International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

QR Based Online Payment System For Enhanced Convivence Using ML

Prof. Rahul D. Ingle [1] , Prof. Rohan B. Kokate [2] , Jyoti Ramesh Lanjewar [3]

[1] Assistant Professor Department of MCA
JD College of Engineering and Management, Nagpur, India
[2] Head of Department Department of MCA
JD College of Engineering and Management, Nagpur, India
[3] MCA Student Department of MCA
JD College of Engineering and Management, Nagpur, India

Abstract- The rapid advancement of digital technology has significantly transformed financial transactions, leading to the widespread adoption of cashless payment systems. Among these, QR code-based payment systems have emerged as one of the most convenient and efficient methods for conducting fast and contactless transactions. However, despite their growing popularity, these systems still face critical challenges such as transaction fraud, unauthorized access, phishing attacks, and security vulnerabilities. To overcome these limitations, there is a need to integrate intelligent technologies that can enhance both security and user experience. This project presents the design and development of a QR Based Online Payment System for Enhanced Convenience Using Machine Learning (ML). The primary objective of the system is to provide a secure, fast, and user-friendly digital payment platform that allows users to make payments simply by scanning QR codes. The system eliminates the need for physical cash, card swiping, or manual bank details entry, thereby reducing transaction complexity and improving efficiency. A key feature of the proposed system is the integration of Machine Learning-based fraud detection mechanisms. The ML model continuously analyzes transaction patterns, user behavior, device information, and payment history to identify unusual or suspicious activities. By using classification and anomaly detection techniques, the system can detect potential fraud in real time and prevent unauthorized transactions before they are completed. This enhances the overall trust and reliability of the payment platform. The system also includes essential modules such as secure user authentication, dynamic QR code generation, transaction processing, payment history tracking, and notification services. Each transaction is securely encrypted and stored in a centralized database to ensure data integrity and confidentiality. The platform is designed using modern web technologies to ensure scalability, responsiveness, and compatibility across multiple devices. From a functional perspective, the system supports both users and merchants, enabling seamless peer-to-merchant and peer to peer payments. Merchants can generate unique QR codes linked to their accounts, while users can scan and complete payments instantly. The inclusion of real-time alerts and dashboards helps users track their financial activities efficiently.

Index Terms - QR Code Payment System, Digital Wallet, Machine Learning, Fraud Detection, Online Transactions, Secure Payments, FinTech, Real-Time Payment Processing, Behavioural Analysis, Payment Gateway, Smart Transactions, Cybersecurity.

I. INTRODUCTION

In the modern digital era, financial transactions are rapidly shifting from traditional cash-based systems to fast, secure, and contactless digital payment methods. This transformation is driven by the widespread use of smartphones, internet connectivity, and advanced financial technologies (FinTech). Among various digital payment solutions, QR code-based payment systems have gained significant popularity due to their simplicity, speed, and ease of use. These systems allow users to make payments instantly by scanning a QR code, eliminating the need for physical cash, cards, or manual entry of bank details.

Despite their convenience, QR-based payment systems are increasingly exposed to security risks such as fraud transactions, QR code tampering, phishing attacks, and unauthorized access. As digital transactions grow, ensuring security and trust has become a major concern for users, merchants, and financial institutions. Traditional rule-based security systems are often insufficient to detect complex and evolving fraud patterns in real-time environments.

To address these challenges, the integration of Machine Learning (ML) into payment systems provides an effective solution. Machine Learning algorithms can analyse large volumes of transaction data, identify behavioural patterns, and detect anomalies that may indicate fraudulent activity. This enables the system to take proactive actions such as alerting users, blocking suspicious transactions, or requiring additional verification.

The proposed developing a QR Based Online Payment System enhanced with Machine Learning to project focuses on improve both convenience and security in digital transactions. The system enables users to perform seamless payments through QR code scanning while ensuring intelligent fraud detection in the background. It includes essential features such as user authentication, QR code generation, secure transaction processing, real-time notifications, and automated fraud analysis. This system not only simplifies the payment process but also enhances

user confidence by ensuring secure and reliable transactions. By combining QR code technology with Machine Learning-based intelligence, the platform aims to create a smarter and safer digital payment ecosystem that supports the growing demands of modern financial services.

II. BACKGROUND

The evolution of payment systems has played a crucial role in shaping modern financial technology (FinTech). In earlier times, transactions were primarily cash-based, requiring physical exchange of

money between individuals and businesses. Although simple, this method had several limitations such as lack of security, difficulty in tracking transactions, and inconvenience in carrying physical cash.

