RADemics

Fundamentals of IoT Architectures and AI Frameworks for Scalable Smart City Infrastructure Development

Sheetal sharma, Durairaji V, Shunmuga Sankari M
FPM scholar Dr. Dy Patil B. School, St. Joseph's College of Engineering, TJS Engineering College

Fundamentals of IoT Architectures and AI Frameworks for Scalable Smart City Infrastructure Development

[1]Sheetal sharma, FPM scholar Dr. Dy Patil B. School, Tathawade Pune. sheetalsharma1128@gmail.com

[2]Durairaji V, Assistant Professor, Artificial Intelligence and Data Science, St. Joseph's College of Engineering, Chennai. durairaji1984@gmail.com

[3]Shunmuga Sankari M, Assistant Professor, EEE, TJS Engineering College, Peruvoyal, Gummidipoondi Taluk. shankusaran@gmail.com

Abstract

The rapid expansion of Internet of Things (IoT) technologies has significantly transformed the infrastructure of smart cities, demanding robust, scalable, and secure architectures for effective interoperability and management. This book chapter explores the fundamental concepts of IoT architectures and AI frameworks that underpin scalable smart city infrastructure development. The integration of edge-native service meshes, trust frameworks, and context-aware reasoning engines is emphasized as essential to overcoming the challenges of device interoperability, lifecycle management, and real-time data processing. With a focus on security, the role of trustworthy middleware incorporating Trusted Platform Modules (TPM) and Hardware Root-of-Trust (RoT) is discussed to ensure data integrity and device authentication. The chapter investigates the application of semantic modeling and ontologies, specifically Resource Description Framework (RDF) and Web Ontology Language (OWL), in creating intelligent, context-aware systems. By addressing key issues in device integration, security, and decentralized management, the chapter provides comprehensive insights into the technologies shaping the future of IoT-powered smart cities.

Keywords: IoT Architectures, AI Frameworks, Smart City Infrastructure, Edge-Native Service Mesh, Trusted Platform Module (TPM), Semantic Modeling.

Introduction

The Internet of Things (IoT) has emerged as one of the most transformative technological advancements of the 21st century, particularly in the context of smart city infrastructure [1]. Smart cities leverage a variety of IoT-enabled devices and systems to enhance the quality of life for urban residents, improve sustainability, and optimize resource management [2]. With the proliferation of connected devices, the need for scalable, efficient, and secure IoT architectures becomes more critical [3]. These architectures must be capable of managing diverse devices, handling large volumes of data, and ensuring seamless interoperability between different systems and components [4]. As urbanization continues to accelerate, understanding the foundational elements

of IoT architectures and AI frameworks for smart cities is essential for designing the next generation of urban infrastructures [5].

At the core of any scalable IoT architecture is the ability to ensure seamless integration and interoperability between a wide range of devices and technologies [6]. The heterogeneous nature of IoT devices, often spanning across various communication protocols and hardware platforms, presents significant challenges in creating a unified ecosystem [7]. Middleware platforms and abstraction layers play a critical role in bridging these gaps by providing a common interface for devices, enabling seamless communication and data exchange [8]. These platforms must also support dynamic and scalable device management to accommodate the frequent changes in device configurations, usage patterns, and network conditions in a smart city environment [9].

In interoperability, security is one of the most pressing concerns when designing IoT systems for smart cities [10]. The vast number of interconnected devices increases the potential attack surfaces, making it crucial to implement robust security measures at every level of the system [11]. One such approach is the integration of trustworthy middleware that leverages Trusted Platform Modules (TPM) and Hardware Root-of-Trust (RoT) [12]. These hardware-based security mechanisms provide a foundation for secure device authentication, data encryption, and system integrity [13]. The use of TPM and RoT ensures that devices can securely communicate with one another, and their identities can be verified before any sensitive data is exchanged [14]. This is essential for maintaining trust in the system and ensuring that smart city services remain secure and resilient against cyber threats [15].