Soft Computing Fusion with Applications

www.scfa.reapress.com

Soft. Comput. Fusion. Appl. Vol. 2, No. 1 (2025) 22–32.

Paper Type: Original Article

AI and IoT Solutions for Efficient Public Service Delivery in Smart Cities

Moitreyee Bhaduri*

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 22052999@kiit.ac.in.

Citation:

Received: 08 August 2024 *Revised: 25 September 2024* *Accepted: 03 February 2025*	Bhaduri, M. (2025). AI and IoT solutions for efficient public service delivery in smart cities. *Soft computing fusion with applications, 2*(1), 22-32.

Abstract

The objective of creating smarter cities for improved urban living involves utilizing technology to enhance public services; however, efficiently delivering these services presents a challenge. In practical terms, Artificial Intelligence (AI) and Internet of Things (IoT) offer innovative solutions such as real-time data analysis, resource optimization, and predictive capabilities to elevate the quality and responsiveness of public services. This paper examines the role of AI and IoT in key areas: traffic management, waste collection, energy distribution, and public safety within urban infrastructures. AI-powered algorithms, combined with IoT-enabled devices, facilitate the adaptive management of traffic systems based on congestion patterns. Concurrently, sensors in smart waste bins optimize collection schedules and reduce fuel expenditures. AI enhances energy management by analyzing data from IoT-connected systems to improve consumption, lower environmental impacts, and reduce costs. Moreover, AI strengthens public safety through real-time surveillance systems that identify anomalies, thereby notifying authorities of possible threats. Case studies have shown significant improvements in service efficiency, resulting in reduced traffic congestion, lower energy usage, minimized waste collection costs, and quicker emergency response times. The findings illustrate the capability of AI and IoT to streamline service provision and create sustainable, resilient urban environments. The integration of AI and IoT in smart city development has proven to be crucial for the future, offering a scalable and flexible framework to meet the evolving needs of urban populations.

Keywords: Real-time data, Resource optimization, Sustainable cities, Smart grids, Digital transformation, Urban resilience, Automated systems.

1 | Introduction

With urbanization accelerated in most parts of the world, cities nowadays are desperate to adapt towards sustainable and effective public service management. The overcrowded cities cannot serve their large population through unhygienic infrastructure, such as crowded roads, open dumping, wasteful consumption of energy sources, and unsafe living or working environments. A solution arises from smart cities through the application of technology, such as Artificial Intelligence (AI) and Internet of Things (IoT), for

Corresponding Author: 22052999@kiit.ac.in

https://doi.org/10.22105/scfa.v2i1.41

optimization in delivering services, proper allocation of resources, and responsive city environments. This is underpinned by IoT sensors embedded within different urban systems that gather real-time data, allowing AI algorithms to process data when making intelligent decisions and providing predictive analytics. This is the ecosystem whereby traffic management systems use AI and IoT to dynamically alter signals to ease congestion while allowing emergency services to come in easily. On the other hand, sensors are used inside the bins in critical waste management areas, which signal when the collection needs are rising. At the same time, AI algorithms determine the routes so that the cost of operation and the impact on the environment are reduced. AI-based systems analyze data from IoT devices to optimize energy distribution, minimize waste, and achieve sustainability goals in managing energy in smart cities. AI-based surveillance systems with predictive analytics enhance public safety by detecting unusual activities to enable faster response to potential threats.

This, despite the above benefits, shall be critical considering that it also presents some of the biggest challenges, such as cybersecurity risks, data privacy issues, and the investment needed to implement massive infrastructure roll-out, which shall be critical in high-scale take-up of AI and IoT in public service delivery. Despite more studies and successful cases showing a different future, integrating AI and IoT with urban infrastructure will change public service delivery and make cities sustainable, resilient, and citizen-centered. This paper aims to present the current status, applications, and benefits of AI and IoT solutions in smart cities and future urban space development.

