RADemics

Real-Time Fraud Detection in Mobile and UPI-Based Payment Systems Using AI

V. Balaraju, M. Vidya
MJR College of Engineering and Technology, Excel Engineering College

Real-Time Fraud Detection in Mobile and UPI-Based Payment Systems Using AI

[1]V. Balaraju, Assistant Professor, Department of EEE, MJR College of Engineering and Technology, Piler, Andhra Pradesh, India. vbraju.tpt@gmail.com

[2]M. Vidya, Assistant Professor, Department of CSE, Excel Engineering College, Namakkal, Tamil Nadu. vidyamcse97@gmail.com

Abstract

The exponential growth of mobile banking applications and Unified Payments Interface (UPI)-based digital transactions transformed modern financial ecosystems by enabling seamless, real-time, and cashless payment services across global markets. Rising transaction volumes, increasing smartphone penetration, and expanding fintech infrastructures simultaneously intensified vulnerabilities associated with cyber fraud, identity theft, phishing attacks, account takeover attempts, QR-code manipulation, and financial data breaches. Conventional rule-based fraud detection mechanisms demonstrate limited capability in identifying sophisticated and evolving attack patterns within high-speed digital payment environments due to static analytical structures and high false-positive rates. Artificial Intelligence (AI) and Machine Learning (ML) technologies emerged as powerful solutions for enhancing fraud prevention through intelligent transaction monitoring, behavioral analytics, anomaly detection, and predictive risk assessment. This book chapter presents a comprehensive analysis of real-time fraud detection frameworks designed for mobile and UPI-based payment systems using advanced AI-driven methodologies. The chapter critically examines supervised learning, unsupervised learning, ensemble models, deep learning architectures, behavioral biometrics, and contextual authentication mechanisms for detecting fraudulent financial activities with improved accuracy and reduced computational latency. Significant emphasis focuses on cloud-edge computing architectures, explainable AI, federated learning, graph-based fraud analytics, and adaptive cybersecurity strategies capable of strengthening transaction security within large-scale financial networks. Critical challenges involving imbalanced datasets, adversarial attacks, privacy preservation, scalability limitations, and regulatory compliance receive detailed analytical attention to support development of resilient and trustworthy fraud prevention ecosystems. Comparative evaluation of intelligent fraud detection models demonstrates the effectiveness of AI-enabled security frameworks in minimizing financial losses, improving transaction reliability, and enhancing user trust within digital payment infrastructures. The chapter contributes toward advancing next-generation financial cybersecurity research through integration of intelligent analytics, real-time monitoring, and adaptive fraud prevention mechanisms suitable for highly dynamic mobile and UPI transaction environments.

Keywords: Artificial Intelligence, UPI Fraud Detection, Mobile Payment Security, Machine Learning, Real-Time Fraud Analytics, Behavioral Authentication

Introduction

The rapid transformation of digital financial ecosystems significantly accelerated the adoption of mobile banking applications and Unified Payments Interface (UPI)-based transaction platforms across global markets [1]. Continuous advancements in smartphone technologies, internet connectivity, cloud computing infrastructures, and financial technology services contributed toward widespread implementation of cashless payment systems within both developed and developing economies [2]. Mobile and UPI payment platforms support instant peer-to-peer transfers, merchant transactions, online retail purchases, utility bill payments, and financial services with enhanced accessibility and operational convenience [3]. Growing consumer dependence on digital payment ecosystems increased transaction volumes across interconnected banking networks and fintech platforms. Financial institutions and governments actively promoted digital transaction infrastructures to strengthen economic digitization, financial inclusion, and transparent monetary circulation [4]. Expanding adoption of real-time payment systems simultaneously increased exposure to cybersecurity risks, fraudulent financial activities, identity theft, and sophisticated cyberattacks targeting sensitive user credentials and transactional information within highly dynamic digital payment environments [5].

The increasing complexity of cyber threats within mobile payment ecosystems created major security concerns for banking organizations, fintech industries, regulatory authorities, and consumers [6]. Fraudulent activities involving phishing attacks, QR-code manipulation, account takeover attempts, SIM swapping, malware injection, fake payment applications, and credential theft generated substantial financial losses and reputational damage across digital banking infrastructures [7]. Real-time payment architectures process large volumes of financial transactions continuously, creating operational challenges for traditional fraud prevention mechanisms dependent on static transaction rules and predefined security thresholds [8]. Conventional rule-based fraud detection frameworks demonstrate limited capability in identifying adaptive fraud behaviors, hidden transaction anomalies, and emerging cyberattack strategies due to restricted analytical flexibility and manual rule maintenance requirements [9]. High false-positive rates associated with conventional fraud monitoring systems also negatively affect user experience, transaction efficiency, and customer trust within digital payment ecosystems [10]. Such operational limitations created significant demand for intelligent and adaptive cybersecurity frameworks capable of supporting real-time fraud prevention within large-scale financial transaction environments.