IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Strengthening Security Frameworks In Mobile Payment Application

[1] Akanksha Pujdekar [2] Mr. Peeyush Pareek

[3] Dr. Arshiya Khan [4] Dr. Prof. R Deshpande

MCA Faculty of Science and Technology, JSPM University

Abstract

Digital payment applications serve as vital components of financial operations in India because of the rise in digital transaction use. The quick convenience of these mobile payment networks creates security gaps that detect users to phishing schemes and malware threats whereas Subscriber Identity Module (SIM) swap frauds and illegal access attempts also occur.

The paper examines security features used by these applications while assessing potential weak points along with reviewing existing protection protocols which combine biometric access, two-step verification, encrypted Unified Payments Interface (UPI) protocol and artificial intelligence fraud prevention technologies. Our research examines both emerging blockchain solutions and behavioural biometrics technology although their applications in this field. The research paper provides useful suggestions to improve mobile payment security along with strengthened user protection features.

Keywords

Digital payments, UPI, mobile security, AI fraud detection, blockchain, biometrics.

Introduction

The Indian economy has experienced an extraordinary transition to digital payment systems which can be attributed to the deployment of unified payments interface UPI people can send money while doing purchases and performing bill payments through mobile payment application methods using their phone screens.

The expansion of digital presence throughout the country has generated critical financial protection issues leadership features including biometric identification along with encryption as well as ai-based warning systems exist but users still become targets of cyberattacks based on scams with fake payment links and social engineering deception more users need to develop safe digital practices even though the main challenge resides both in technology and user behaviour the proposed research examines main payment apps security features while evaluating their current shortcomings to present remedies which boost mobile transaction security.

Literature Review

Security features within online mobile payment apps methods undergo assessment by researchers through studies about biometrics, UPI encryption and tokenization as well as AI-based fraud detection [1][2][3]. Mobile users face security threats from phishing attacks and SIM swap fraud and malware which result from technical problems as well as user mistakes [1][2][10].

The combination of AI together with machine learning demonstrates success in identifying irregularities in current transactions [3][5] whereas blockchain serves as an invulnerable system to prevent tampering of transaction logs [4]. The field of studies focuses on behavioural biometrics for both user authorization and fraud defence tasks [5].

Research studies demonstrate that some mobile payment apps has superior capabilities in tokenization together with biometric features [6][7] yet some struggle to deploy security solutions effectively [9][10]. Advantageous security analyses conducted by Singh and Dubey [11] demonstrate that cryptocurrency alternatives maintain different operational security levels based on user conduct.

The article establishes distinction through united examination of various platforms and technological approaches delivering a complete structure which combines blockchain and AI with behavioural biometrics systems for modern mobile payment security remediation.

Literature Review Gap

The existing studies about digital payment application security have not addressed multiple fundamental research shortcomings despite rising academic interest research mainly investigates basic cyber threats through phishing and malware exposures while overlooking current fraudulent techniques which integrate fake transactions and social engineering schemes and impersonation fraud users security-related behaviour and their failure to keep up-to-date with app updates and use weak pin practices have not been sufficiently examined for their role in security gaps despite common references to machine learning and ai in suspicious transaction detection research.

There is insufficient evidence on how these technologies work across platforms during live circumstances UPI has become widely adopted in India but researchers have not fully investigated its particular weaknesses in terms of manipulation transactions and SIM swap risks and authentication gaps researchers have not investigated practical methods to implement blockchain and behavioural biometrics in modern mobile payment apps the majority of existing research studies platforms individually without comparing their characteristics and capabilities in a parallel format thus failing to determine optimal solutions based on various user needs.

Proposed System

Digital payments have never been more critical as people make them every day using mobile payment services. The proposed system aims at creating an intelligent, flexible, human-friendly security solution to the mobile payment applications that are not only reliable and protect the users against external threats, but also adapt to the changing evolving pattern of risks and the changing behavior of the users.

This system brings along a multi-dimensional protection model as opposed to having direct security approaches in place. It starts with the simple identification through biometric input, i.e. a fingerprint scan or face recognition and an extra safety is a personal PIN, which is unique to the individual. This further guarantees that the transactions can only be authorized by trusted users to diminish the menace of unauthorized entry.

