WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Enhancing medical data privacy and security in wireless networks via smart card and QR code

Devesh Jadhav [1], Khushal Bhamre[2], Srushti Jalgaonkar[3], Nupur Bhoite[4], Mrs.Vanita Babanne[5]

Department of Computer Engineering, RMD School of Engineering Warje, Pune

ABSTRACT:

The integration of information technology into medical administration is becoming increasingly essential for enhancing operational efficiency. Systems such as Hospital Information Management Systems (HIMS) are employed to handle core patient information and medical records, while one- and two-dimensional wristband codes simplify patient identification processes. Despite the convenience offered by digital systems, several security challenges still exist due to underdeveloped technologies or administrative oversights. These include insufficient access control over sensitive medical records, potential breaches of patient privacy due to non-confidential reporting practices, the absence of reliable verification methods for medical procedures like infusions, and vulnerabilities such as identity theft and complicated payment processes. A more detailed explanation of these security issues follows. Wireless Medical Networks (WMNs) are increasingly being adopted in healthcare environments to track patient status, positioning them as a promising application of wireless sensor networks. Current healthcare innovations emphasize reducing energy consumption, enhancing patient mobility, and ensuring uninterrupted patient communication.

Keywords: QR Code Generation, Data Encryption, SMTP and OTP Protocol, Smart Card.

Introduction

1. Information technology is becoming an integral part of medical administration, significantly enhancing operational productivity. Systems like Hospital Information Management Systems (HIMS) are employed to store patient profiles and medical histories efficiently. Additionally, one-dimensional QR codes on patient wristbands facilitate quick access to personal information such as names and IDs [1].
2. As traditional security perimeters around sensitive data become less effective, there is a growing dependence on mobile platforms, cloud solutions, high-speed internet, and wearable technology. This shift requires security measures that begin from the data's origin and persist through its transmission to its endpoint—whether it's a medical app, sensor, database, electronic health record (EHR), or the end user, including patients or researchers [2].
3. Wireless technologies have significantly transformed healthcare services by enabling remote monitoring, virtual consultations, and electronic access to medical records [3]. However, the rise in wireless network usage brings with it critical concerns regarding the privacy and protection of sensitive health data. These include the risks of unauthorized access, data leaks, and violations of patient confidentiality [4].
4. Today's healthcare environment relies on a dynamic and loosely connected digital infrastructure powered by the internet. While this tech-based ecosystem streamlines research and healthcare delivery, it also introduces serious threats to patient data privacy and system integrity [5].
5. To tackle these issues, this research explores the use of smart cards and QR codes as tools to bolster data privacy and security in wireless healthcare systems. Smart cards offer built-in cryptographic features, serving as secure means of identity verification and data protection. Meanwhile, QR codes present an efficient and user-friendly way to share information and manage access control [6].
6. In the healthcare context, smart cards serve as a strong layer of authentication and permission control. These physical cards store encrypted data securely and are used to confirm the identity of healthcare professionals accessing patient records. By mandating smart card usage, healthcare organizations can prevent unauthorized data access and enhance security across wireless communication channels [7].

1.1 Medical Data Privacy and Security: An Overview of Challenges

As healthcare continues to digitize, ensuring the confidentiality and safety of medical data has become a top priority for medical professionals, patients, and regulatory authorities. Wireless networks have revolutionized how medical information is stored, accessed, and shared. However, this convenience also introduces significant privacy risks.

Medical records often include highly confidential information—such as a patient's medical history, treatment details, diagnostic data, and personal identifiers—which makes them attractive targets for cyberattacks. Patients expect their private health data to be protected. A breach of this trust can lead to decreased patient engagement, reluctance to disclose critical information, and hesitance in seeking timely care.

Related Work

In 2020, Mohammad Ayoub Khan and colleagues [1] highlighted the transformative role of IoT-based medical sensors in improving patient monitoring and data management within healthcare. However, they also pointed out serious concerns about safeguarding sensitive data during wireless transmission. To address these issues, they proposed a secure framework using enhanced Elliptic Curve Cryptography (ECC) for encrypting and authenticating sensor-generated health data.

