RADemics

IoT-Enabled Fraud Detection in Smart Retail and Supply Chain Management Systems

Anmol Narayan, Kanchan Kamlesh Ingale
MTech SAU Student, Raisoni College of Engineering and Management

IoT-Enabled Fraud Detection in Smart Retail and Supply Chain Management Systems

[1]Anmol Narayan, BTech KIIT, MTech SAU Student, New Delhi, Delhi India. anmol.narayan32@gmail.com

[2]Kanchan Kamlesh Ingale, Assistant professor, Electronics and Telecommunication, G H Raisoni College of Engineering and Management Nagpur Maharashtra India. kanchanbawane1994@gmail.com

Abstract

The rapid digital transformation of smart retail and supply chain ecosystems through Internet of Things (IoT) technologies has significantly enhanced operational automation, inventory visibility, customer engagement, and intelligent logistics management. Extensive deployment of interconnected devices, RFID infrastructures, wireless sensors, cloud platforms, and edge-enabled analytical systems has simultaneously increased exposure to sophisticated fraud activities, cybersecurity vulnerabilities, counterfeit product circulation, transactional manipulation, and operational data tampering across digital commerce environments. Traditional fraud detection mechanisms encounter major limitations in processing large-scale heterogeneous IoT data streams and identifying dynamic fraud patterns in real time. This book chapter presents a comprehensive analysis of IoT-enabled fraud detection frameworks for smart retail and supply chain management systems by examining the integration of artificial intelligence, machine learning, blockchain technology, predictive analytics, and edge computing within intelligent commerce architectures. Advanced analytical models for anomaly detection, risk scoring, behavioral monitoring, decentralized authentication, and secure transaction verification receive detailed investigation for strengthening operational transparency and fraud resilience across interconnected retail infrastructures. Critical challenges associated with scalability, interoperability, data integrity, cybersecurity, privacy preservation, and blockchain integration within IoT ecosystems also receive extensive discussion. Emerging technological paradigms involving federated learning, explainable artificial intelligence, digital twin systems, and autonomous security orchestration highlight future directions for intelligent fraud prevention in next-generation retail and logistics networks. The chapter provides valuable insights for researchers, academicians, industry professionals, and policymakers seeking secure, scalable, and intelligent solutions for fraud mitigation within rapidly evolving digital commerce ecosystems.

Keywords: Internet of Things (IoT), Fraud Detection, Smart Retail Systems, Supply Chain Security, Machine Learning, Blockchain Technology

Introduction

The rapid evolution of digital commerce and Industry 4.0 technologies has transformed conventional retail and supply chain management systems into highly interconnected and intelligent operational ecosystems [1]. Internet of Things (IoT) technologies have emerged as a

major driving force behind this transformation by enabling seamless communication among sensors, RFID tags, smart shelves, cloud platforms, surveillance systems, automated billing terminals, and logistics infrastructures [2]. Smart retail environments increasingly depend on connected devices and real-time analytical systems for inventory optimization, customer engagement, operational automation, and personalized service delivery [3]. Similarly, modern supply chain networks utilize IoT-enabled transportation systems, environmental monitoring sensors, warehouse automation technologies, and intelligent tracking platforms for improving logistics coordination and product visibility across global commerce ecosystems [4]. Large-scale deployment of interconnected digital infrastructures has significantly enhanced operational efficiency, reduced manual intervention, and improved data-driven decision-making processes within retail and logistics environments [5]. Continuous technological advancement within intelligent commerce ecosystems has accelerated the adoption of scalable and automated operational frameworks across global retail industries.

The growing integration of IoT technologies within smart retail and supply chain systems has simultaneously increased exposure to cybersecurity vulnerabilities, fraudulent activities, and operational risks across interconnected digital infrastructures [6]. Smart retail platforms continuously generate massive volumes of sensitive transactional records, customer information, behavioral analytics, inventory data, and logistics histories through connected operational devices and cloud-based communication systems [7]. Cybercriminals frequently target such interconnected infrastructures for conducting payment fraud, counterfeit product insertion, invoice manipulation, shipment diversion, identity theft, loyalty abuse, and unauthorized access attacks [8]. Traditional fraud detection systems relying on static rule-based monitoring approaches often fail to identify evolving fraud patterns and complex cyber threats occurring within large-scale digital commerce ecosystems [9]. Increasing sophistication of cyberattacks and operational manipulation strategies has created an urgent requirement for intelligent fraud detection frameworks capable of supporting real-time analytical processing, adaptive threat recognition, and predictive risk assessment across distributed retail and supply chain networks [10]. Secure operational coordination has therefore become a critical requirement within modern commerce infrastructures.