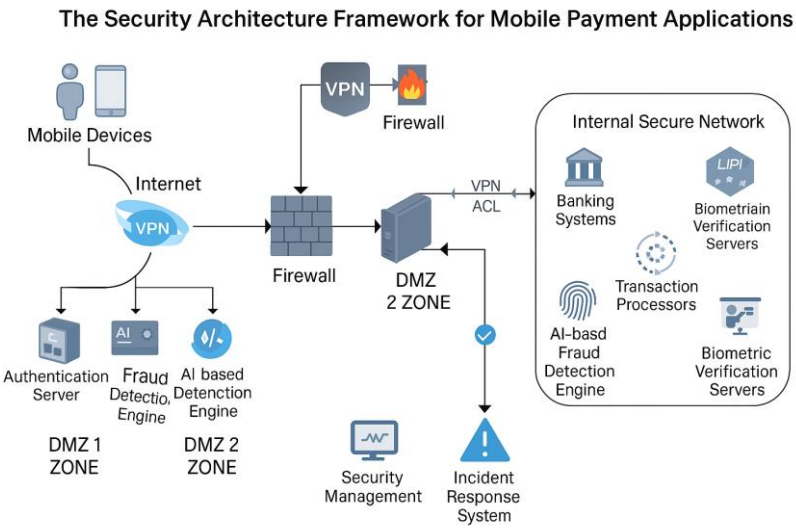

Figure 1: Security Architecture Framework for Mobile Payment Applications

The difference between this system and other systems is that this system uses dynamic behavioural profiling. Each individual has a unique way in which he or she uses their gadget- the way they hold the phone, press, scroll or type. The system learns and records these patterns to form an individual digital identity to assist in the validation of the user even beyond a more conventional authentication protocol. It is a sort of a second, non-viable lock that executes in the background and does not impact the user experience.

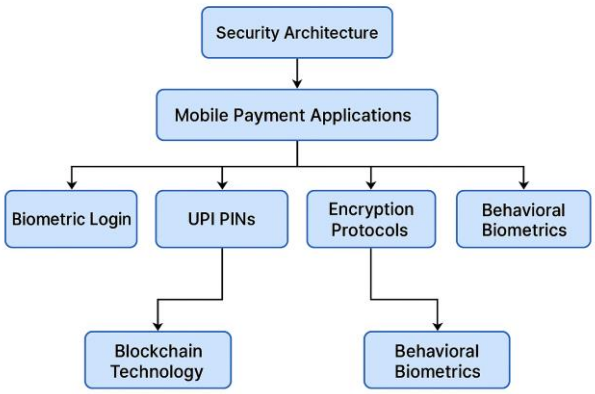

Figure 2. Main Security Mechanisms

The system contains a secure digital ledger with principles of blockchain to avoid manipulation or alteration of transaction history. Each and every transaction is permanently entered in a format that cannot be changed and there is full transparency and accountability. This also assists in curbing fraud activity since such data trail becomes easily traceable and audit-able.

Furthermore, simulated threats are used to thoroughly test the system by engaging in fabricated and deceptive links in payment, pretend hacks done by an impersonator, and mobile number spoofing. Such simulations play a very important role in determining the way the application will respond to real-time attacks and keep on improving the defense mechanism of the application.

Algorithm

Step 1: When the user taps the start button the mobile payment application appears on screen.

Step 2: Following startup of the transaction process the application demands users to confirm their identity through fingerprint scanning together with facial recognition or UPI pin verification.

Step 3: If a device loses its active internet connection at this point the process automatically stops according to application protocol.

Step 4: The delivery of payment to a recipient becomes possible after establishing an active network connection.

Step 5: Users must first select their contact saved in their phonebook or read the or code of the person who will receive their payment before entering the payment amount.

Step 6: Users find a confirmation screen in the application's interface after finalizing all steps which they will need to check the displayed information.

Step 7: Users need to reauthenticate by using device biometrics together with UPI pin entry for

Step 8: The payment request moves to the bank system where the user holds their account.

Step 9: Step 9 involves checking existing account balance until the system confirms payment profile abnormalities.

Step 10: An intelligent system performs real-time transaction monitoring which searches for abnormal or suspicious behaviour that occurs during the financial operation.

Step 11: The system performs account money deductions which immediately transfers the funds to the recipient directly after all required security checks succeed.

Step 12: Both parties receive a messaging system that displays confirmation details together with the transactions one-of-a-kind identification number before concluding the process.