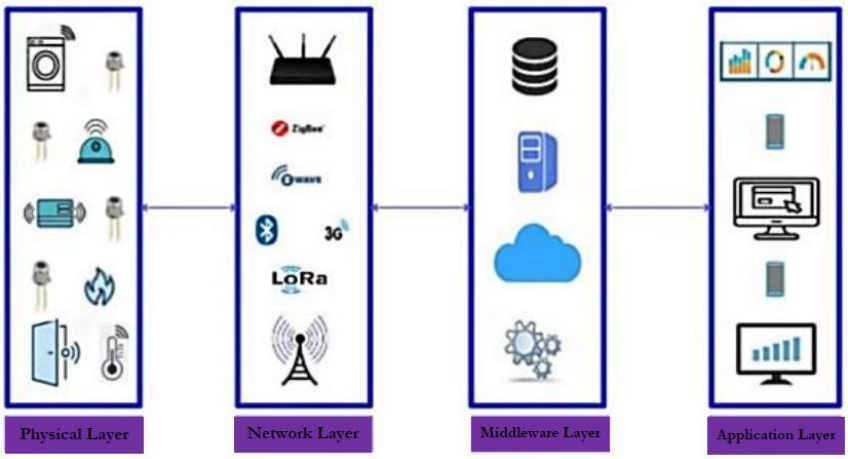

Fig. 1. Proposed layers in internet of things system.

2 | Literature Review

The integration of AI and the IoT in smart cities has recently become a buzzword since most urban centers are challenged with population growth, resource management, and public service delivery issues. The literature review provides a general overview of the studies and applications of AI and IoT solutions to improve public services in transportation, waste management, energy management, public safety, healthcare, and education.

2.1 | Transportation Services

AI and IoT technologies have been implemented comprehensively in transportation systems to address issues such as optimizing traffic management, controlling congestion, and improving movement in general. For example, Musa et al. [1] show how AI-driven adaptive control systems of traffic signals prove effective by using information derived from real-time traffic sensors that are IoT-integrated in managing traffic flow in real-time situations. Through signal time adaptation to actual traffic behavior, such systems have minimal waiting times and emissions during operations. Similarly, according to Lee et al. [2], smart parking solutions utilize IoT sensors to monitor the availability of parking spaces and assist drivers in finding available parking spots, thus reducing the time spent searching for parking.

2.2 | Public Safety

AI and IoT greatly augment smart cities' public safety and emergency response capabilities. As Wang et al. [3] have shown, AI-based analytics enable surveillance systems to detect abnormal behaviors and send alerts to the police. IoT devices, including environment sensors, can provide real-time data for air quality, noise pollution, and other factors that impact public health and safety. These integrated technologies can be proactive measures such as emergency services being deployed in cases of critical incidents better, according to Faggiano et al. [4].

3 | Traffic Management

As urban populations grow, cities face increasing challenges in managing traffic congestion, leading to delays, increased emissions, and decreased quality of life. Integrating AI and the IoT presents innovative solutions for traffic management in smart cities. By leveraging real-time data from connected devices and advanced algorithms, these technologies can optimize traffic flow, enhance safety, and improve overall mobility in urban environments [5].

AI can analyze traffic data from IoT sensors, CCTV cameras, and connected vehicles to optimize traffic signals, reduce congestion, and predict traffic patterns. This leads to smoother traffic flow, less pollution, and quicker emergency response times.

IoT sensors embedded in parking spaces can notify drivers of available spots via mobile apps, reducing time spent searching for parking [6].

3.1 | Internet of Things Technologies in Transportation

IoT applications in transportation involve an interconnected network of devices and systems, such as sensors, actuators, analytics platforms, and cloud-based solutions. Core components include [7]:

I. Sensors and GPS: These devices collect data on vehicle location, traffic patterns, and environmental factors.

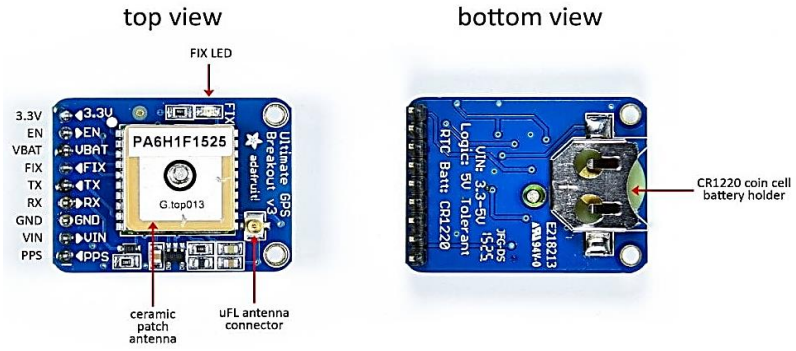

Fig. 2. Key components of internet of things technologies in transportation.