In 2023, HUMBERTO JORGE DE MOURA COSTA et al. [2] introduced ID-Care, a decentralized system leveraging blockchain to create a transparent and tamper-proof healthcare data exchange platform. This system fosters trust by ensuring all transactions are traceable and verifiable. Through advanced access controls and smart contracts, data sharing is secured, automated, and managed efficiently.

Also in 2023, Abdullah M. Almuhaideb et al. [3] examined the integration of health monitoring technologies with secure gate control systems in healthcare institutions. Their study reviewed the latest developments in RFID, biometrics, and surveillance to manage physical access and enhance safety for both patients and staff.

In 2019, Tarak Nandy [4] conducted a comprehensive review of authentication mechanisms in IoT environments. The study addressed the vulnerabilities in current authentication processes, categorizing them into password-based, cryptographic, and biometric methods, and discussed their advantages and limitations.

Chih-Ming Lin and team [5], in 2020, investigated the application of smart cloud technology in hospital management. Their system focused on improving appointment scheduling and card-swipe-based access to patient data, allowing seamless synchronization of real-time information among patients, doctors, and administrative units.

Proposed System

This system aims to strengthen the confidentiality and security of patient data by integrating smart cards and QR codes. At the time of registration, patients are issued a smart card and a distinct QR code. These credentials enable secure access to an online application through which users can search for doctors, manage medical histories, upload documents, and view insurance options.

Doctors utilize QR codes on prescriptions, allowing pharmacists or patients to access the details securely. Additionally, uploaded medical documents can be viewed only by authorized personnel. The system can also generate custom insurance recommendations based on a patient's health records. Overall, the solution enables safe data exchange and access control, while ensuring the protection of sensitive health information

System Architecture

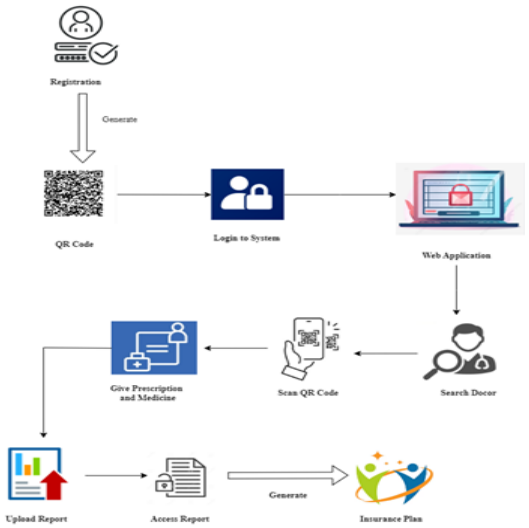


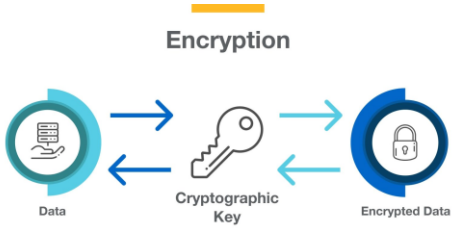
Fig : System Architecture

1. Registration: Users create an account within the system.
2. QR Code Generation: A unique QR code is assigned to each new user for identification.
3. Login: Users log in with their credentials.
4. Search Doctor: Enables patients to search for doctors as per their medical needs.
5. QR Code Scan & Decryption: Doctors scan and decrypt the patient's QR code to access medical information.

6. Insurance Verification: Doctors consult with the insurance department for eligibility checks.
7. Prescription: Doctors issue prescriptions and medicines.
8. Insurance Generation: Patients can create personalized insurance plans.
9. Access Reports: Users can view their previous medical records and documents.
10. Upload Reports: Patients can upload relevant medical data.
11. Logout: Ends the session securely.

Algorithm

To protect patient information, data encryption converts plain text into unreadable ciphertext using cryptographic keys. Only those with the corresponding decryption keys can retrieve the original content.



Common Encryption Algorithms:

- AES (Advanced Encryption Standard): Trusted for its strong encryption and varying key sizes (128/192/256 bits).
- DES (Data Encryption Standard): An older but still occasionally used algorithm with lower security.
- 3DES (Triple DES): Applies DES three times for improved protection.
- RSA: Uses public-key cryptography and is known for secure communications and digital signatures.
- ECC (Elliptic Curve Cryptography): Provides similar security to RSA but with smaller keys, ideal for mobile and embedded devices.