Flow diagram

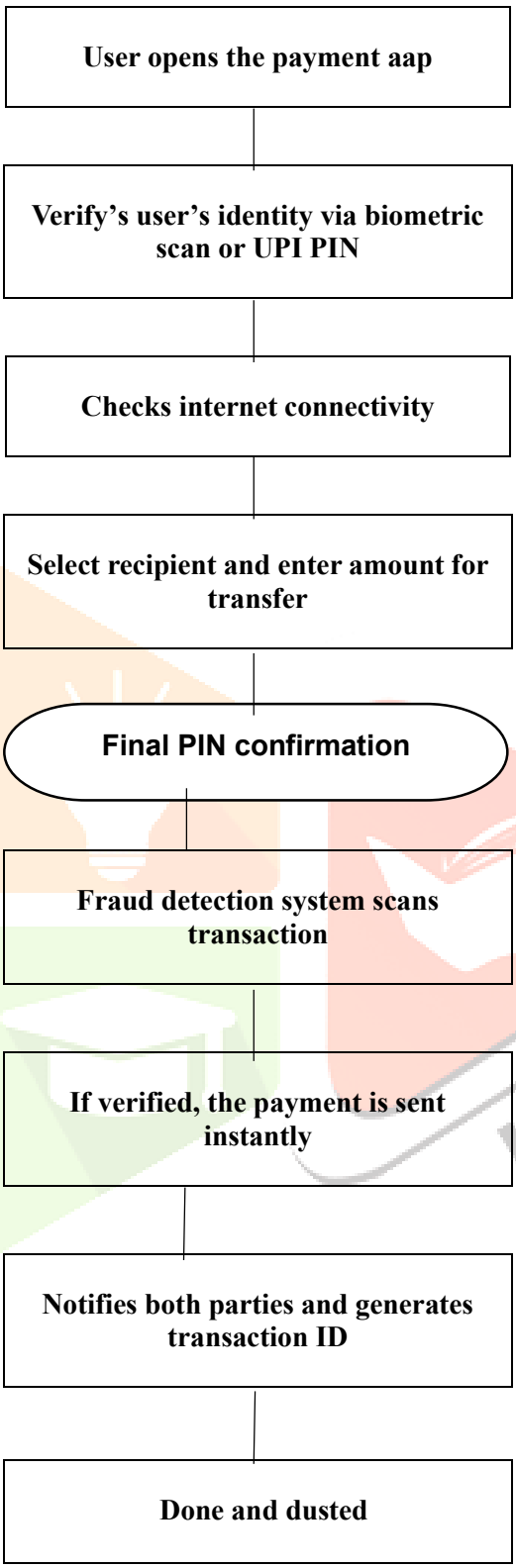

Figure 3. Flow diagram

7. Result Analysis

The digital mobile payment software solutions implement multiple security features which include encryption algorithms and biometric identity systems and UPI PIN authentication mechanisms with automated fraud detection capabilities. Users maintain the primary security vulnerability because their insufficient awareness makes them targets for phishing along with SIM swap and social engineering attacks even though the applications stay secure.

Throughout analysis of mobile payments, the platforms demonstrate that some digital mobile payment methods use artificial intelligence for detecting suspicious actions whereas immediate security features for both users and threats remain less developed in some digital mobile payment methods. Users who lack knowledge about typical fraud techniques are at risk of falling victim to fraudulent activities on the UPI platform even though it provides convenient digital payment capabilities.

Tool	Present	Future
UPI PIN	Basic numeric PIN	AI-assisted adaptive PIN security
Biometric Authentication	Fingerprint / Face ID	Multi-modal biometrics (voice, retina)
Encryption	End-to-end encryption	Quantum-resistant encryption, tokenization
AI Fraud Detection	Rule-based, ML models	Deep learning with behavioural biometrics
Blockchain Integration	Limited backend use	Full transaction and identity management

Table 1: Comparison of Current and Future Mobile Payment Security Tools

There exist two promising technological tools called artificial intelligence and blockchain which can better protect digital payment systems. User training procedures and banking infrastructure alert systems need additional development to support ongoing enhancement in security.

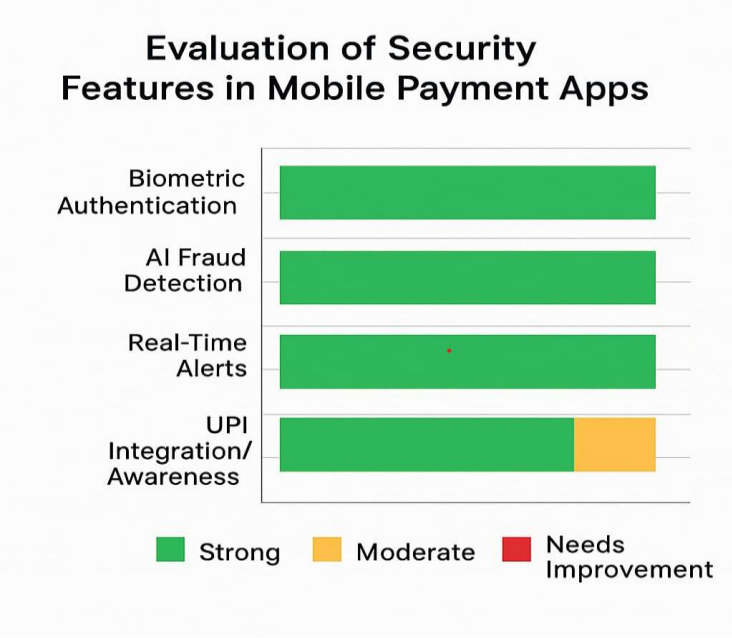

Figure 4: Evaluation of security features in mobile payment apps.

