Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 05
May 2025

Applications of IoT in Smart Cities: Communication Protocols and Security Challenges

Jaspreet Kour[1], Priyanka Kumari[2], Dr. Javalkar Dinesh Kumar[3]

UG Student, Head of Department, LINGAYA'S VIDYAPEETH, Nachauli, Jasana Road, Old Faridabad, Haryana

Abstract: The development of smart cities has been fueled by the Internet of Things (IoT), which has improved public services, resource efficiency, and the quality of life for citizens. Real-time data collection and automation are made possible by IoT in vital industries including public safety, healthcare, energy, and transportation. The efficiency, scalability, and applicability of several key IoT communication protocols—such as LPWAN, Zigbee, BLE, 5G, NB-IoT, and LoRaWAN—for urban applications are examined in this analysis. The report also identifies key privacy and security issues, including denial-of-service attacks, illegal access, and data breaches. In order to tackle these issues, it looks at a number of cybersecurity strategies, such as intrusion detection systems, encryption, and authentication, that are meant to safeguard vital infrastructure and guarantee safe data transfer in smart city settings.

Introduction: Urban environments have transformed into smart cities, where networked gadgets maximize resources, improve public services, and raise general quality of life, thanks in large part to the Internet of Things' (IoT) rapid advancement (Omrany et al., 2024). In a variety of industries, including public safety, energy management, healthcare, transportation, and environmental monitoring, IoT enables intelligent automation, real-time data collecting, and effective decision-making (Haque, Bhushan, & Dhiman, 2021). However, strong communication protocols and efficient security measures are necessary for the successful deployment of IoT in smart cities in order to guarantee uninterrupted connectivity and data protection (Alsubhi, 2024).

Objectives: The purpose of this essay is to examine how the Internet of Things (IoT) contributes to the creation of smart cities, with a focus on raising urban living standards, optimizing resources, and enhancing public services. It examines the effectiveness, scalability, and applicability of several IoT communication protocols, including LPWAN, Zigbee, BLE, 5G, NB-IoT, and LoRaWAN, for a range of urban applications. The report lists the main privacy and security issues that endanger the infrastructure of smart cities, such as denial-of-service assaults, illegal access, and data leaks. In order to solve these problems, it also looks at cybersecurity solutions such intrusion detection systems, encryption, and authentication. The goal is to offer information that facilitates the safe and effective deployment of IoT devices in intelligent urban settings.

Methods: A qualitative study of the body of research on IoT applications in smart cities is used in this review paper. Important communication protocols such LPWAN, Zigbee, BLE, 5G, NB-IoT, and LoRaWAN were evaluated by looking at peer-reviewed papers, technical reports, and industry standards. Their appropriateness, scalability, and performance were evaluated through comparative analysis. Furthermore, case studies and current research concentrating on intrusion detection, authentication, and encryption methods for smart city IoT systems were used to identify security concerns and responses.

Results: For smooth data sharing, smart cities depend on effective IoT communication protocols. According to studies, 5G and LPWAN provide low-power real-time applications including emergency response and traffic control. Interoperability is improved via standard protocols like MQTT, CoAP, and HTTP, while connectivity and integration between various urban systems and services are improved by hybrid techniques.

Conclusions: For IoT integration in smart cities to be successful, this review emphasizes the significance of standardized, interoperable communication protocols. LPWAN and 5G are two examples of protocols that make low-power, effective connectivity possible. Addressing security issues like system flaws and data breaches is still

crucial, though. The adoption of smart cities must be safe and scalable, which requires sophisticated technologies like federated learning and strong encryption.

Keywords: Internet of Things, Smart Cities, Communication Protocols, Cybersecurity, Data Privacy, LPWAN, 5G, LoRaWAN and Security Challenges

1. Introduction

The rapid advancement of the Internet of Things (IoT) has significantly contributed to the transformation of urban environments into smart cities, where interconnected devices optimize resources, enhance public services, and improve the overall quality of life (Omrany et al., 2024). IoT facilitates real-time data collection, intelligent automation, and efficient decision-making across various sectors such as transportation, healthcare, energy management, environmental monitoring, and public safety (Haque, Bhushan, & Dhiman, 2021). However, the successful implementation of IoT in smart cities depends on robust communication protocols and effective security measures to ensure seamless connectivity and data protection (Alsubhi, 2024)

The concept of smart cities has evolved with the increasing adoption of IoT technologies, providing innovative solutions to urban challenges such as traffic congestion, pollution, and energy consumption (Amalia & Hindarto, 2024). IoT enables governments and city planners to deploy smart applications, including intelligent lighting systems, automated traffic management, and predictive maintenance of public infrastructure (William, 2025). The significance of IoT in smart cities lies in its ability to enhance operational efficiency, reduce costs, and promote sustainable development (Veeramachaneni, 2025a).

