Int. J. Sci. R. Tech., 2026 3(3)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

Secure Bank: Enhancing Trust Through Advanced Websecurity

Prasad Gavhane, Atharva Ghule, Yash Shinde*, Priti Malkhede

Artificial Intelligence and Data Science, P.E.S Modern College of Engineering, Pune, India

ABSTRACT

The digital transaction landscape has undergone a paradigm shift with the advent of real-time payment infrastructures like the Unified Payment Interface (UPI). While these systems offer unprecedented convenience, they introduce complex security challenges ranging from sophisticated phishing attacks to static QR code tampering. This paper presents "Secure Bank," a comprehensive software requirement specification for a full-stack, non-custodial digital wallet. By synthesizing recent advancements in ensemble learning for fraud detection [1], dynamic QR code generation [2], and conversational payment pipelines [3], Secure Bank aims to mitigate the "risk-risk trade-off"($R^2T$) users face between cash health hazards and digital security risks [4]. The proposed system integrates a Neural Network-based Ensemble Learning model (NNEnsLeG) to handle data imbalance in fraud detection and utilizes blockchain- verified QR codes to ensure transaction immutability. Furthermore, it addresses financial inclusion by incorporating voice-based accessibility features designed for "Bottom of the Pyramid" (BoP) users [5].

Keywords: Digital Wallet, UPI, Ensemble Learning, Dynamic QR Codes, Conversational Payments, Phishing Mitigation, Risk-Risk Trade-off, Zero Trust Architecture, Explainable AI (XAI)

INTRODUCTION

The proliferation of mobile devices has accelerated the adoption of mobile payment systems (MPS), positioning them as a critical lifeline for economic inclusion, particularly in developing economies. The transition from cash to digital is not merely a matter of convenience; it is a complex decision governed by a "risk-risk trade-off" ($R^2T$). As identified by Pal et al., users must weigh the health risks associated with physical cash (contamination, transmission) against the technological risks of mobile payments (privacy, performance, and security) [4]. Despite the growth of digital payments, trust remains a fragile commodity. Traditional custodial wallets often act as single points of failure, vulnerable to centralized data breaches and "quishing" (QR phishing) attacks [18]. Furthermore, standard rule-based fraud detection systems struggle to adapt to the dynamic nature of modern financial crime. "Secure Bank" addresses these concerns by establishing a trusted transaction environment. Unlike traditional custodial wallets, Secure Bank operates as a secure client orchestrator that does not hold fiat balances, thereby reducing the custodial risk profile. It enhances user trust by integrating three core pillars: proactive fraud prevention derived from advanced neural networks [1], accessible conversational interfaces for diverse user demographics [3], and robust authentication protocols aligned with NIST standards [6]. This paper reviews the architectural principles of Secure Bank in the context of current state-of-the-art research. We examine the evolution of QR code security, the application of ensemble learning for fraud detection, and the behavioral determinants of UPI adoption to validate the proposed system's design.

LITERATURE REVIEW

A. The Evolution of QR Code Security

QR codes have evolved from simple inventory tracking tools to the backbone of modern digital banking. Bhattacharya and Singla highlight how QR codes now facilitate everything from identity verification to secure online transactions, replacing traditional paper-based banking methods [7]. However, the ubiquity of static QR codes has made them a prime target for fraud. Yadav et al. propose Dynamic QR Codes as a solution to the vulnerabilities

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

of static codes. Unlike static codes, which are permanent and easily cloned, dynamic codes refresh periodically or per transaction, utilizing cryptographic techniques like SM2 and SM3 algorithms to ensure uniqueness and randomness [2]. This mechanism effectively mitigates replay attacks and unauthorized data reuse. Furthermore, Udoy et al. introduce the 4SQR-Code model, a novel 4-state generation process that significantly increases data storage capacity compared to traditional 2-state codes. By utilizing a 4-state pattern (Black Square, White Square, Triangle, Circle), this model enhances the security payload capacity within the QR matrix, making it suitable for complex digital twin frameworks where high-density data transmission is required [8].