With the advancement of banking systems, card-based payments such as debit and credit cards were introduced, enabling electronic transactions through Point of Sale (POS) machines. This marked a significant improvement in payment convenience and security. Later, the emergence of internet banking and mobile banking further transformed the financial ecosystem by allowing users to perform transactions online without visiting banks physically.

In recent years, QR code-based payment systems have become one of the most widely adopted digital payment methods. QR (Quick Response) codes allow users to complete transactions instantly by scanning a code using a mobile device. This technology has gained popularity due to its simplicity, low cost of implementation, and compatibility with smartphones. Platforms such as UPI-based applications have further accelerated the adoption of QR payments in both urban and rural areas. However, with the rapid increase in digital transactions, security concerns have also grown significantly. Cybercriminals exploit vulnerabilities through methods such as QR code tampering, fake payment links, phishing attacks, and transaction manipulation. Traditional security systems rely on predefined rules, which are often unable to detect new or evolving fraud patterns effectively.

To overcome these limitations, Machine Learning (ML) has emerged as a powerful tool in financial security systems. ML based models can analyse large datasets of transaction history, user behavior, device patterns, and location data to identify anomalies and detect fraudulent activities in real time. Unlike rule-based systems, Machine Learning continuously improves its accuracy by learning from new data.

Therefore, integrating Machine Learning with QR-based payment systems represents a significant advancement in digital payment technology. It not only enhances transaction efficiency but also strengthens security, making the payment ecosystem more reliable, intelligent, and user-friendly.

III. METHODOLOGY

The development of the QR Based Online Payment System enhanced with Machine Learning follows a structured Software Development Life Cycle (SDLC) approach to ensure systematic planning, design, implementation, testing, and deployment of the system. The process begins with requirement analysis, where the needs of different users such as customers, merchants, and administrators are studied in detail. This phase focuses on understanding the complete payment workflow, including QR code scanning, transaction processing, and security requirements. Special attention is given to identifying fraud risks and defining the need for a Machine Learning-based detection system to enhance transaction safety.

In the system design phase, the overall architecture of the application is planned, including the frontend user interface, backend server, database structure, and Machine Learning module. The frontend is designed to provide a simple and user-friendly experience for scanning QR codes and making payments, while the backend manages authentication, transaction processing, and data storage. The database is structured to securely store user details, transaction records, and QR code information. The Machine Learning module is designed to analyse transaction patterns and detect suspicious activities in real time, ensuring a secure payment environment.

The implementation phase involves the actual development of system components. This includes building the QR code generation and scanning functionality, integrating payment gateway APIs for secure transactions, and developing backend services for handling requests. The Machine Learning model is trained using historical transaction data to identify fraudulent patterns and is integrated into the system for real-time fraud detection. User authentication modules are also implemented to ensure secure login and role-based access for users and administrators.

In the testing phase, the system is evaluated to ensure accuracy, security, and performance. Unit testing is performed on individual components such as QR scanning, payment processing, and authentication. Integration testing ensures smooth communication between frontend, backend, and the Machine Learning module. The ML model is tested for accuracy in detecting fraud cases, while security testing checks for vulnerabilities such as

International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

unauthorized access and data breaches. Performance testing ensures that the system can handle multiple transactions efficiently without delays.

Finally, in the deployment phase, the system is hosted on a cloud or server environment to make it accessible to users in real time. The database and backend services are configured for secure operation, and the Machine Learning model is deployed for continuous monitoring of transactions. Real-time transaction tracking and alerts are enabled to enhance user experience and security.

Regular updates and maintenance are performed to improve system performance and ensure long-term reliability. and usability.

