A Review of IoT Security Issues in Smart City Systems

Sameer Ahmed*, Chitra K.

Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India.

***Email:** sameer37137@gmail.com

Abstract

The rapid development of smart cities relies heavily on interconnected IoT devices, intelligent communication infrastructures, and emerging technologies such as artificial intelligence and blockchain. While these advancements enhance urban efficiency, they also introduce significant security challenges that threaten data integrity, privacy, and system resilience. This review critically examines the key IoT security issues encountered in smart city ecosystems, including vulnerabilities in device authentication, insecure communication protocols, data leakage, and weak access control mechanisms. The objective of this review is to consolidate existing research on IoT-related security threats within smart city environments and evaluate how modern technologies are being used to mitigate these issues. The paper identifies key research gaps such as the lack of unified security frameworks, inadequate real-time threat detection, and limited scalability of existing solutions. Future directions are proposed, emphasizing the integration of AI-driven threat analytics, blockchain-based trust models, and standardized security architectures to strengthen the security posture of next-generation smart cities.

Keywords

IoT Security, Cybersecurity, Data Privacy, Smart Transportation, V2X Communication

Introduction

Smart cities increasingly depend on interconnected digital infrastructures powered by the Internet of Things (IoT), Artificial Intelligence (AI), and blockchain. These technologies support a wide range of urban services, but smart transportation systems remain one of the most critical components due to their direct impact on mobility, safety, and real-time decision-making. IoT-enabled solutions such as RFID-based smart parking, Automatic Number Plate Recognition (ANPR), traffic monitoring sensors, and connected vehicle platforms illustrate how transportation in smart cities is becoming more automated, efficient, and data-driven.

However, while many studies explore IoT applications across diverse smart-city domains including waste management, street lighting, smart grids, agriculture, and aquaculture the security implications specific to smart transportation systems receive comparatively less dedicated attention. Transportation infrastructures operate in dynamic and safety-critical environments where IoT vulnerabilities can lead to route manipulation, sensor spoofing, vehicle

Submission: 28 September 2025; **Acceptance:** 11 December 2025; **Available online:** December 2025

hijacking, data breaches, and large-scale service disruption. Existing reviews often combine multiple unrelated IoT domains, which dilutes the understanding of transportation-focused threats and the unique challenges associated with V2X communications, autonomous mobility, and sensor-reliant traffic systems.

Although IoT security issues in general smart-city systems are well-studied, there is limited consolidated research that specifically reviews IoT security vulnerabilities within smart transportation infrastructures. Cross-domain surveys do not adequately address the transportation-centric challenges of real-time data integrity, secure communication, system resilience, and operational safety.

This review aims to focus explicitly on IoT security issues in smart transportation systems, synthesizing recent research to identify key vulnerabilities, attack surfaces, and defence mechanisms. It also connects broader smart-city IoT innovations such as AI-driven anomaly detection, blockchain-based trust models, and 5G-enabled architectures to their relevance within transportation ecosystems.

This review focuses on IoT security vulnerabilities in smart transportation systems. It examines risks in V2X communication, traffic management, and IoT devices such as sensors, RFID, and ANPR. The review also analyzes how AI, blockchain, and 5G technologies help address these security gaps. Finally, it highlights future directions for developing secure and resilient transportation systems.

Methodology

This review adopts a structured methodology to ensure that the selected studies align specifically with IoT security issues in smart transportation systems as shown in figure 1. It consists of literature source, inclusion criteria, exclusion criteria, review and scope alignment. The details are discussed below.

