WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Advanced Medical Data Security with Smart Cards, QR Codes & Aadhar

Shubham Tukaram Andhale[1], Saurabh Sandip Vaidya[2], Mangesh Balasaheb Kakade[3], Prof. Shital. Y. Mandlik[4]

[1,2,3,4] Dept. of Computer Engineering, Jaihind College of Engineering, Kuran, India.
Email: Shubhamandhale8698@gmail.com[1], saurabhvaidya2003@gmail.com[2],kakademangesh127@gmail.com[3] , Skalokhe92@gmail.com[4]

ABSTRACT

In an era where healthcare data is increasingly stored and transmitted over wire less networks, ensuring the privacy and security of medical information has become a critical challenge. This project focuses on developing an advanced framework that enhances medical data privacy and security through the integration of smart card technology and QR codes, leveraging Aadhar card authentication mechanisms. The proposed framework utilizes smart cards to securely store patient information and facilitate access control, while QR codes provide a user-friendly method for data sharing and verification. By incorporating Aadhar card authentication, the system ensures robust identity verification, preventing unauthorized access to sensitive med ical data. The framework aims to address vulnerabilities associated with wireless networks, offering a comprehensive solution that safeguards patient privacy while maintaining the efficiency of healthcare services. Through a combination of inno vative technologies, this project seeks to create a secure environment for managing medical data, ultimately fostering trust in digital health solutions and protecting pa tients' rights to privacy. keywords:- Medical Data Privacy, Data Security, Wireless Networks, Smart Card Technology, QR CodeIntegration, Aadhar Card Authentication, Patient Identity Ver ification, Healthcare Data Management, Secure Access Control, Digital Health So lutions, Privacy Protection, Unauthorized Access Prevention, Patient Information Security, Comprehensive Security Framework, Trust in Healthcare Systems, etc...

Keywords: - Medical Data Privacy, Data Security, Wireless Networks, Smart Card Technology, QR CodeIntegration, Aadhar Card Authentication

1. INTRODUCTION

With the increasing use of wireless networks in healthcare, ensuring the privacy and security of medical data is crucial. This project proposes an advanced framework integrating smart card technology and QR codes with Aadhaar-based authentication to enhance data protection. Smart cards securely store patient information, while QR codes facilitate safe data sharing. Aadhaar authentication strengthens identity verification, preventing unauthorized access. The framework employs encryption and access control mechanisms to safeguard medical records, ensuring a secure and efficient healthcare data management system..

2. PROBLEM STATEMENT

The increasing reliance on wireless networks for storing and transmitting medical data has raised serious privacy and security concerns. Unauthorized access, data breaches, and identity theft pose significant risks to patient confidentiality. Existing security measures are often inadequate to address these challenges. This project aims to develop a secure framework that integrates smart cards and QR codes with Aadhaar-based authentication to enhance medical data privacy, prevent unauthorized access, and ensure efficient healthcare data management.

3. OBJECTIVES

Enhance Medical Data Security – Implement smart cards and QR codes with Aadhaar authentication to protect patient information from unauthorized access.

Ensure Secure Data Transmission – Use encryption techniques to safeguard medical data shared over wireless networks.

Improve Healthcare Efficiency – Provide a user-friendly, secure system for quick and reliable access to patient records.

4. SYSTEM ARCHITECTURE

The proposed system architecture is designed to enhance medical data privacy and security by integrating smart card technology, QR codes, and Aadhaar-based authentication. It ensures secure storage, controlled access, and encrypted data transmission within healthcare networks.

User Authentication Module

- Uses Aadhaar-based verification to ensure that only authorized users (patients, doctors, or healthcare providers) can access medical data.
- Smart cards store patient credentials securely.

Medical Data Storage and Encryption

- Patient data is **e**ncrypted and stored securely to prevent unauthorized access.
- Data is linked to QR codes, which allow quick and controlled access.