B. AI-Driven Fraud Detection Strategies

The sophistication of e-commerce fraud requires dynamic defense mechanisms. Traditional machine learning models often struggle with the "class imbalance" problem, where legitimate transactions vastly outnumber fraudulent ones. Zeng et al. introduce NNEnsLeG (Neural Network-Based Ensemble Learning with Generation), a comprehensive model designed to address this specific challenge [1]. NNEnsLeG combines ensemble learning with a data generation module that produces synthetic fraud samples during training. This prevents the model from overfitting to legitimate transaction patterns and allows it to simulate dynamic fraud behaviors. Experimental results show that NNEnsLeG outperforms standard benchmarks like Random Forest, XGBoost, and isolated Neural Networks in detecting e-commerce payment fraud [1]. Recent surveys on credit card fraud detection also emphasize the necessity of Explainable AI (XAI) to make these black-box models transparent to regulators and users, bridging the gap between accuracy and interpretability [15], [19].

C. Phishing Mitigation and Human-Centric Security

Phishing remains a primary vector for financial loss, evolving from simple email scams to sophisticated "smishing" (SMS phishing) and "vishing" (voice phishing) attacks. Naqvi et al. conducted a systematic literature review of 248 articles, identifying that technical filters alone are insufficient [9]. They advocate for human-centric mitigation strategies that account for user behavior and risk perception. Their findings suggest that anti-phishing guidelines must be integrated directly into the transaction flow, providing real-time warnings and educational nudges to users [9]. Ahmed et al. further survey the security landscape of next-generation mobile payment systems, emphasizing the need to protect mobile money servers against Distributed Denial of Service (DDoS) attacks. They classify attacks into categories affecting privacy, authentication, confidentiality, and integrity, underscoring the need for a multi-layered security approach [10].

D. Behavioral Determinants of Adoption

Understanding why users adopt or reject digital payments is crucial for system design. Fahad and Shahid utilize the Diffusion of Innovation (DOI) theory to explore UPI adoption in India [11]. They identify "relative advantage," "complexity," and "observability" as key determinants. Their study reveals that while users appreciate the relative advantage of UPI over cash, perceived complexity remains a significant barrier. Complementing this, Pal et al. introduce the Risk-Risk Trade-off (R^2T) framework. Their study posits that user decision-making is a negotiation between the health risks of cash (e.g., virus transmission during a pandemic) and the digital risks of mobile payments (e.g., fraud, privacy loss) [4]. This framework suggests that digital wallets must not only be secure but must also visibly demonstrate their safety superiority over cash to drive continued usage.

E. Financial Inclusion and Accessibility

For "Bottom of the Pyramid" (BoP) users, technology must be inclusive. Sinha et al. argue that mobile payments can drive positive social change by providing financial inclusion to street vendors and low-income workers [5]. However, literacy barriers often hinder adoption. To bridge this gap, Kamaraju et al. propose a Conversational Payment Pipeline for UPI apps. By leveraging Automatic Speech Recognition (ASR) models like Whisper and multilingual NLP engines (e.g., MuRIL), this pipeline allows users to execute transactions using voice commands in local languages (e.g., "Send 100 rupees to Raju") [3]. This dramatically reduces the complexity barrier identified in DOI studies. Additionally, Pino et al. discuss accessible Point of Sale (POS) systems that use "beep-systems" to guide visually impaired users through transaction steps, ensuring autonomy and security [12].

F. Blockchain and Decentralized Verification

Blockchain offers a path toward decentralized trust. Kim and Kim propose an e-commerce payment model that eliminates intermediaries like Payment Gateways (PG) by using blockchain public/private keys for direct verification, thereby reducing transaction fees [13]. Furthermore, Sharma highlights blockchain's role in protecting Geographical Indications (GIs), ensuring that products purchased via digital wallets are authentic and traceable to their origin, thus preventing counterfeiting [14]. Recent research also explores Zero Trust Architecture (ZTA) in banking, which operates on the principle of "never trust, always verify," eliminating implicit trust even for users inside the network perimeter [20].

System Architecture: Secure Bank

Secure Bank employs a microservices-inspired architecture comprising a React frontend, a Flask backend, and a specialized Machine Learning service.

A. Intelligent Fraud Detection Engine (Adapting NNEnsLeG)

The core security component of Secure Bank is an intelligent fraud detection engine that moves beyond static rule sets.

- **Ensemble Learning Framework:** Drawing from the NNEnsLeG model [1], Secure Bank utilizes an ensemble of classifiers. This approach aggregates predictions from multiple models to improve accuracy and robustness against novel fraud patterns.

- **Synthetic Data Generation:** To handle the class imbalance inherent in financial datasets (where fraud is rare), the system incorporates a data generation module. This module creates synthetic fraud samples during the training phase, ensuring the model learns to identify fraud markers effectively without overfitting to the majority class [1].