II. RFID and cameras: RFID tags help in tracking vehicles, while cameras monitor congestion, supporting effective traffic management.

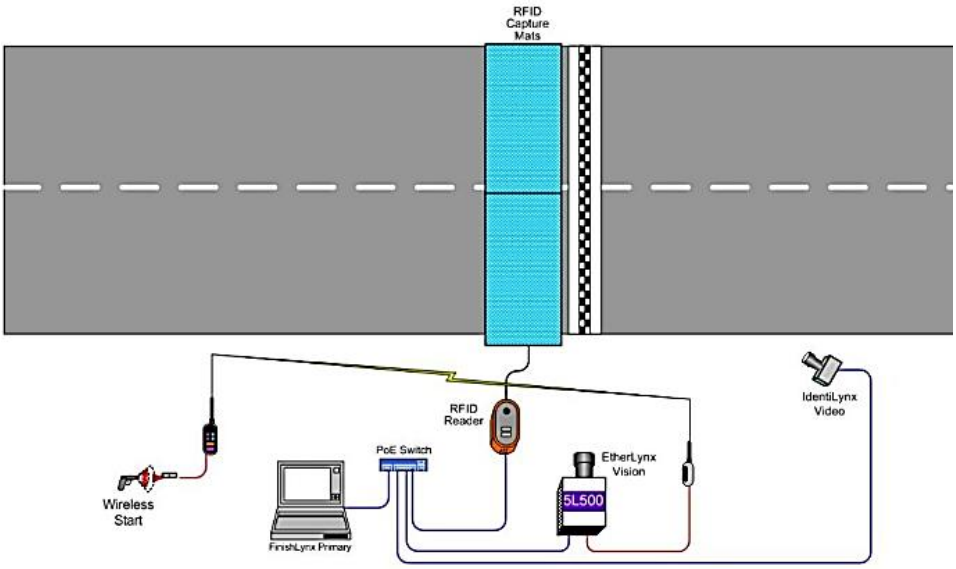

Fig. 3. Sample road race system combines chip timing with a photo-finish camera and video camera.

III. Communication protocols: Technologies like 5G, Wi-Fi, Zigbee, and Dedicated Short-Range Communication (DSRC) allow for real-time data exchange between devices and central systems, ensuring high-speed, low-latency communication essential for IoT [8].

Together, these components create a framework for smart traffic management, vehicle tracking, and improved passenger safety, forming the foundation of intelligent transportation networks.

3.2|Tracking Vehicles Using Adaptive Traffic Management, Accident Alert Light and Sound and Secure Early Traffic-Related Event Detection

The Adaptive Traffic Management (ATM) system, combined with an Accident Alert Light and Sound (AALS) system and Secure Early Traffic-Related Event Detection (SEE-TREND), aims to create a safer and smarter transport system. This innovative approach has four layers to enhance traffic management and improve safety.

Application layer

It tracks the vehicles' locations, captures photographs in real time, and allows the AALS system to trigger an alarm signal to the driver if the vehicle is within a particular distance from a potential accident location.

This service layer fetches all the data, processes the data, and brings all the information together, ready for subsequent analysis. The network layer provides secured data communication. This layer uses the SEE-TREND system to transfer vehicle-related data safely.

Here, data is sent forward while preserving the critical information it contains. The sensing layer collects data from the distributed sensing devices in the whole transport network. These devices give real-time information concerning the events that keep updating while monitoring the changes to the traffic conditions and, therefore, the responses to every event.

All these four layers work together to create a safe and intelligent transport system that ensures safety and efficiency on roads.