IV. FLOW DIAGRAM

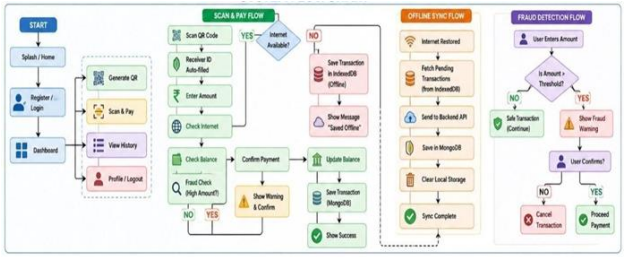


Fig 1. System Flowchart

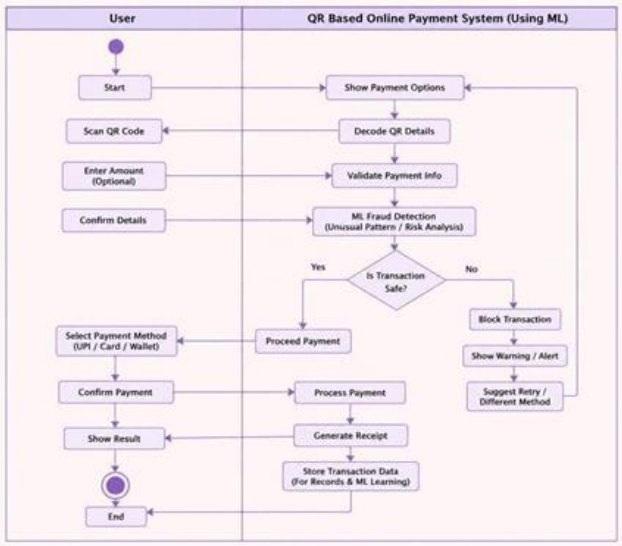


Fig 2.QR Based Online Payment System (Using ML)

This diagram represents the working of a QR Based Online Payment System using Machine Learning (ML). The process starts when the user scans a QR code, after which the system decodes the QR details such as merchant information and amount. The user can enter or confirm the payment amount and proceeds further. The system then validates the payment information and applies an ML-based fraud detection mechanism to analyse risk and detect unusual patterns. If the transaction is considered safe, the user selects a payment method like UPI, card, or wallet, and the payment is processed. If the transaction is not safe, it is blocked and a warning is shown to the user. After successful payment, the system generates a receipt, displays the result to the user, and stores the transaction data for record-keeping and future ML learning

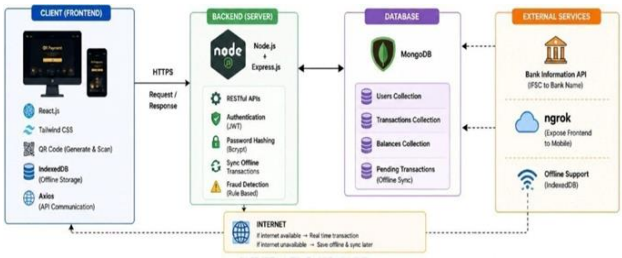


Fig 3. System Architecture Diagram

Functional Requirements:

1. User Registration and Authentication

- The system shall allow users (customers, merchants, and admins) to register using email/username and password.
- The system shall provide secure login functionality for all users.
- The system shall support password recovery options (forgot/reset password).

2. User Profile Management

- Users shall be able to view their personal profile details.
- Users shall be able to update their profile information.
- The system shall securely store all user data.
- The admin shall manage user accounts (activate, deactivate, delete).

3. QR Code Generation

- Merchants shall be able to generate unique QR codes.
- Each QR code shall be linked to a merchant account or payment request.
- QR codes shall contain encrypted payment-related information for security.

4. QR Code Scanning and Payment Initiation

- Users shall be able to scan QR codes using web or mobile applications.
- The system shall retrieve merchant details after scanning.
- The system shall initiate the payment process automatically after scanning.

5. Payment Processing

- Users shall be able to enter payment amount when required.
- The system shall process payments through a secure payment gateway.
- The system shall validate payment details before confirmation.

6. Machine Learning-Based Fraud Detection

- The system shall analyse transactions using ML algorithms.
- It shall detect suspicious or fraudulent activities.
- It shall evaluate factors like transaction amount, frequency, location, and device behavior.

7. Transaction Verification

- The system shall verify all transactions with the payment gateway.
- The system shall integrate ML fraud detection before approval.
- Only verified and valid transactions shall be processed successfully.

8. Transaction History Management

- The system shall store all transaction records securely.
- Users shall be able to view their transaction history.
- Admins shall have access to all transaction logs for monitoring.

9. Notifications and Alerts

- The system shall send real-time notifications for transactions.
- Notifications shall include success, failure, and fraud alerts.
- Alerts may be displayed on dashboard or sent via email.

10. Admin Dashboard

- The admin shall monitor users, transactions, and fraud reports.
- The dashboard shall provide overall system activity tracking.
- The admin shall manage system settings and user permissions.