- **Behavioral Feature Engineering:** The engine analyzes distinct feature sets including transaction indicators (amount, frequency), user behavior (login rituals, device changes), and account correlations (IP address clusters), as recommended by Zeng et al. [1].

- **Explainability Integration:** Incorporating XAI techniques like SHAP (SHapley Additive exPlanations) ensures that when a transaction is flagged, the user receives a clear reason (e.g., "Unusual location" or "High-value transfer to new beneficiary"), building trust in the AI system [21].

B. Dynamic and Blockchain-Verified QR Infrastructure

To mitigate the risks of static QR codes identified by Yadav et al. [2], Secure Bank implements a dynamic QR generation protocol.

- **Time-Bound Validity:** Generated QR codes expire after a set duration, preventing replay attacks.

- **Cryptographic Verification:** Aligning with the blockchain models proposed by Kim and Kim [13], transactions are signed using private keys. The system leverages blockchain principles to verify the integrity of the transaction data, ensuring that the QR code payload (payee, amount) has not been tampered with. This establishes a "trustless" verification layer where users do not need to rely solely on the central server's integrity. Recent studies on blockchain-based UPI technology further validate this approach for securing peer-to-peer transactions [22].

C. Voice-First Conversational Interface

Secure Bank integrates the Conversational Payment Pipeline proposed by Kamaraju et al. [3] to democratize access.

- **ASR & NLP Integration:** The system captures audio commands and processes them through an ASR module (e.g., OpenAI Whisper) to convert speech to text. An Intent Classification model (fine-tuned BERT or MuRIL) then maps the text to specific banking actions (e.g., PAY_USER, CHECK_BALANCE) and extracts entities like names and amounts.

• **Multilingual Support:** By supporting local languages, the platform addresses the "complexity" barrier identified in the DOI study [11], making digital payments accessible to BoP users with lower digital literacy.

D. Advanced Security and Phishing Mitigation

Secure Bank implements a multi-layered security strategy informed by the comprehensive surveys of Ahmed et al. [10] and Naqvi et al. [9].

• **NIST-Aligned MFA:** Following the systematic review by Tran-Truong et al. [6], the platform mandates multi-factor authentication (MFA) for high-value transactions. This combines "something you know" (PIN) with "something you have" (device token) or "something you are" (biometrics). Recent research into behavioral biometrics suggests measuring keystroke dynamics and touch interaction as a passive, continuous authentication layer [23].

• **Heuristic Phishing Detection:** The system employs heuristic analysis to flag suspicious URLs and "look-alike" domains often used in social engineering attacks, providing real-time warnings to users before they authorize a transaction.

DISCUSSION

A. Mitigating the Risk-Risk Trade-off (R^2T)

The R^2T framework posits that users choose between cash and mobile payments by weighing their respective risks [4]. By implementing rigorous fraud detection and decentralized verification, Secure Bank lowers the perceived "technological risk" of the digital wallet. Simultaneously, by offering a contactless, voice- enabled interface, it amplifies the safety benefits over cash (avoiding contamination and theft). This dual approach effectively tips the trade-off in favor of digital adoption.

B. Enhancing Financial Inclusion

The integration of conversational payments directly addresses the needs of the BoP segment [5]. By removing the requirement for text-based navigation, Secure Bank makes digital finance accessible to illiterate or semi-literate users. Furthermore, the inclusion of accessible POS features [12] ensures that visually impaired users can transact independently, fostering a truly inclusive financial ecosystem.

CONCLUSION

Secure Bank represents a next-generation digital wallet that moves beyond basic transaction processing to offer a secure, intelligent, and inclusive financial platform. By synthesizing the NNEnsLeG fraud detection model [1], dynamic QR cryptographic verification [2], and conversational AI [3], the system effectively mitigates the security risks that traditionally hinder digital adoption. It addresses the complexity barriers identified in innovation theories [11] and provides a robust defense against the evolving threat landscape outlined in security surveys [10]. Future work will focus on integrating Geographical Indication (GI) protection via blockchain [14] and exploring Zero Trust principles to further secure merchant authenticity and expand the trusted ecosystem [20.