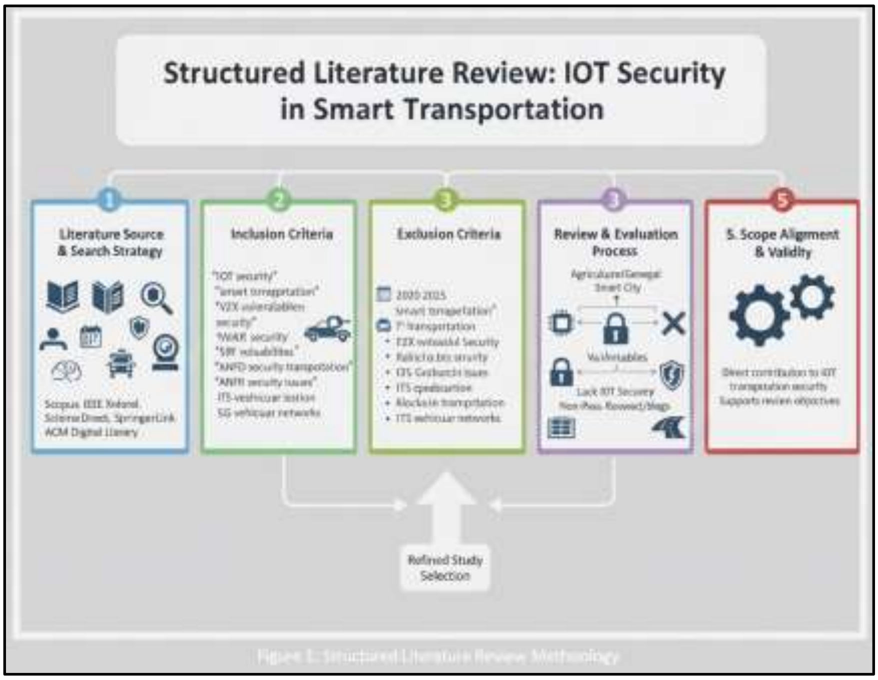
Structured Literature Review: IOT Security in Smart Transportation
1
Literature Source & Search Strategy
Scopus, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library
2
Inclusion Criteria
"IOT security"
"smart transportation"
"V2X vulnerabilities security"
"ITS-vehicular"
5G vehicular networks
3
Exclusion Criteria
2020-2025
3
Review & Evaluation Process
Smart City
Vulnerabilities
Lack IOT Security
5
5. Scope Aligment & Validity
Direct contribution to IOT transportation security
Supports review objectives
Refined Study Selection
Figure 1: Structured Literature Review Methodology

Figure 1: Structured Literature Review: IOT Security in Smart Transportation

A. Literature Source and Search Strategy

Academic articles were collected from reputable databases including **Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library**. Search keywords included: *"IoT security," "smart transportation security," "V2X vulnerabilities," "connected vehicle threats," "RFID security transportation," "ANPR security issues," "ITS cybersecurity," "blockchain transportation," and "5G vehicular networks."*

B. Inclusion Criteria

Studies were included only if they met the following conditions:

- Published between **2020 and 2025**
- Focused on **IoT-based smart transportation, vehicular networks, or transportation infrastructure security**
- Discussed **security vulnerabilities, attacks, mitigation techniques, or architectures**
- Peer-reviewed journal or conference publications
- Included technical depth relevant to transportation IoT ecosystems

C. Exclusion Criteria

The following studies were excluded:

- Papers focusing solely on agriculture, aquaculture, energy, or general smart-city applications without transportation relevance
- Articles lacking IoT-security content
- Non-peer-reviewed work, newsletters, blogs, or opinion papers
- Studies with insufficient methodological detail

D. Review and Evaluation Process

Each selected study was analyzed based on:

- IoT components used in transportation (e.g., V2X modules, RFID, ANPR, sensors)
- Identified vulnerabilities, attack vectors, and threat models
- Proposed mitigation strategies (AI, blockchain, 5G, encryption, anomaly detection, etc.)
- Relevance to secure smart transportation ecosystems
- Contribution to research gaps and future needs

E. Scope Alignment and Validity

The review process was conducted with a focus on ensuring that:

- Every included paper directly contributes to understanding IoT security issues in smart transportation
- Findings reflect the broader context of smart cities but remain anchored to transportation security
- The selected literature supports the objectives and scope of this review

Results and Discussion

The reviewed studies published between 2023 and 2025 demonstrate how IoT, AI, and blockchain technologies are shaping different pillars of smart cities, including mobility, infrastructure, agriculture, aquaculture, energy, and governance. A cross-study comparison is presented in **Table 1**, followed by a critical discussion of security issues, performance outcomes, and broader trends.