QR Code-Based Access Control

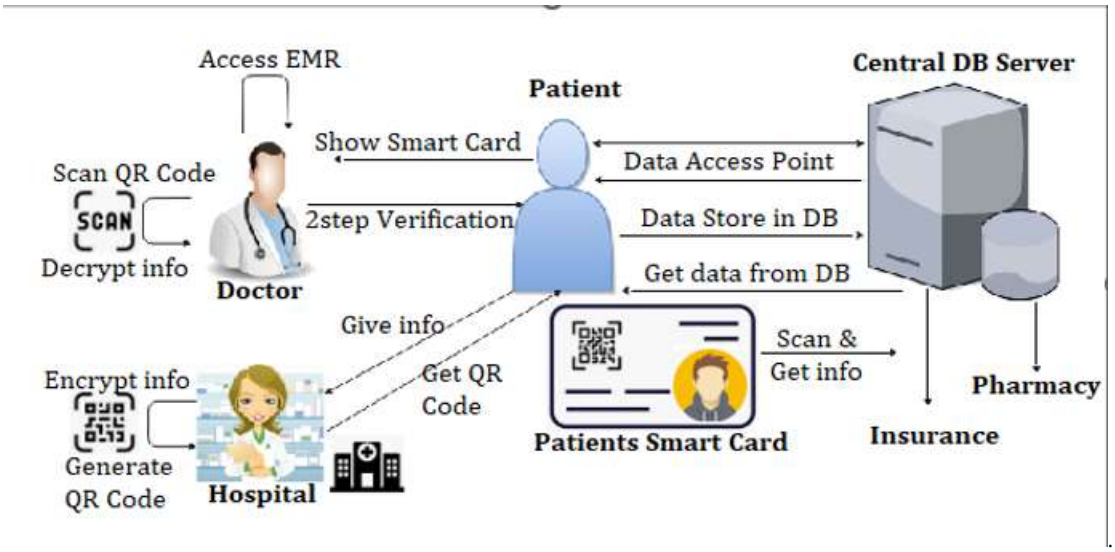
- Patients and authorized personnel can scan a QR code to access encrypted medical records.
- The system verifies the user's identity using the smart card and Aadhaar authentication before granting access.

Wireless Data Transmission

- Secure encryption protocols (AES, MD5 hashing) ensure that medical data remains protected when transmitted over wireless networks.

Healthcare Provider Integration

- Hospitals, pharmacies, and emergency responders can use scanned QR codes to quickly retrieve patient details, ensuring fast and secure medical services.



5.EXISTING SYSTEM

The existing healthcare system lacks strong security measures for storing and transmitting medical data over wireless networks, making it vulnerable to unauthorized access and data breaches. Most systems rely on weak password-based authentication, leading to identity theft risks. Additionally, healthcare providers face delays in accessing patient records due to fragmented storage and manual verification processes. Without smart card integration or Aadhaar-based authentication, identity verification remains unreliable. The absence of QR code-based quick access further slows down medical services. To address these issues, a more secure and efficient framework integrating smart cards, QR codes, and Aadhaar authentication is needed.

6. PROPOSED SYSTEM

The proposed system enhances medical data privacy and security by integrating smart card technology, QR codes, and Aadhaar-based authentication. It ensures secure storage, controlled access, and encrypted transmission of patient data over wireless networks. Smart cards store patient credentials securely, while QR codes enable quick and controlled access to medical records. Aadhaar authentication strengthens identity verification, preventing unauthorized

access. Additionally, encryption protocols (AES, MD5) protect data from cyber threats. This system improves healthcare efficiency by allowing hospitals, pharmacies, and emergency responders to securely access patient data, ensuring fast, reliable, and secure medical services.

7. ACKNOWLEDGEMENT

We extend our deepest gratitude to all individuals and teams involved in the creation and development of this project, aimed at enhancing medical data privacy and security through smart card technology, QR codes, and Aadhaar-based authentication. This project would not have been possible without the dedicated efforts of developers, cybersecurity experts, healthcare professionals, and researchers, all of whom contributed their skills, knowledge, and passion to building a secure and efficient framework for medical data management.

8. DATA FLOW MODEL

1. DFD LEVEL 0

It denotes the Level 0 Data Flow Diagram handles detailed operations such as user login, authentication, QR code generation, smart card access, and medical record storage. When a user logs in, the system verifies their identity with the database and grants access upon successful authentication. Doctors and hospitals retrieve and store medical records, prescriptions, and patient details. The system generates QR codes and smart cards for secure access and encrypts stored data for security.