REFERENCE

1. Q. Zeng, L. Lin, R. Jiang, W. Huang, and D. Lin, "NNEnsLeG: A novel approach for e-commerce payment fraud detection using ensemble learning and neural networks," Information Processing and Management, vol. 62, 2025.
2. O. P. Yadav, A. Kumar, K. Shandilya, and S. Kumar, "Dynamic QR Codes: A Solution for Secure Mobile Payments," Proc. Int. Conf. Cybersecurity and Cybercrime, vol. XI, 2024.
3. S. K. Kamaraju, J. Hegde, S. Panchal, T. Gandi, and S. Shrivastav, "Conversational Payments on UPI Apps: A Pipeline Approach Leveraging ASR and NLP Techniques," CODS-COMAD Dec 24, 2024.
4. A. Pal, R. Dé, and H. R. Rao, "The risk-risk trade-off (R2T) framework: Examining contact [cash] versus contactless [mobile] payment usage,"

Decision Support Systems, vol. 196, 2025. versus contactless [mobile] payment usage.pdf]

5. N. Sinha, J. Paul, and N. Singh, "Mobile payments for bottom of the pyramid: Towards a positive social change," Technological Forecasting & Social Change, vol. 202, 2024.
6. P. T. Tran-Truong et al., "A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis," Journal of Systems Architecture, vol. 162, 2025.
7. S. Bhattacharya and B. Singla, "The Role of QR Code Technology in Revolutionizing Banking," Journal of Computers, Mechanical and Management, vol. 3, no. 3, 2024.
8. A. I. Udoy et al., "4SQR-Code: A 4-state QR code generation model for increasing data storing capacity in the Digital Twin framework," Journal of Advanced Research, vol. 66, pp. 15-30, 2024.
9. B. Naqvi et al., "Mitigation strategies against the phishing attacks: A systematic literature review," Computers & Security, vol. 132, 2023.
10. W. Ahmed et al., "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey," IEEE Access, vol. 9, 2021.
11. M. S. Fahad and M. Shahid, "Exploring the determinants of adoption of Unified Payment Interface (UPI) in India: A study based on diffusion of innovation theory," Digital Business, vol. 2, 2022.
12. B. Pino, M. D. Sánchez, and Z. Sancha, "Towards Payment Systems for All: Accessible POS," Journal of Accessibility and Design for All, vol. 4, no. 3, pp. 255- 269, 2014.
13. S.-I. Kim and S.-H. Kim, "E-commerce payment model using blockchain," Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 1673-1685, 2020.
14. U. Sharma, "The Role of Blockchain in Protecting Geographical Indications Worldwide," Abhidhvaj Law Journal, vol. 3, no. 3, 2025.
15. J. Zhang et al., "Explainable AI for credit card fraud detection: Bridging the gap between accuracy and interpretability," World Journal of Advanced Research and Reviews, 2025.
16. S. Vasan, "Evaluating Security Concerns and User Trust in UPI-Based Digital Payment Systems," ResearchGate, Dec. 2024.
17. M. Baza et al., "Blockchain Mobile Wallet with Secure Offline Transactions," CMC, vol. 75, no. 2, 2023.
18. S. Tiwary et al., "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions," 2024 2nd International Conference on Disruptive Technologies (ICDT), IEEE, 2024.
19. B. Lebichot et al., "Machine Learning Methods for Credit Card Fraud Detection: A Survey," IEEE Access, vol. 12, pp. 158939 - 158965, 2024.
20. "Zero Trust Architecture in Banking: A New Paradigm for Cybersecurity Protection," ResearchGate, 2024.
21. "Explainable AI for Fraud Detection in Financial Transactions," Journal of Information Systems Engineering and Management, 2024.
22. "Blockchain Based UPI Technology for Secured Peer-to-Peer Cryptocurrency Transactions," IEEE Conference Publication, 2023.
23. "Behavioral Biometrics for Mobile User Authentication: Benefits and Limitations," IEEE Conference Publication, 2023.
24. "Authentication using Biometric Data from Mobile Cloud Computing in Smart Cities," IEEE Conference Publication, 2023.
25. "Secure Mobile Payment Architecture Enabling Multi-Factor Authentication," IEEE Conference Publication, 2023.

HOW TO CITE: Prasad Gavhane, Atharva Ghule, Yash Shinde*, Priti Malkhede, Secure Bank: Enhancing Trust Through Advanced Websecurity, Int. J. Sci. R. Tech., 2026, 3 (3), 217-221. https://doi.org/10.5281/zenodo.18942390