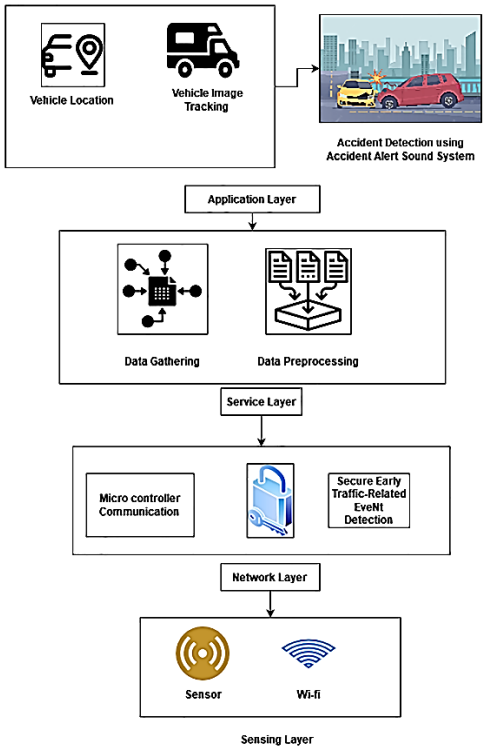

Fig. 4. Four-layered approach for adaptive traffic management, accident alert light and sound, and secure early traffic-related event detection system.

3.3 | Functioning of Adaptive Traffic Management-ALTREND System

The ATM-ALTREND system enhances route selection accuracy. The model's quality is evaluated using the test's lower limit precision level. If the proposed model successfully achieves this lower bound with the expected precision, it indicates the presence of effective pathways while eliminating less efficient communication channels. Conversely, if the lower bound exceeds the anticipated precision rate, it suggests a lack of available routes. In this case, the basic routes for efficient vehicle positioning are extended.

The functional design of the proposed module for the vehicle positioning monitoring system is shown in the figure below. First, data is collected using sensors and cameras. Data preprocessing is a vital step in the Intelligent Traffic Management (ITM) system that involves applying techniques to estimate any missing values. Once the data is captured, it is processed, and the data set is then trained using the training method. This will gather traffic information and enable a proper determination of the vehicle's position.

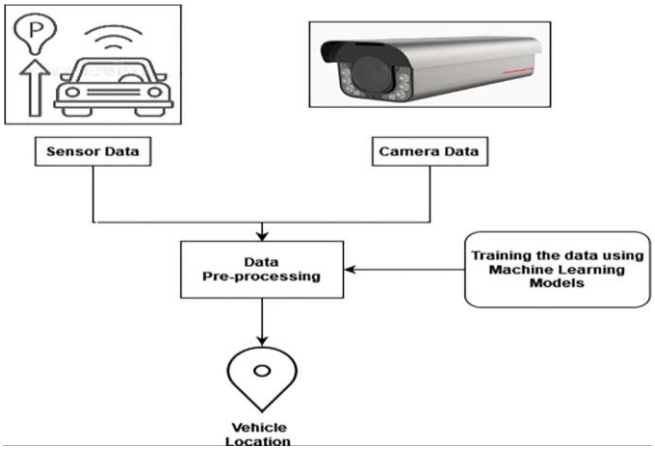

Fig. 5. Functional design of the adaptive traffic management-ALTREND vehicle positioning monitoring system.

3.4 | Feature Clustering

After plotting the locations of the moving objects, feature clustering is conducted. For this, a graph is constructed. Such a graph would involve nodes that represent feature groups concerning vehicle sightings. Connection signs between path clusters represent the edges; even for nodes, feature routes would be denoted. At any given TIi, if the cumulative sum of the estimated individual movements is large, features observed within that time interval at some FRi are followed across some frames.

The Euclidean distance, defined to some minimum value, can then be used to associate nearly all newly found features with the observed set [9].

