Chapter 11
Artificial Intelligence–Enabled Cybersecurity and Internet of Things Applications in Smart Cities

Wasswa Shafik
https://orcid.org/0000-0002-9320-3186
Dig Connectivity Research Laboratory (DCRLab), Kampala, Uganda & School of Digital Science, Universiti Brunei Darussalam, Brunei

ABSTRACT

The rapid adoption of Smart Cities (SCs) has increased reliance on AI-based IoT technologies to enhance smart infrastructure and services, contributing to the UN's sustainable development goals. However, this integration brings significant cybersecurity (CS) challenges, such as DDoS, MITM, phishing, and ransomware attacks. This chapter underscores the importance of CS in SCs, highlighting vulnerabilities and risks. It examines IoT's role in SC infrastructure and services, AI's impact on SC efficiency, and various AI techniques used in SC applications. The chapter analyzes cyberattacks on SC infrastructure, suggesting CS measures like protocols, encryption, authentication techniques, access control, and incident response. AI and IoT integration enhances CS, reducing cyber threats through anomaly detection and real-time data collection for AI-based security solutions. The chapter also presents SC application case studies demonstrating the integration's effectiveness and best practices. It concludes by emphasizing the need for continued research and innovation in SC cybersecurity.

DOI: 10.4018/979-8-3693-8029-1.ch011

1. INTRODUCTION

Smart cities[1] (SCs) have increased substantial fraction in urban development because of their integration with technological advancements such as artificial intelligence[2] (AI), information and communication technologies[3], and the Internet of Things (IoT). Several cities globally are embracing the potential of SC initiatives to improve the life quality of their residents, optimize resource utilization, and improve sustainability[4]. At the core of this transformative shift lies the seamless integration of two enabling technologies, explicitly, AI and IoT (Bilali et al., 2022). Traditionally, SCs are urban areas that utilize digital technologies, data analytics, and internet connectivity to boost their infrastructure and services' livability, effectiveness, and efficiency (Alaali et al., 2022). These cities employ an inclusive tactic for urban growth, considering smart energy[5], waste management, transportation, healthcare, and public safety. This integration allows SCs to seamlessly interact with devices such as sensor systems and transform traditional urban environments into interconnected and intelligent ecosystems (Rajasekar et al., 2022).

The growing significance of SCs stems from their capacity to address the myriad challenges of quickly urbanizing areas. As the global population becomes progressively concentrated in urban areas, cities are confronted with the need to manage limited resources, ease traffic bottlenecks, offer efficient and reliable public facilities, and ensure the well-being and safety of its citizens (Alotaibi & Barnawi, 2023). SC initiatives offer a promising solution by connecting these enabling technologies to automate processes, optimize resource allocation, data-driven decision-making, and enhance the urban experience. AI is the SCs' backbone due to its advanced machine learning[6] (ML), analytical, and predictive capabilities. AI-driven systems can process vast amounts of data collected through IoT devices, identify cyber anomaly patterns, detections make actionable insights, and enable self-sufficient decision-making (Lupton et al., 2022). From smart traffic management to predictive maintenance of perilous infrastructure, AI aids in optimizing the operations of SCs, resulting in enhanced efficiency, cost savings, and sustainability, and technological acceptance in different aspects (Abubakari & Kalinaki, 2024).

The interconnected nature of SC ecosystems and the sheer volume of generated data makes them vulnerable to cyber-attacks and threats (Toma et al., 2022). Developing robust CS measures and strategies to protect SC systems and data integrity, confidentiality, and availability is critical. IoT devices range from daily 'things', for example, smart wearables and phones, to industrial machinery and SC infrastructure (Ahmadi-Assalemi et al., 2022; Gul et al., 2024a; Gul et al., 2024b). With connectivity and sensing capabilities, IoT devices avail vast massive data that can be analyzed for valuable insights (Dhanaraj et al., 2022). IoT systems aim for interoperability, allowing devices from diverse manufacturers to communicate and operate together