Chapter 5
Cybersecurity at the Edge:
Defending Decentralized Cities in a Borderless Threat Landscape

Fadi Bata
https://orcid.org/0009-0008-3034-7693
Applied Science Private University, Jordan

Mohammad Albadareen
Hashemite University, Jordan

Bashar Khassawneh
Amman Arab University, Jordan

Mahmoud Aljawarneh
https://orcid.org/0000-0003-2003-6310
Applied Science Private University, Jordan

Qais Al-Na'amneh
Applied Science Private University, Jordan

Ayoub Alsarhan
https://orcid.org/0000-0001-9075-2828
Hashemite University, Jordan

Ahmad Saleh Alhazaimeh
King Abdaulaziz University, Saudi Arabia

ABSTRACT

The paradigm of decentralized cities, reliant on edge computing, redefines urban functionality but introduces acute cybersecurity challenges within a borderless threat environment. Traditional perimeter-based security is ill-suited for dispersed edge assets and sophisticated adversaries. This chapter critically examines these challenges, dissects threat vectors, and proposes adaptive defense mechanisms. Through simulation-based evaluation over multiple replications (N=5), we demonstrate the efficacy of a combined defense strategy (Basic Firewall and AI-driven IDS) against defined attack scenarios. Averaged results show substantial improvements in threat

DOI: 10.4018/979-8-3373-4455-3.ch005

detection (e.g., F1-Score increased from 0.0000 to 0.8876 ± 0.0150) and mitigation compared to a baseline, alongside a quantified analysis of performance overhead and consistently immediate Time-to-Detect (TTD). The work provides foundational insights, robust quantitative validation, and strategic foresight, emphasizing proactive postures essential for safeguarding future decentralized smart cities.

1 INTRODUCTION

Unprecedented urbanization exerts immense pressure on municipal infrastructures, compelling a pivot towards technologically infused smart cities to manage resources and enhance citizen well-being (Masoumi & van Genderen, 2024). These digitally interwoven urban environments leverage IoT (Al-Na'amneh et al., 2024), AI (Aljaidi et al., 2023), and advanced networks to optimize services like transport, energy, and healthcare, forming vast cyber-physical systems (Al-Na'amneh et al., 2024) critical to urban function (Han & Kim, 2024). Two converging trends now redefine this landscape: the decentralization of services and the proliferation of edge computing (Satyanarayanan, 2017). Decentralization fosters resilience and local autonomy by distributing control away from monolithic centers, while edge computing brings processing closer to data sources, minimizing latency and enabling real-time, context-aware responses crucial for agile urban services (Veeramachaneni, 2025).

This confluence of decentralization and edge computing (Al-Na'amneh, 2025), however, fundamentally reshapes the cybersecurity posture, creating complex challenges that legacy security models cannot address (Liu et al., 2020; Yan, Zhao, Liu, & Luo, 2024). Cybersecurity models predicated on well-defined network perimeters (Jaradat, Nasayreh, Al-Na'amneh, Gharaibeh, & Al Mamlook, 2023), centralized security operations centers (SOCs), and signature-based detection of known threats struggle to adapt to these highly distributed, heterogeneous, dynamic, and often resource-constrained environments. The attack surface expands exponentially, with every edge node becoming a potential vulnerability, making the entire urban sociotechnical system dependent on its weakest, often physically accessible, components (G. He, Li, Shu, & Luo, 2024; Neshenko, Bou-Harb, Crichigno, Kaddoum, & Ghani, 2019). This systemic vulnerability is magnified by a borderless threat landscape where sophisticated adversaries operate globally, exploiting seams in distributed architectures with evolving Tactics, Techniques, and Procedures (TTPs) (World Economic Forum, 2021; Saha et al., 2025). A successful cyberattack on a decentralized city's critical infrastructure could trigger catastrophic consequences for economic stability, public safety, and citizen trust (Demertzi, Demertzis, & Demertzis, 2023; Achaal, Adda, Berger, Ibrahim, & Awde, 2024).