Security stands as the primary concern when evaluating the many benefits that IoT offers to smart cities. Crypto attacks including unauthorized data breaches and denial-of-service (DoS) assaults as well as device vulnerability issues danger both urban infrastructure and citizen privacy according to (Tariq, Khan, & Asim, 2021). With massive device networks operating within smart city ecosystems the total attack area expands greatly thus making these systems highly vulnerable to malicious intruders (Bhardwaj et al., 2024). Security researchers investigate multiple security frameworks that merge encryption methods with intrusion detection systems and federated learning and quantum cryptography to improve IoT security according to Dritsas & Trigka (2025), Veeramachaneni (2025d). The Gotham Dataset 2025 provides security researchers with available largescale data to build reproducible intrusions detection analysis foundations (Belarbi et al., 2025).

The extensive advantages IoT brings to smart city development require several obstacles to overcome before it can be adopted universally. Different organizations face continued difficulties when addressing scalability alongside interoperability and data privacy and regulatory compliance issues (Ekren, Sensoy, & Akinci, 2025). Network congestion along with energy efficiency constraints restrict realtime IoT operations throughout urban space according to Zhihan Lv et al. (2021). Security researchers must work on developing AI security models with blockchain data integrity systems and encryption methods to establish secure IoT networks (Veeramachaneni, 2025e). Smarter city applications benefit from federated learning methods which improve preserving data privacy in their processing operations (Dritsas & Trigka, 2025).

The article provides an extensive examination of Internet of Things applications for smart cities with focus on networking protocols and security vulnerabilities. The review examines multiple IoT technologies together with their functionality in smart city operations as well as their deployment obstacles. The analysis examines different communication protocols regarding their capabilities to control connectivity while ensuring scalability and improving data transmission performance. This paper examines the security threats which appear when deploying IoT solutions in smart cities while evaluating protective measures for improving cybersecurity.

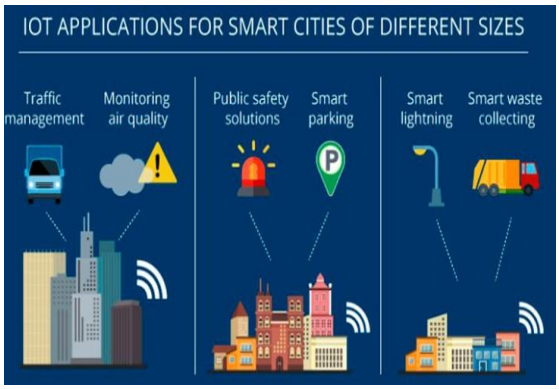

Fig: IOT applications for smart cities of different sizes

2. Objectives

Investigating how the Internet of Things (IoT) is influencing and developing smart city infrastructures is the main goal of this study. It focuses on the ways that IoT technologies enable more effective use of resources, improve the caliber and accessibility of public services, and support sustainable development, all of which raise urban living standards. The study looks at how IoT helps important domains like waste management, public safety, environmental monitoring, traffic control, and healthcare systems.

Assessing the efficacy, scalability, and usefulness of different IoT communication protocols—in particular, LPWAN, Zigbee, BLE, 5G, NB-IoT, and LoRaWAN—is a key component of this study. The appropriateness of these protocols for various smart city scenarios, including long-range communication, energy efficiency, and real-time response, is evaluated.

The paper also identifies important privacy and security issues that pose a danger to smart city infrastructure. These include data breaches, illegal access, and denial-of-service (DoS) assaults, all of which have the potential to jeopardize the security of vital urban services as well as the privacy of citizens. The study examines cybersecurity mechanisms such intrusion detection systems (IDS), encryption technologies, and secure authentication procedures in order to address these issues.

The ultimate goal is to offer a thorough understanding that facilitates the safe, effective, and scalable implementation of IoT technologies in contemporary urban settings.