The upper and lower limit intervals are updated along with the approximation of the distance Dist i,j between the actively monitored sets of connected features LIf i,j. The separation threshold for features is denoted as Dfseg. The following equation thus describes the properties of the connected vehicles:

$$\left[\mathrm{Max\ TI_i d_{ij}(TI_i)} - \mathrm{Min\ TI_i d_{ij}(TI_i)}\right] > \left(\mathrm{D}\left(\mathcal{A}_{\mathrm{seg}}\right)\right).$$

The graph's related aspects are then determined. Each combination of feature pathways forming a related component or vehicle observation is represented as a single entity. If an element no longer contains recorded features, the vehicle's attributes (Such as velocity vectors, centroid location, and vehicle type) are estimated after the features are removed.

4 | Public Safety

The rapid growth of IoT devices in urban areas has created a security gap. Over the years, researchers have investigated various security measures to protect IoT networks, and recently, AI has gained attention as a tool to improve IoT security. This literature review examines existing research on IoT security challenges, AI-based approaches, and their applications in urban networks [10].

4.1 | Artificial Intelligence-Enhanced Security Solutions for Urban Networks

Several studies investigated AI-based security solutions specifically tailored for urban IoT environments. Mohanty [11] discusses the applications of AI in smart city security, focusing on smart surveillance, infrastructure monitoring, and emergency procedures. AI-based solutions such as face recognition and vulnerability detection in smart projects have been applied in urban IoT networks to enhance security. The background to this is the application of identifying vulnerabilities in connected vehicles.

Fig. 6. Artificial intelligence and internet of things applications for smart city security.

4.2 | Integration of Robots and Drones

In physical security, IoT and AI technology are relieving security personnel but bringing the possibility of replacing human law enforcement with AI-powered security robots. Robotic units equipped with advanced sensors and cameras can patrol smart city streets and even prevent crimes through their presence alone. They outshine human officers in basic security tasks such as crowd control and search operations [12].

More importantly, human security waits and acts only if situations improve; however, drones can also be used for surveillance purposes to warn human security close by about the dangers posed to safety.

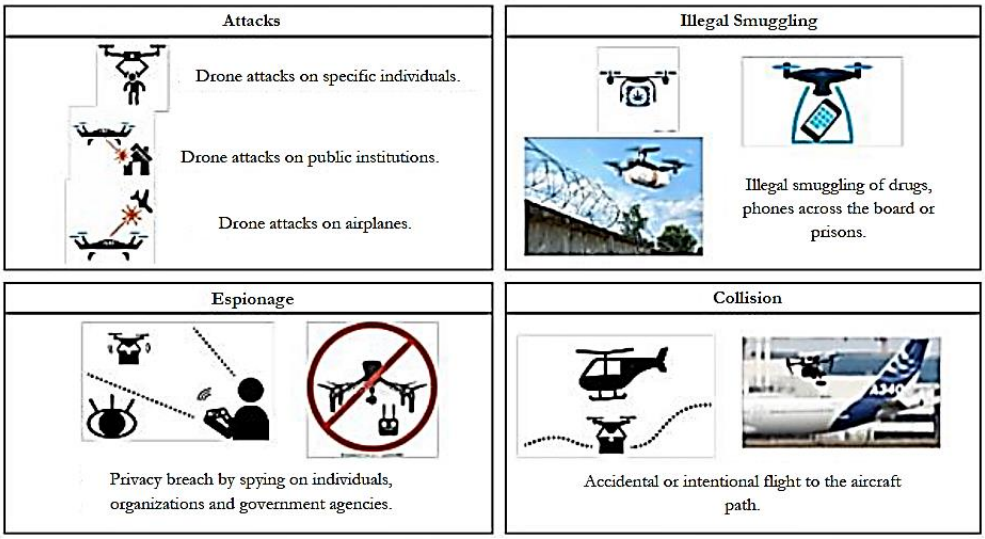

Fig. 7. The main drone threat categories: Drone attacks, illegal smuggling, drone espiong, and drone collisions.

4.3 | Threat Modeling and Security Requirements

Develop a threat model to identify the top security threats to urban IoT networks. The model is based on information gathered from research articles, real-world events, and existing knowledge of smart cities in energy-intensive areas. This includes threats at the device, network, and data level. Core security principles (Such as confidentiality, integrity, availability, and privacy) are described to guide the design of AI solutions.