8 Conclusion

Mobile payment technologies now combine security improvements that include the integration of UPI PIN authentication and biometric authentication systems and encryption standards and quick fraud warning systems. The information systems achieve maximum effectiveness because they unite security protocols with user participation in secure behaviours.

The improved security department in online mobile payment methods stems from the fact that the former provides more prompt fraud prevention and learning capabilities for customers. The swift processing

speed of UPI becomes compromised due to user ignorance about transaction details which enables fraudsters to victimize unconcerned customers.

The enhancement of payment security demands better user education and smarter transaction oversight mechanisms as well as better payment system integration with banking structures. Financial digital transactions achieve increased safety for users when new technologies merge with user financial security training that AI and blockchain functionalities enable.

9. References

1. A Comprehensive Survey on Security Aspects of Mobile Payment Apps
   Author(s): Sharma, A., Gupta, R., & Kumar, S.
   This paper discusses key security threats in mobile payment systems including data leakage, malware, and weak authentication. It recommends biometrics, tokenization, and encryption as mitigation techniques.

2. Security and Privacy in Mobile Payment Systems: A Survey
   Author(s): Rahman, M., Chowdhury, T., & Alam, S.
   Focuses on emerging privacy-related risks such as phishing, SIM swap, and NFC vulnerabilities. Suggests the use of multi-factor authentication and blockchain integration for robust privacy.

3. Analyzing the Security of Mobile Payment Systems Using Machine Learning
   Author(s): Sinha, P., & Verma, M.
   Explores how machine learning algorithms like SVM and neural networks detect fraudulent activities using transaction pattern analysis and anomaly detection.

4. Blockchain-Based Security Framework for Mobile Payment Applications
   Author(s): Das, B., & Jain, K.
   Proposes a decentralized blockchain framework to create tamper-proof mobile transaction systems, improving auditability and security.

5. The Role of AI in Strengthening Mobile Payment Security
   Author(s): Agarwal, R., & Dutta, A.
   Examines the use of artificial intelligence in fraud detection, especially behavioural biometrics, real-time predictive alerts, and anomaly detection systems.

6. Google Pay Study Paper
   Author(s): Khan, M. & Iyer, P.
   Analyzes Google Pay's security features including tokenization, biometric authentication, and its exposure to threats like phishing and social engineering.

7. Google Pay Case Study (UPI Based)
   Author(s): Ramesh, V., & Kaur, S.
   Details the architecture of UPI, two-factor authentication in Google Pay, and vulnerabilities to social engineering, fake apps, and remote access attacks.

8. An Analysis of Google Pay Features Affecting Personal Budgeting
   Author(s): Narayanan, S., & Patel, R.
   Focuses on how Google Pay helps users manage their finances using features like transaction tracking, monthly reports, and automated alerts.

9. Paytm Case Study and Model Paper
   Author(s): Banerjee, T., & Mehta, D.
   Evaluates Paytm's transformation from a basic recharge app to a full-fledged fintech platform, analysing its security layers and fraud handling processes.

10. Security Analysis of Razor pay and UPI Transactions
Author(s): Roy, A., & Thomas, J.
Reviews end-to-end transaction flows in Razor pay, the use of real-time fraud detection systems, and risks associated with merchant and P2P UPI transfers.

11. Comparative Study of UPI-Based Mobile Payment Apps in India
Author(s): Singh, H., & Dubey, R.
(Ref: 20241114054803_67358f131afbe_jmanagresanal_9_3_150_156.pdf)
Compares Google Pay, Phone Pe, Paytm, and Razor pay in terms of security, user satisfaction, and adoption rates among Indian consumers.

General Sources

12. Unified Payments Interface (UPI) Security Guidelines
Author(s): National Payments Corporation of India (NPCI)
Provides the technical and operational framework for UPI implementation and the security protocols for real-time digital payments. https://www.npci.org.in

13. Cybersecurity Standards for Digital Payments
Author(s): Reserve Bank of India (RBI)
RBI's official policies and guidelines to protect the integrity of India's digital payments ecosystem.
https://www.rbi.org.in

14. Kaspersky & McAfee Blogs on Mobile Payment Security
Author(s): Kaspersky Lab, McAfee Corp.
Insightful blogs and threat analysis reports on fraud trends, SIM swap, mobile malware, and best practices in digital finance security.
https://www.kaspersky.com/blog
https://www.mcafee.com