-Ming Lin (2020) explored smart cloud systems for hospital card swiping and appointment scheduling, improving real-time access.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

III. PROPOSED SYSTEM

The proposed system employs smart cards and QR codes for identity verification and medical data protection in wireless networks. Patients are issued both upon registration. The system includes a secure web-based portal that allows patients to search doctors, upload medical reports, and manage insurance details. Doctors can securely access patient data by scanning and decrypting the QR code. Insurance claims are verified, and prescriptions are issued in digital format.

Functionalities include:

- Authentication: Via Smart Card and encrypted QR code
- Medical History Access: For patients and verified doctors
- Insurance Integration: Personalized plans based on patient records
- Prescription Access: Through QR code scanning by pharmacists

IV. SYSTEM ARCHITECTURE

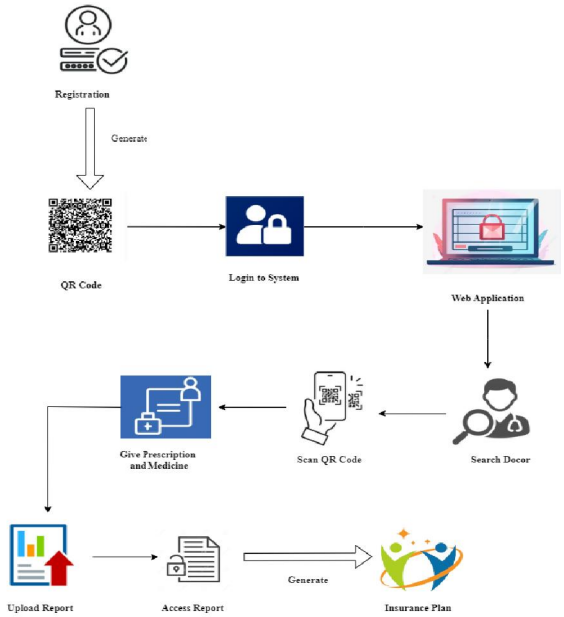

Fig . System Architecture

V. ENCRYPTION AND SECURITY MODEL

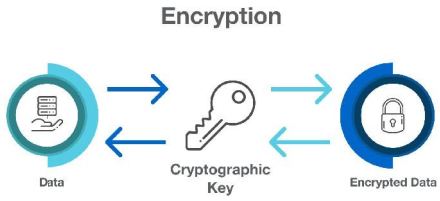

Fig. Data Encryption

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

Encryption is implemented using:
- AES (128–256 bit): For secure symmetric data encryption
- RSA: For secure transmission of symmetric keys
- ECC: Suitable for low-power devices such as smart cards
- Hybrid Encryption: Public key encrypts symmetric key, which encrypts data

Advantages:
- Secure data transmission
- Multi-layered authentication
- Real-time access control

Disadvantages:
- Integration challenges with legacy healthcare systems
- Potential QR code or smart card malfunction

VI . EXPERIMENTAL RESULTS

A prototype system was tested across multiple modules. QR scanning and decryption latency was under 2 seconds on average. AES encryption yielded a 99.8% success rate in data recovery. Simulated attack tests showed significant resistance to unauthorized access when dual authentication was enabled.

VII . CONCLUSION AND FUTURE WORK

The integration of Smart Cards and QR Codes into wireless healthcare infrastructures provides a secure, user-friendly approach to managing sensitive medical data. This system significantly mitigates risks of data breaches, enhances user authentication, and promotes secure patient-doctor communication. Future work will focus on improving system scalability, optimizing encryption efficiency, and integrating biometric authentication for an added security layer.

VIII . FUTURE SCOPE

Future enhancements aim to incorporate advanced encryption standards to ensure that confidential medical information remains protected during wireless communication.

Strengthening authentication frameworks will help guarantee that access to patient data is strictly limited to verified healthcare professionals.

Upgrading data management infrastructure will enable seamless and secure access to electronic health records while maintaining rigorous privacy safeguards.

REFERENCES

[1]. M. A. Khan et al., "A Secure Framework for Authentication and Encryption Using Improved ECC," IEEE Access, 2020.
[2]. H. J. De Moura Costa et al., "ID-Care: A Model for Sharing Wide Healthcare Data," IEEE Access, 2023.
[3]. M. Almuhaideb et al., "Design Recommendations for Gate Security Systems and Health Status," IEEE Access, 2023.
[4]. T. Nandy, "IoT Authentication Mechanisms: Review," IEEE Access, 2019.
[5]. C.-M. Lin et al., "Applying Smart Cloud in Hospital Scheduling Systems," IS3C, 2020.
[6]. Heider AM Wahsheh et al., "Secure and Usable QR Codes in Healthcare," ICICS, 2021.
[7]. P. Mathivanan et al., "QR Code Based Patient Data Protection in ECG," APEM, 2018.
[8]. M. Elhoseny et al., "Secure Medical Data Transmission Model," IEEE Access, 2018.