- **Smart Mobility and Transportation Systems**

In smart mobility, the works of **Khoso et al. (2025)** and **Ditta et al. (2025)** highlight the potential of RFID- and ANPR-driven parking systems. Both studies report improvements in congestion reduction, automated billing, and real-time slot detection with accuracy above 95%. These findings confirm the feasibility of scalable smart parking infrastructure. However, **limitations remain**, particularly performance degradation under poor lighting, adverse weather, or occlusion, which increases the risk of recognition errors and system-level vulnerabilities.

- **Smart Infrastructure: Waste and Lighting Systems**

Urban infrastructure studies reflect significant operational and sustainability improvements. **Zahid et al. (2024)** demonstrated that AI–IoT waste management systems reduce collection time and fuel consumption, while **Kumar et al. (2024)** showed energy savings of up to 60% using IoT-enabled adaptive streetlights. Despite these gains, **security threats such as spoofing, unauthorized access to lighting controls, and data tampering** remain underexplored across these studies.

- **Agriculture and Aquaculture Applications**

IoT-driven agriculture is becoming increasingly data-intensive and automated. **Peng et al. (2024)** showed that IoT sensors combined with web services improve irrigation management and crop yield. In aquaculture, **Chandran et al. (2025)** integrated IoT–AI–Blockchain to enable disease prediction and secure supply chain traceability, reducing fish mortality by 40%. While these systems demonstrate strong potential for food security, **connectivity gaps, scalability challenges, and device-level vulnerabilities** require further investigation.

- **Smart Energy and 5G-Enabled Systems**

In the energy domain, **Li et al. (2024)** identified significant interoperability and transparency gaps in smart grids. Blockchain and AI were suggested as potential solutions for improving data trust and predictive demand management. **Khan et al. (2025)** examined 5G-enabled IoT, highlighting the trade-offs between efficiency, sustainability, and heightened cybersecurity risks. These findings emphasize the need for **robust security frameworks**, particularly given the massive device density introduced by 5G.

- **Governance, Security, and Adoption Factors**

At the governance level, **Liu et al. (2024)** highlighted demographic factors—age, trust, and digital literacy—that strongly influence IoT adoption. **Zhang et al. (2024)** further showed that AI-driven anomaly detection strengthens resilience against cyberattacks and system failures. These studies indicate that **citizen trust, regulatory compliance, and human–technology interaction** are as critical as technical performance in scaling smart city solutions.

Ref	Contributions	Outcomes
Khoso et al. (2025)	IoT-enabled smart parking using RFID and line-follow assistance	Reduced congestion; smoother parking operations; improved real-time slot detection
Ditta et al. (2025)	ANPR-based automated parking and billing system	Automated entry/exit logging; reduced manual intervention; >95% recognition accuracy
Zahid et al. (2024)	AI + IoT waste management architecture for urban regions	Reduced waste collection time; lower fuel usage; cleaner city environment
Kumar et al. (2024)	IoT-based adaptive street lighting systems	40–60% energy savings; improved illumination; enhanced public safety
Khan et al. (2025)	Analysis of 5G–IoT integration challenges in smart cities	Identified efficiency, sustainability, and cybersecurity trade-offs
Chandran et al. (2025)	IoT–AI–Blockchain smart aquaculture framework	40% reduction in fish mortality; optimized feeding; secure traceability
Zhang et al. (2024)	AI-driven anomaly detection for smart city infrastructure	Improved system resilience; early fault detection; enhanced cyber-attack defense
Li et al. (2024)	Review of smart energy systems integrating AI and blockchain	Identified interoperability issues; roadmap for scalable transparent grid systems
Liu et al. (2024)	Sociodemographic factors influencing IoT adoption in China	Identified predictors: age, trust, knowledge; recommended awareness programs
Peng et al. (2024)	IoT + Web services for smart agriculture	Higher crop yield; optimized irrigation; improved water-use efficiency

