Chapter 2
Adaptive AI Models for Real-Time Data Mobility and Security in Urban IoT Networks

Raj Kishor Verma
http://orcid.org/0009-0005-7216-7752
ABES Institute of Technology, India

Raj Kishor Verma
http://orcid.org/0009-0009-9645-718X
Galgotias University, India

ABSTRACT

Abstract Intelligent and contextual decisions at the network edge are opening up exciting new possibilities in real-time data movement as well as urban IoT network safe. Diverse machine learning techniques are deployed in these models which are constantly evolving. They enable the live processing and analysis of data streams from a wide variety of IoT sensors located in an urban environment: this also facilitates adaptation to the rapidly changing conditions surrounding us as well as adapting itself quickly to widely different application needs. The collaborative deployment of large AI models (LAMs) throughout edge devices allows the system to learn across multiple modalities and scenarios. In this way, it increases scalability for smart urban services. Thus, adaptive AI frameworks not only fuse in stringent security measures such as anomaly detection and federated learning but also satisfy the requirements for real-time threat identification as well as data privacy protection under resource-constrained conditions in dynamic networks.

DOI: 10.4018/979-8-3373-4202-3.ch002

1. INTRODUCTION

The fast development of Internet of Things (IoT) devices in the urban setting has completely transformed the entire idea of smart cities, where it is now possible to keep track of, streamline and automate real-time on the most vital of the areas: transportation, energy, safety of the population, and utilization of limited resources (Reis, 2025). Although the urban IoT networks produce large streams of data flows that are heterogenous, dynamic and massive in size, the pressing issue at hand is now to be addressed on how to push the data out in an efficient manner and within appropriate physical and programmatic protection. Conventional AI designs, more likely to be founded on fixed data sets and fixed regulations, are struggling to keep up with the dynamic environments and threats to security that characterize modern city infrastructures (Nikitas et al., 2020). The adaptive AI models are a game changer to these challenges. They also learn on the spot and make decisions on the fly, and engage in self-optimization at all times. These unconventional types of AI are able to process and analyze the flows of distributed urban IoT nodes and adjust their behavior according to the variations in network conditions, user needs, the emergence of threats to security or whichever. Federated learning and edge computing are the means to have deep reinforcement learning and provide quick and decentralized answers where privacy of data is ensured and low latency requirement is not violated. Upon integration of adaptive AI in urban IoT networks, mobility of data and security are improved. There are AI-based methods of data transmission routes and bandwidth management that reduce congestion and ensure that the most important information reaches the destination. In the meantime, advanced AI-based security systems (Nikitas et al., 2020; Reis, 2025) that include technologies like graph neural networks, multi-agent systems, and neuro-symbolic reasoning, among others, do such critical tasks as threat anticipation, anomalies, biasing defenses in a way that they can be maintained: securing lives in a way that is specially sensitive to the special vulnerabilities of IOT ecosystems. In conclusion, adaptive AI models play a significant role in ensuring that data, in urban IoT networks, or anywhere else, is secure and available (Hamza & Ullah, 2025; Mutambik, 2025). These smart systems offer a foundation of a strong, extendible, and dependable smart city infrastructure by constantly learning through the actual world and adapting to fit the emerging conditions (Gheorghe & Soica, 2025).

1.1 Adaptive AI

The Adaptive AI is a new form of artificial intelligence which is capable of changing in real-time depending on the incoming inputs, goals or surroundings. Contrary to the traditional AI which is trained on fixed models based on past