V. IMPLEMENTATION AND EXPERIMENTAL SETUP

The proposed QR Based Online Payment System is developed using a client–server architecture. The frontend (HTML/CSS/JavaScript or React) provides an interface for users to scan QR codes and enter payment details. The backend (Python Flask/Node.js) processes requests, decodes QR data using OpenCV, and validates transaction details. A Machine Learning model (e.g., Random Forest using Scikit-learn) is integrated for fraud detection by analysing features like transaction amount and user behavior. When a user initiates a payment, the system checks the transaction through the ML model. If the transaction is safe, payment is processed and a receipt is generated; otherwise, the transaction is blocked and a warning is displayed. All transaction records are stored in a database (MySQL/MongoDB) for future reference and model improvement.

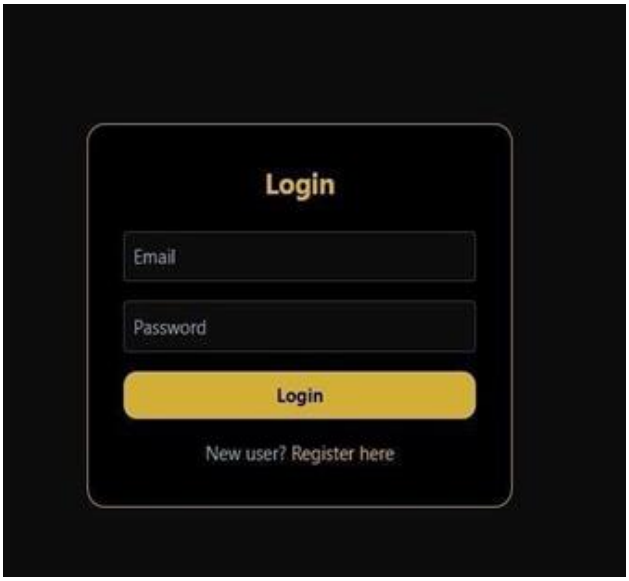
VI. TECHNOLOGY STACK SUMMARY

Component	Description
Frontend	User interface for QR scan & payment (HTML/CSS/JS or React)
Backend	Server handles requests (Flask / Node.js)
QR Processing	QR generate & decode (rode, OpenCV)
ML Model	Fraud detection (Random Forest, Scikit-learn)
Payment Processing	Validate & complete transaction
Database	Store transaction data (MySQL / MongoDB)
Security	ML-based fraud detection + validation

VII. SYSTEM INTERFACE

The system is tested on a standard computer system with required software such as Python, Flask, OpenCV, and Scikit-learn. A dataset containing both normal and fraudulent transaction data is used to train and evaluate the ML model. The performance is measured using metrics like accuracy and precision. Different test cases are executed by varying transaction values and patterns to check system behavior. The results show that genuine transactions are processed successfully, while suspicious transactions are effectively detected and blocked, improving overall security and reliability of the payment system.

International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X



VIII. FUTURE DIRECTION

The future development of the system focuses on enhancing security, scalability, and user experience by integrating advanced technologies. One of the major improvements includes the use of more sophisticated Artificial Intelligence and Machine Learning algorithms for fraud detection, which will help in identifying suspicious transactions more accurately in real time by analysing complex behavioural patterns such as user spending habits, device usage, location changes, and transaction frequency. This will significantly reduce false transactions and improve overall system trust.

Another important direction is the adoption of blockchain technology to make financial transactions more transparent, secure, and tamper-proof. By storing transaction records in a decentralized ledger, the system can ensure data integrity and eliminate the risk of unauthorized modifications. In addition, the development of dedicated mobile applications for both Android and iOS platforms will make QR code-based payments more accessible, faster, and user-friendly, especially in real-world commercial environments.

The system can also be expanded to support multi-currency transactions and integration with global payment gateways, enabling its use for international users and businesses. Furthermore, the incorporation of biometric authentication methods such as fingerprint scanning and facial recognition can strengthen user security and reduce the chances of unauthorized access.

In the future, advanced analytics dashboards can be implemented to provide real-time insights, predictive analysis, and financial behavior reports for users, merchants, and administrators.

Integration with widely used payment systems such as UPI, digital wallets, and banking APIs will further enhance payment flexibility and convenience. Additionally, the system can be optimized using cloud computing and edge computing technologies to handle large-scale transactions efficiently with minimal latency.

Finally, the platform can evolve by adding intelligent recommendation systems that analyse user transaction history and provide personalized financial insights, spending patterns, and alerts. With continuous upgrades in security, performance, and usability, the system has the potential to become a highly scalable, intelligent, and globally adaptable digital payment solution.