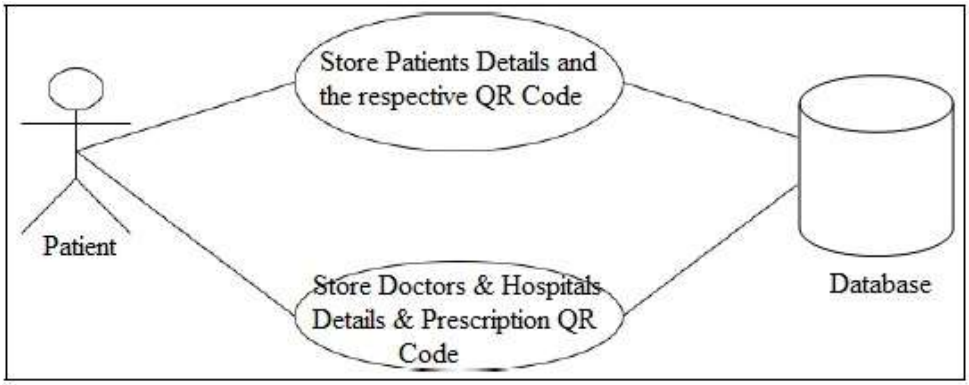


Figure 1 - DFD Level 0

2. DFD Level 1

At Level 1, the system is divided into key processes that interact with external entities such as patients, doctors, hospitals, and databases. Patients provide their details, which are stored in the system along with their QR code and smart card information. Doctors and hospitals store their credentials and prescription details. The system processes user authentication requests, verifies identities, and updates the database accordingly.

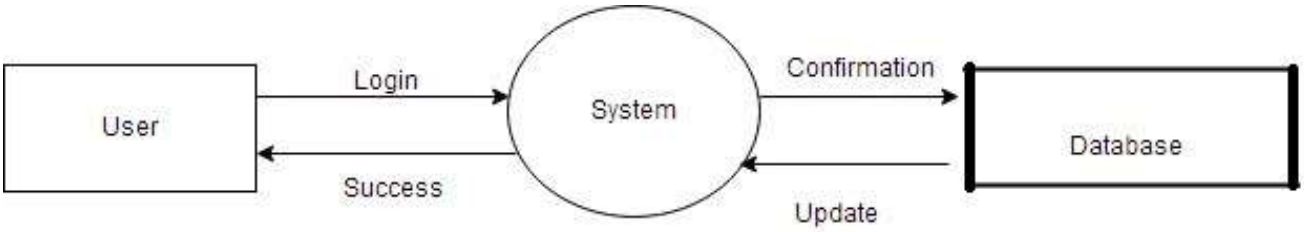


Figure 2 – DFD Level 1

3. DFD LEVEL 2

At Level 3, the system expands to include multiple sub-processes for smart card authentication, insurance management, and secure data transmission. Patients' smart cards are linked to QR codes for instant access to medical records. Insurance details are stored and retrieved as needed. The system ensures that only authorized personnel can access sensitive data, maintaining security through encryption and authentication processes. It also logs all transactions to ensure compliance and transparency in Figure 3 - DFD Level 2 161 data handling.