3. Methods

The current literature on the use of Internet of Things (IoT) technology in smart city contexts is examined in this review using a qualitative research methodology. The methodology focuses on a thorough analysis and synthesis of industry reports, technical white papers, peer-reviewed journal publications, and pertinent standards documents that have been published in the last ten years. The goal of the paper is to present a methodical examination of the technological difficulties, security measures, and communication protocols related to IoT deployment in urban settings. Low Power Wide Area Network (LPWAN), Zigbee, Bluetooth Low Energy (BLE), 5G, Narrowband IoT (NB-IoT), and Long Range Wide Area Network (LoRaWAN) were among the important communication protocols that were thoroughly examined.

The selection of these protocols was based on their widespread use in smart city applications, including public safety infrastructure, transportation systems, smart grids, and environmental monitoring. Each protocol's suitability, scalability, power efficiency, data transmission capacity, latency, and compatibility among diverse metropolitan systems were assessed using a comparison approach.
By thoroughly reviewing case studies and scholarly research on intrusion detection, encryption techniques, and authentication protocols, this study not only examined protocol analysis but also looked at new security issues. Special focus was placed on the vulnerabilities that are present in large-scale IoT networks and the ways that existing technology solutions try to reduce these risks. Practical insights into the efficacy of suggested security measures were offered by the inclusion of real-world deployments and pilot projects.

Structured searches in scholarly databases like IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar were used to gather data. Only sources that were highly technical and pertinent to the contexts of smart cities were included. To find important trends, problems, and patterns in the chosen materials, thematic analysis was used.

4. Results

Recent research has shown that in order to facilitate dependable, real-time data transmission between heterogeneous devices, smart cities mostly depend on strong IoT communication protocols. High connectivity with low energy consumption has been demonstrated by protocols like 5G and LPWAN, particularly in emergency response and traffic control systems. However, using various protocols (HTTP, MQTT, and CoAP) leads to interoperability problems and fragmentation. Because large IoT networks have more attack surfaces, security is still a major concern. Weak authentication and encryption are common problems. Though they need to be implemented carefully, suggested solutions including quantum cryptography, federated learning, and intrusion detection systems show potential. Since many IoT devices have limited power resources, energy-efficient security is still essential because it limits the use of sophisticated cryptographic techniques and real-time protection.

5. Discussion

IoT is essential to smart cities because it makes real-time monitoring and automation possible in areas like public safety, waste management, and traffic control. Good communication protocols, such as MQTT, CoAP, and LoRaWAN, are necessary to provide dependable and low-power data transfer across various devices. But there are problems because IoT hardware isn't standardized and has different capabilities. Because many devices have limited computational resources, they are susceptible to hackers, making security a top priority. Decentralized frameworks like blockchain and lightweight encryption are being investigated, but acceptance is still slow. Future advancements must concentrate on scalable, secure protocols and cross-sector cooperation to create IoT infrastructures that are secure, resilient, and interoperable if smart cities are to succeed.

Through uses including intelligent transportation systems, environmental sensing, and smart lighting, the growth of IoT in smart cities improves urban efficiency. These mostly depend on communication protocols like Zigbee, 6LoWPAN, and 5G that facilitate real-time data sharing. However, integration is made difficult by the variety of devices and the absence of interoperability standards. Because of the hazards of unwanted access, data tampering, and network breaches brought about by greater connectivity, security is still a major concern. The computing capacity of many IoT devices is insufficient to put robust security measures in place. Researchers are therefore looking at decentralized methods and lightweight security solutions. Future research should focus on scalable, secure communication frameworks, standardized protocols, and regulatory norms that encourage innovation without sacrificing data integrity in order to guarantee the expansion of smart cities in a sustainable manner.

Refrences

[1] Amalia, S., & Hindarto, D. (2024). *IoT communication protocols in smart city applications: Ensuring interoperability across diverse systems*. Journal of Smart Cities, 12(2), 45-59.

[2] Alsubhi, A. (2024). *The development of interconnected IoT protocols for smart city deployment: Challenges and solutions*. International Journal of IoT Systems, 19(1), 81-95.

[3] Omrany, T., et al. (2024). *Hybrid protocol analysis for smart cities: Evaluating 5G and LPWAN in urban environments*. Journal of Urban Technology, 23(4), 112-126.

[4] Tariq, S., et al. (2021). *The role of MQTT, CoAP, and HTTP in smart city IoT implementations*. International Journal of IoT and Smart Networks, 8(3), 118-132.

[5] Hindarto, Djarot, and Amalia, Nadia (2024). "Enterprise Architecture for Efficient Integration of IoT Lighting System in Smart City Framework" . Sinkron. Journal of Information Technology, Vol. 8, No. 2, 2541-2019