RADemics

AI and IoT for Digital Payment Systems and Financial Security

Preeti Srivastava, Prathibha Kiran
BBD University, AMC Engineering college

AI and IoT for Digital Payment Systems and Financial Security

[1]Preeti Srivastava, Assistant Professor, BBD University, Lucknow, India. spreet0801@bbdu.ac.in

[2]Prathibha Kiran, Associate Professor, Dept of ECE, AMC Engineering college,Bangalore, Karnataka. India.prathibha.kiran@amceducation.in

Abstract

The rapid expansion of digital payment ecosystems has transformed global financial transactions through the convergence of Artificial Intelligence (AI) and the Internet of Things (IoT). Smart point-of-sale terminals, wearable payment devices, biometric authentication systems, and cloud-integrated banking platforms generate massive volumes of real-time transactional data, demanding intelligent, scalable, and secure processing frameworks. Conventional security architectures struggle to address evolving cyber-financial threats, including adaptive fraud schemes, adversarial attacks, identity compromise, and decentralized finance exploits. An integrated AI–IoT security paradigm offers a resilient solution by enabling real-time anomaly detection, adaptive risk scoring, device-level authentication, and continuous behavioral monitoring across distributed financial infrastructures. This book chapter presents a comprehensive exploration of AI-driven analytics, reinforcement learning–based adaptive decision models, federated learning for privacy-preserving intelligence, and lightweight deployment strategies tailored for resource-constrained IoT financial devices. A unified Zero-Trust architecture combined with blockchain-assisted auditability strengthens transaction integrity while ensuring regulatory compliance and data governance alignment. Emphasis is placed on explainable AI mechanisms to enhance transparency in automated financial decision-making and to support accountability within high-stakes payment environments. Emerging research challenges, including adversarial robustness, energy-efficient model optimization, and cross-platform interoperability, are critically examined to establish a forward-looking framework for secure digital finance. The proposed perspective advances a scalable and privacy-aware AI–IoT integrated security architecture designed to mitigate financial risk, reduce false positives, and enhance trust in decentralized and intelligent payment systems. This contribution aims to support researchers, financial technologists, and policy architects in developing next-generation digital payment infrastructures capable of sustaining security, efficiency, and transparency in an increasingly connected global economy.

Keywords: Artificial Intelligence; Internet of Things; Digital Payment Systems; Financial Security; Reinforcement Learning; Zero-Trust Architecture.

Introduction

Digital payment systems have undergone a profound structural transformation driven by rapid advancements in Artificial Intelligence (AI), the Internet of Things (IoT), high-speed communication networks, and cloud-based financial infrastructures [1]. The global economy increasingly relies on contactless transactions, mobile wallets, biometric authentication platforms, and decentralized financial services that operate across interconnected digital ecosystems. Payment terminals, wearable devices, smart ATMs, and embedded financial sensors continuously generate transactional and behavioral data streams that require real-time processing and secure validation [2]. Such expansion enhances convenience, operational efficiency, and financial inclusion, while simultaneously enlarging the cyber-attack surface within distributed payment architectures. Sophisticated fraud schemes, identity manipulation techniques, and coordinated cyber intrusions target vulnerabilities across network layers, application interfaces, and device firmware [3]. Traditional perimeter-based security frameworks prove inadequate in environments characterized by decentralized endpoints and continuous data exchange. Intelligent, adaptive, and context-aware protection mechanisms therefore become fundamental components of modern financial infrastructures. The integration of AI-driven analytics with IoT-enabled transaction ecosystems provides a pathway toward proactive threat detection, automated risk mitigation, and dynamic authentication control [4]. This convergence establishes the foundation for resilient digital payment networks capable of sustaining high transaction throughput while maintaining integrity, confidentiality, and regulatory compliance across heterogeneous operational environments [5].

Artificial Intelligence introduces advanced analytical capabilities that extend beyond conventional rule-based fraud detection systems [6]. Machine learning algorithms, deep neural networks, reinforcement learning models, and graph-based analytics enable dynamic evaluation of transaction patterns, user behavior, geospatial anomalies, and device fingerprinting attributes [7]. Continuous learning mechanisms facilitate adaptation to evolving fraud tactics, synthetic identity construction, and coordinated attack strategies. Predictive risk scoring models enhance transaction validation processes by balancing security enforcement with customer experience optimization [8]. Context-aware decision engines evaluate multifactor signals in milliseconds, reducing false positives and operational friction within high-volume payment ecosystems. The emergence of explainable AI techniques strengthens transparency in automated financial decisions, addressing regulatory requirements and governance standards that demand accountability in algorithmic processing [9]. Integration of AI within distributed financial infrastructures supports intelligent orchestration of authentication intensity, adaptive credit evaluation, and anti-money laundering analytics. Intelligent automation therefore transforms digital payment environments into self-monitoring systems capable of responding to dynamic financial threats while preserving transactional efficiency and consumer trust [10].