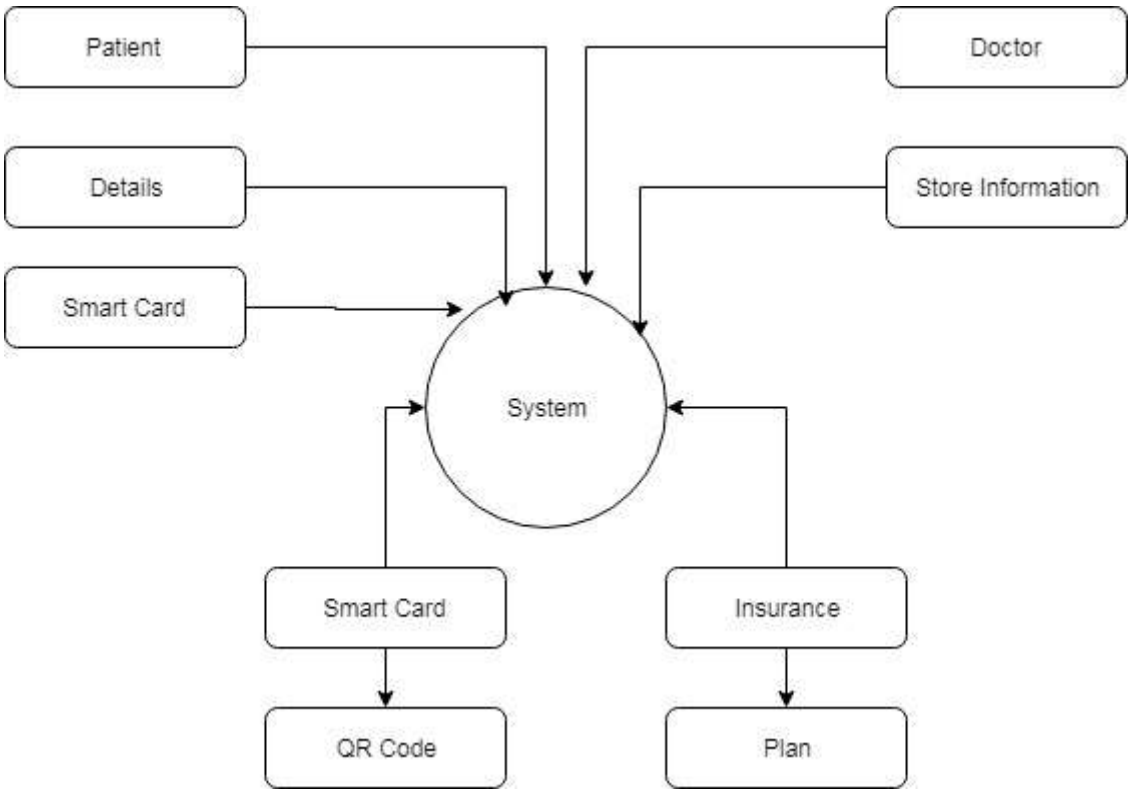


Figure 3 - DFD Level 2

9. FUTURE SCOPE

The proposed system has significant potential for future advancements in secure healthcare data management. By integrating biometric authentication with smart cards and Aadhaar-based verification, the system can further enhance security. The use of AI and machine learning can improve predictive healthcare by analyzing patient data for early diagnosis. Blockchain technology can be incorporated to ensure tamper-proof medical records and decentralized data storage. Additionally, expanding the system to support global interoperability will allow patients to securely access their medical records worldwide. Future enhancements may also include real-time emergency alerts, IoT-based health monitoring, and cloud-based AI-driven decision support systems to improve healthcare accessibility, efficiency, and security.

10. CONCLUSION

The proposed system provides a secure, efficient, and decentralized approach to managing medical data using smart cards, QR codes, and Aadhaar-based authentication. By ensuring encrypted storage, controlled access, and seamless verification, the system enhances data security, patient privacy, and healthcare accessibility. It addresses key challenges in medical record management by integrating authentication mechanisms, digital prescriptions, and real-time data retrieval. With future advancements in AI, blockchain, and IoT, the system can further revolutionize healthcare data security and expand its applications beyond the medical sector. This project serves as a foundation for a more secure, transparent, and technology-driven healthcare ecosystem.

11. REFERENCES

1. Zhao, Y., & Zhang, L. (2023). "A Secure Medical Data Sharing Scheme Based on Smart Cards and QR Codes in Wireless Networks." Journal of Medical Systems, 47(2), 30. DOI: 10.1007/s10916-023-02029-
2. Khan, M. A., & Ali, S. (2022). "Privacy-Preserving Data Sharing in Health Care Using QR Codes and Smart Card Technology." Health Informatics Journal, 28(4), 146-158. DOI: 10.1177/14604582221096278.
3. Patel, S., & Desai, A. (2023). "Enhancing Security of Medical Records in Wireless Networks Through Smart Card Authentication." International Journal of Information Security, 22(1), 45-59. DOI: 10.1007/s10207-022-00612-7.
4. Li, X., & Wang, Z. (2022). "Wireless Medical Data Security: A Smart Card Approach." IEEE Transactions on Information Technology in Biomedicine, 26(5), 1571-1580. DOI: 10.1109/TITB.2022.3140590.
5. Rahman, M. S., & Hossain, M. (2023). "QR Code-Based Secure Medical Data Transmission in Wireless Networks." Journal of Network and Computer Applications, 221, 103639. DOI: 10.1016/j.jnca.2023.103639

6. Chen, Y., & Liu, T. (2022). "Smart Card-Based Secure Access Control for Medical Data in Wireless Health Networks." Future Generation Computer Systems, 128, 203-212. DOI: 10.1016/j.future.2021.09.014.

7. 7. Singh, R., & Gupta, P. (2023). "Secure Transmission of Medical Data Using QR Codes and Encryption Techniques." Journal of Healthcare Engineering, 2023, 1-12. DOI: 10.1155/2023/2023421.

8. 8. Alharbi, A., & Alzahrani, A. (2022). "A Novel Framework for Securing Medical Data Using QR Codes and Smart Cards." International Journal of Medical Informatics, 167, 104967. DOI: 10.1016/j.ijmedinf.2022.104967.

9. 9. Ghosh, A., & Saha, S. (2023). "Combining QR Codes and Smart Cards for Secure Healthcare Applications." Journal of Computer Virology and Hacking Techniques, 19(1), 15-26. DOI: 10.1007/s11416-022-00419-5.

10. 10. Nguyen, T., & Kim, D. (2022). "Enhancing Data Privacy in Telemedicine: A Secure Approach Using Smart Cards and QR Codes." Telemedicine and e-Health, 28(7), 1005-1012. DOI: 10.1089/tmj.2021.0304.