RADemics

Fraud Detection in Smart Cities Using IoT, AI, and Big Data Analytics

K. Suresh, M. Keerthi Priya
Hyderabad institute of Technology and Management,
Mallareddy University

Fraud Detection in Smart Cities Using IoT, AI, and Big Data Analytics

[1]K. Suresh, Associate Professor, Hyderabad institute of Technology and Management, India. sureshk.eee@hitam.org

[2]M. Keerthi Priya, Assistant professor, Department of CS & IoT, Mallareddy University, Hyderabad, India. mkeerthi.priya@mallareddyuniversity.ac.in

Abstract

Rapid expansion of smart city infrastructures has transformed urban environments through integration of Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, and Big Data Analytics across transportation systems, healthcare services, energy grids, financial platforms, and digital governance applications. Continuous data exchange among interconnected devices and intelligent communication networks has significantly improved operational efficiency and urban sustainability while simultaneously increasing exposure to sophisticated fraud activities and cyber threats. Fraudulent transactions, identity manipulation, smart meter tampering, healthcare fraud, transportation anomalies, and unauthorized digital access create serious security concerns within modern smart city ecosystems. Traditional fraud detection approaches fail to address dynamic attack patterns, heterogeneous data environments, and real-time analytical requirements associated with large-scale urban infrastructures. Intelligent fraud detection frameworks driven by AI and Big Data technologies provide advanced capabilities for anomaly detection, predictive analytics, behavioral monitoring, and automated threat recognition across distributed digital platforms. Machine learning, deep learning, edge computing, blockchain integration, and real-time streaming analytics strengthen security operations through adaptive decision-making and continuous monitoring of suspicious activities. Explainable Artificial Intelligence (XAI) further improves transparency, accountability, and reliability within automated fraud detection systems operating across critical urban infrastructures. Scalable Big Data architectures support efficient storage, distributed processing, and rapid analysis of massive datasets generated from IoT-enabled environments, enabling proactive fraud prevention and enhanced cybersecurity resilience. This chapter presents a comprehensive exploration of intelligent fraud detection mechanisms within smart city ecosystems by examining IoT-based monitoring frameworks, AI-driven analytical models, scalable Big Data architectures, transportation fraud analytics, blockchain-enabled security mechanisms, and emerging research challenges associated with privacy preservation, interoperability, and ethical AI implementation. The proposed discussion contributes toward development of secure, adaptive, and resilient fraud prevention frameworks capable of supporting sustainable digital transformation and trustworthy urban governance within future smart cities.

Keywords: Smart Cities, Fraud Detection, Internet of Things (IoT), Artificial Intelligence, Big Data Analytics, Cybersecurity.

Introduction

Rapid urbanization and continuous advancements in digital technologies have accelerated transformation of conventional cities into highly interconnected smart city ecosystems [1]. Smart cities utilize Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, wireless communication technologies, and Big Data Analytics to improve operational efficiency, urban sustainability, resource management, transportation systems, healthcare services, and governance infrastructures [2]. Intelligent sensors, smart meters, surveillance systems, wearable devices, and communication platforms continuously generate enormous volumes of real-time data across urban environments. Such technologies support automated decision-making, predictive monitoring, and intelligent service delivery for modern societies [3]. Increasing dependence on interconnected digital infrastructures has also expanded opportunities for cybercriminals to exploit vulnerabilities within smart city networks [4]. Fraudulent activities targeting financial systems, healthcare applications, transportation platforms, energy grids, and digital governance infrastructures create serious challenges for urban security management [5]. Advanced fraud prevention frameworks therefore play a critical role in ensuring reliability, transparency, and secure digital transformation within future smart city ecosystems.

Internet of Things technologies form the foundation of smart city infrastructures by enabling communication among interconnected devices, sensors, communication gateways, and cloud-based analytical systems [6]. Continuous data collection from transportation systems, healthcare networks, public surveillance platforms, and utility management infrastructures strengthens operational intelligence and service optimization within urban environments [7]. Large-scale IoT deployments also introduce multiple attack surfaces vulnerable to cyber intrusions, unauthorized access, identity manipulation, and data tampering activities [8]. Traditional fraud detection approaches based on static rules and signature-based mechanisms fail to identify evolving attack patterns operating within dynamic smart city ecosystems [9]. Rapid growth in connected devices and real-time communication networks increases complexity in monitoring suspicious activities across heterogeneous urban infrastructures. Intelligent IoT-based fraud detection frameworks support continuous observation of operational behavior, network traffic, and transactional activities for identifying anomalies and preventing malicious actions before significant disruption occurs within critical urban services and communication environments [10].