Hybrid Encryption:

- Combines symmetric (fast) and asymmetric (secure) encryption.
- A symmetric key is encrypted using a public key, then used to encrypt the actual data.

Advantages:

- Smart cards and QR codes add a robust security layer to protect patient records.
- These tools support encrypted wireless transmission of sensitive information.
- They ensure only verified users can access critical data, preserving privacy.

Disadvantages:

- Technical issues may affect QR or smart card functionality, impacting data access.
- Poor implementation may leave systems vulnerable to breaches.
- Compatibility challenges may arise during integration with existing infrastructure.

Conclusion

Smart cards and QR codes offer promising solutions for securing medical data in wireless healthcare networks. These technologies enhance authentication, ensure secure data exchanges, and restrict access to authorized users only. Despite some challenges like potential security gaps or technical failures, the advantages—including efficient data handling and enhanced privacy—make them viable for modern healthcare systems. Incorporating encryption standards, strong user verification, and ongoing security monitoring will further improve their reliability. Ultimately, this integration serves as a proactive measure to protect sensitive patient information in an increasingly connected healthcare environment.

Future Scope

- Adoption of robust encryption standards to ensure data confidentiality during wireless transmission.
- Deployment of strong authentication protocols to restrict data access to verified personnel only.
- Improvement of data handling systems to balance accessibility with strict privacy controls.

REFERENCES:

[1] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in *IEEE Access*, vol. 8, pp. 52018-52027, 2020, doi: 10.1109/ACCESS.2020.2980739.

[2] H. J. De Moura Costa, C. A. Da Costa, R. S. Antunes, R. Da Rosa Righi, P. A. Crocker and V. R. Q. Leithardt, "ID-Care: A Model for Sharing Wide Healthcare Data," in *IEEE Access*, vol. 11, pp. 33455-33469, 2023, doi: 10.1109/ACCESS.2023.3249109

[3] A. M. Almuhaideb *et al*., "Design Recommendations for Gate Security Systems and Health Status: A Systematic Review," in *IEEE Access*, vol. 11, pp. 131508-131520, 2023, doi: 10.1109/ACCESS.2023.3335115.

[4] s Authentication Mechanism," in *IEEE Access*, vol. 7, pp. 151054-151089, 2019, doi: 10.1109/ACCESS.2019.2947723.

[5] C. Suresh, C. Chandrakiran, K. Prashanth, K. V. Sagar and K. Priyanka, ""“Mobile Medical Card” – An Android Application For Medical Data Maintenance," *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2020, pp. 143-149, doi: 10.1109/ICIRCA48905.2020.9183307.

[6] C. -M. Lin, T. -K. Wang, Y. H. Lin, J. R. Wu and C. H. Chao, "Applying smart cloud in the hospital card swiping and scheduling system," *2020 International Symposium on Computer, Consumer and Control (IS3C)*, Taichung City, Taiwan, 2020, pp. 255-258, doi: 10.1109/IS3C50286.2020.00073.

[7] Wahsheh, Heider AM, and Mohammed S. Al-Zahrani. "Secure and usable QR codes for healthcare systems: the case of covid-19 pandemic." In *2021 12th international conference on information and communication systems (ICICS)*, pp. 324-329. IEEE, 2021.

[8] Mathivanan, Ponnambalam, Sam Edward Jero, Palaniappan Ramu, and Athi Balaji Ganesh. "QR code based patient data protection in ECG steganography." *Australasian physical & engineering sciences in medicine* 41 (2018): 1057-1068.

[9] Daoui, Achraf, Mohamed Yamni, Hicham Karmouni, Mhamed Sayyouri, Hassan Qjidaa, Saad Motahhir, Ouazzani Jamil et al. "Efficient Biomedical Signal Security Algorithm for Smart Internet of Medical Things (IoMTs) Applications." *Electronics* 11, no. 23 (2022): 3867.

[10] Elhoseny, Mohamed, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, N. Arunkumar, and Ahmed Farouk. "Secure medical data transmission model for IoT-based healthcare systems." *Ieee Access* 6 (2018): 20596-20608.