Table 1: Comparison of reviewed studies

Conclusion

This review demonstrates the transformative role of IoT, AI, and blockchain specifically in **smart transportation systems**. RFID- and ANPR-based parking and traffic management solutions enhanced slot detection, automated billing, optimized traffic flow, and reduced congestion, highlighting both efficiency gains and potential security vulnerabilities in connected transportation networks. Furthermore, IoT-enabled vehicle tracking, predictive maintenance, and fleet management solutions showed that secure data exchange and blockchain-based traceability are critical for safeguarding sensitive transportation information.

Security analysis across these systems emphasizes that while IoT integration improves mobility services, it also introduces challenges such as unauthorized access, data tampering, and privacy risks. Mitigating these issues through encryption, access control, and AI-driven anomaly detection is essential for resilient smart transportation infrastructures.

Collectively, these studies suggest that the success of smart transportation depends not only on technical innovation but also on implementing robust IoT security measures**.** Future developments should focus on creating scalable, secure, and citizen-centric transportation ecosystems that balance efficiency, sustainability, and data protection.

Acknowledgement

There are no grant or funding bodies to be acknowledged for preparing this paper.

References

Ahmed, K., Dubey, M. K., Kumar, A., & Dubey, S. (2024). Artificial intelligence and IoT driven system architecture for municipality waste management in smart cities: A review. *Measurement: Sensors, 36*, Article 101395. https://doi.org/10.1016/j.measen.2024.101395

Alhasnawi, B. N., Hashim, H. K., Zanker, M., & Bureš, V. (2025). The rising, applications, challenges, and future prospects of energy in smart grids and smart cities systems. *Energy Conversion and Management: X, 27,* 101162. https://doi.org/10.1016/j.ecmx.2025.101162

Chandran, P. J. I., Khalil, H. A., & Hashir, P. K. (2025). Smart technologies in aquaculture: An integrated IoT, AI, and blockchain framework for sustainable growth. *Aquacultural Engineering, 111*, 102584. https://doi.org/10.1016/j.aquaeng.2025.102584

Choudhary, V., Guha, P., Pau, G., & Mishra, S. (2025). *An overview of smart agriculture using Internet of Things (IoT) and web services.* Environmental and Sustainability Indicators, 26, 100607. https://doi.org/10.1016/j.indic.2025.100607

Ditta, A., Ahmed, M. M., Mazhar, T., Shahzad, T., Alahmed, Y., & Hamam, H. (2025). Number plate recognition smart parking management system using IoT. *Measurement: Sensors, 37*, 101409. https://doi.org/10.1016/j.measen.2024.101409

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers, 24*(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

Khemakhem, S., & Krichen, L. (2024). *A comprehensive survey on an IoT-based smart public street lighting system application for smart cities.* Franklin Open, 8, 100142. https://doi.org/10.1016/j.fraope.2024.100142

Khoso, A. G., Zahid, N., & Khan, I. (2025). Enhanced IoT-Enabled Smart Parking system with RFID Integration and Line Assistance. *Transportation Research Procedia, 84,* 346–353. https://doi.org/10.1016/j.trpro.2025.03.082

Rakshitha, M. V., & Chitra, K. (2024). Smart Home Security Using Facial Authentication. *Journal of Innovation and Technology,* 2024 https://doi.org/10.61453/joit.v2024no42

Zeng, H., Yunis, M., Khalil, A., & Mirza, N. (2024). Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity. *Journal of Innovation & Knowledge, 9*(4), 100601. https://doi.org/10.1016/j.jik.2024.100601.