RADemics

AI-Enabled Risk Assessment and Secure Digital Payment Systems

S. Mohanap Priya, Anushree Wagde
KAMARAJ COLLEGE OF ENGINEERING AND TECHNOLOGY, G. H. RAISONI COLLEGE OF ENGINEERING AND MANAGEMENT

AI-Enabled Risk Assessment and Secure Digital Payment Systems

[1]S. Mohanap Priya, Assistant Professor, Department of Artificial Intelligence and Data Science, Kamaraj College of Engineering and Technology, Madurai, Tamil Nadu, India. mohanappriyapree@gmail.com

[2]Anushree Wagde, Assistant professor, Department of computer engineering, G. H. Raisoni college of engineering and management, Nagpur, Maharashtra, india. anushree.wagde@ghrstu.edu.in

Abstract

Rapid expansion of digital payment ecosystems has intensified exposure to fraud, cyber threats, operational vulnerabilities, and regulatory pressures. Conventional rule-based security mechanisms struggle to address the scale, velocity, and evolving complexity of modern transaction environments. Artificial intelligence has emerged as a transformative enabler for intelligent risk assessment and secure payment operations by supporting data-driven decision-making, adaptive threat detection, and real-time response. This book chapter presents a comprehensive examination of AI-enabled risk assessment frameworks within secure digital payment systems, highlighting machine learning, deep learning, unsupervised learning, and hybrid intelligence approaches for transaction monitoring, behavioral analysis, anomaly detection, and fraud mitigation. Emphasis is placed on end-to-end security architectures, explainable and privacy-preserving AI techniques, and real-time risk scoring models that balance security effectiveness with user experience and regulatory compliance. Key challenges related to data privacy, model transparency, governance, and scalability receive critical analysis, alongside emerging solutions such as federated learning and interpretable analytics. The chapter synthesizes fragmented research into an integrated perspective, offering valuable insights for researchers, practitioners, and policymakers seeking to design resilient, trustworthy, and future-ready digital payment systems.

Keywords: Artificial Intelligence, Digital Payment Systems, Risk Assessment, Fraud Detection, Privacy-Preserving AI, Explainable AI.

Introduction

The global financial ecosystem has undergone a profound transformation driven by the rapid adoption of digital payment systems across banking, commerce, and financial technology platforms [1]. Electronic payment mechanisms such as mobile wallets, online banking portals, contactless cards, and peer-to-peer payment applications have reshaped transactional behavior by enabling speed, accessibility, and convenience at unprecedented scales [2]. This widespread digitalization has accelerated financial inclusion and operational efficiency while supporting seamless cross-border transactions [3]. At the same time, the increasing reliance on digital infrastructures has expanded the exposure of payment systems to complex and evolving risks [4]. High transaction velocity, massive data volumes, and interconnected payment networks have created environments where traditional security controls struggle to maintain effectiveness. As

digital payments continue to replace cash-based transactions, ensuring transaction integrity, user trust, and systemic resilience has become a critical priority for financial institutions and regulators alike [5].

The risk landscape associated with digital payment systems extends beyond conventional financial loss to encompass fraud, cyberattacks, identity misuse, operational disruptions, and regulatory non-compliance [6]. Sophisticated attack strategies exploit vulnerabilities across multiple layers of payment architectures, including user interfaces, application programming interfaces, network infrastructures, and backend processing systems [7]. Static, rule-based risk assessment mechanisms lack the adaptability required to detect emerging fraud patterns and coordinated attacks operating across channels and jurisdictions [8]. Delayed detection and excessive false alerts further undermine operational efficiency and customer experience [9]. As payment ecosystems evolve toward greater automation and decentralization, risk management approaches require continuous learning, contextual awareness, and real-time decision capability. Addressing these challenges demands advanced analytical techniques capable of operating effectively under dynamic conditions and large-scale data flows [10].

Artificial intelligence has emerged as a foundational technology for enhancing risk assessment and security within digital payment systems [11]. Learning-based models enable automated analysis of complex transaction patterns, behavioral signals, and contextual attributes that exceed human interpretative capacity [12]. Machine learning and deep learning techniques support predictive risk classification, behavioral modeling, and anomaly detection by identifying non-linear relationships and subtle deviations indicative of malicious activity [13]. Unsupervised and hybrid intelligence approaches further extend detection capability to unknown and evolving threat scenarios. Through continuous adaptation and feedback integration, AI-enabled systems support proactive risk mitigation rather than reactive response [14]. Such capabilities represent a paradigm shift from static security enforcement toward intelligent, adaptive protection mechanisms embedded throughout the payment lifecycle [15].