IX. CONCLUSION:

In conclusion, the proposed QR Code-Based Secure Payment System integrated with Machine Learning for Fraud Detection presents a comprehensive and modern approach to digital
transactions. The system effectively combines multiple core functionalities such as user registration and authentication, role-based access control, QR code generation and scanning, secure payment processing, transaction verification, and detailed transaction history management. Together, these

features ensure a smooth, efficient, and user-friendly payment experience for customers, merchants, and administrators.

A major strength of the system lies in its integration of Machine Learning techniques for fraud detection. By analysing key parameters such as transaction amount, frequency, location, device behavior, and user patterns, the system is capable of identifying suspicious activities in real time. This significantly enhances the security of financial transactions and reduces the risk of fraud,
making the platform more reliable and trustworthy for users.

The system also provides a centralized admin dashboard that enables effective monitoring and management of users, transactions, and fraud alerts. This improves transparency and gives administrators full control over system operations. Additionally, features such as notifications and alerts ensure that users are continuously updated about their transaction status, further improving user confidence.

From a technical perspective, the system is designed to be scalable, secure, and efficient. It supports multiple simultaneous transactions and ensures fast processing even under high load conditions.
The use of encryption and secure authentication mechanisms strengthens data protection and prevents unauthorized access.

Overall, this project demonstrates a strong foundation for a next-generation digital payment system that is both intelligent and secure. It successfully addresses the limitations of traditional payment methods by introducing automation, real-time fraud detection, and QR-based convenience. With further advancements such as blockchain integration, mobile application development, biometric authentication, and cloud-based scalability, the system can evolve into a highly advanced, globally adaptable financial solution.

REFERENCES

1. H. Singh, V. V. Singh, A. K. Gupta, and P. K. Kapur, “Assessing e-learning platforms in higher education with reference to student satisfaction,” International Journal of System Assurance Engineering and Management, 2024.
2. L. Pham, et al., “Evaluation of the functionality of a new e-learning platform vs. previous experiences,” Sustainability Journal, 2020.
3. L. Pham et al., “Evaluation of the functionality of a new e-learning platform versus previous experiences,” Sustainability, vol. 12, no. 23, 2020.
4. M. M. Sural et al., “Effectiveness of e-learning experience through online quizzes: A case study,” 2023.
5. J. W. Gikandi, D. Morrow, and N. E. Davis, “Online quizzes in a virtual learning environment as a tool for formative assessment,” Computers & Education, 2011.
6. S. Can, “Emerging trends of online assessment systems in higher education,” 2022.
7. M. Yorulmaz and G. J. Hwang et al., “Web-based quiz-game-like formative assessment,” Computers & Education, 2007.
8. F. Merrouch, K. Frasson, and M. Kaltenbach, “An online placement test based on item response theory,” arXiv preprint arXiv:1411.5225, 2014.
9. B. Das, M. Majumder, S. Phadikar, and A. A. Sekh, “Automatic question generation and answer assessment: A survey,” Research and Practice in Technology Enhanced Learning, vol. 16, no. 5, 2021.

10. G. Boateng, V. Kumbol, and E. E. Kaufmann, “Can an AI win Ghana’s National Science and Maths Quiz? An AI grand challenge for education,” arXiv preprint, 2023.
11. I. Sommerville, Software Engineering, Pearson Education.
12. R. S. Pressman, Software Engineering: A Practitioner’s Approach, McGraw Hill.
13. W. Stallings, Cryptography and Network Security, Pearson.
14. A. S. Tanenbaum, Computer Networks, Pearson.
15. T. Mitchell, Machine Learning, McGraw Hill.
16. E. Alpaydin, Introduction to Machine Learning, MIT Press.
17. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press.
18. K. P. Murphy, Machine Learning: A Probabilistic Perspective, MIT Press.
19. N. Koblitz, A Course in Number Theory and Cryptography, Springer.
20. Oracle Corporation, “Oracle Database Documentation,” Official Website.
21. MongoDB Inc., “MongoDB Documentation,” Official Website.
22. Node.js Foundation, “Node.js Documentation,” Official Website.
23. ReactJS Official Documentation, Meta Platforms Inc.
24. Mozilla Developer Network (MDN), “Web Technologies Documentation.”
25. IEEE Xplore Digital Library, “Research papers on machine learning-based fraud detection and digital security systems.”