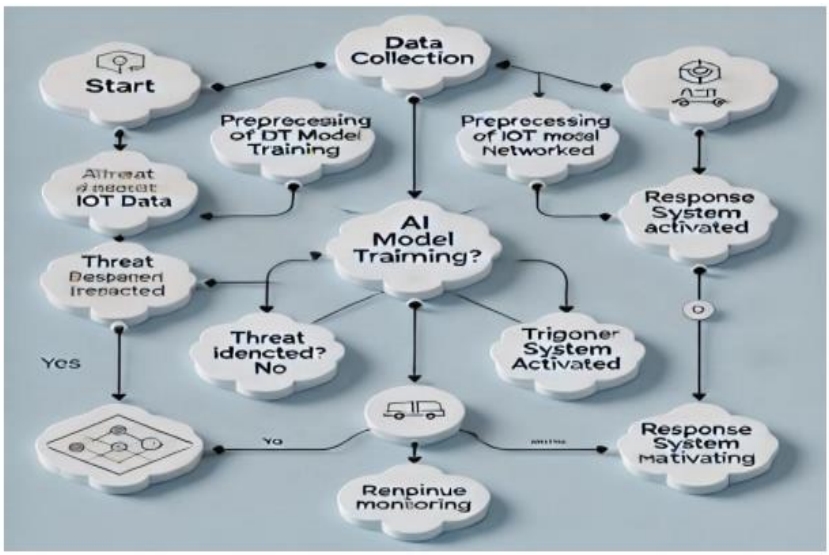

Fig. 8. Threat modeling framework for urban internet of things security.

4.3.1|Design of artificial intelligence-based security models

The study proposes several AI-based models tailored to address key IoT security issues.

I. Supervised machine learning for anomaly detection: We train learning machines (e.g., decision trees, random forests, support vector machines) using data collection on bad and lousy work to detect known security threats.

II. Unsupervised learning for unknown threat detection: Unsupervised learning techniques (e.g., k-means clustering, autoencoders) are used to identify vulnerabilities in IoT systems and identify unknown or zero-day attacks.

III. Deep learning for intrusion detection: Deep neural networks, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are used to capture complex patterns in network connections and AI behavior for better access detection.

4.3.2|Dataset selection and preprocessing

This study uses publicly available IoT security data (e.g., Bot-IoT dataset, IoT-23 dataset) and accurate city traffic data collected from smart cities where possible. To be efficient, the data is pre-processed, including:

I. Cleaning: Incomplete data or invalid data is removed.

II. Normalization: Standardize data features to improve the performance of machine learning models.

III. Feature selection: Identify the most important features (Such as packet size, connection time, and device performance) that help correctly identify threats.

4.3.3|Model training and testing

The AI model is trained using 70% of the dataset and tested on the remaining 30%. Cross-validation avoids overfitting and ensures that the model generalizes well to unobserved data. The main metrics used to evaluate the model include:

I. Accuracy: The proportion of predictions produced by the model.

II. Precision: The ratio of true positives to the total number of predicted positives, indicating the model's ability to avoid false alarms.

III. Recall: The ratio of true positives to the total number of actual positives, reflecting the model's ability to detect all relevant threats.

IV. F1 score: The harmonic mean of precision and recall, providing a balanced evaluation metric.

V. False positive rate: To assess how frequently the models incorrectly identify benign activity as malicious.

4.3.4 | Simulation environment for testing artificial intelligence-based security models

To test the effectiveness of the AI model, a simulated urban IoT environment was created using software such as Network Simulator-3 (NS-3) and Cooja (IoT Network Simulator). The simulation simulates various IoT-based smart city scenarios (Traffic control, smart energy, and public safety) and includes IoT security threats (Such as DDoS attack threats, malware, and unauthorized access).

4.3.5 | Evaluation and comparative analysis

The effectiveness of AI-enhanced security models is compared with traditional security methods (e.g., signature-based access detection, custom-based firewalls). The comparison evaluates each model's performance, efficiency, and ability to manage different devices with urban IoT constraints. Also, the model's effectiveness in detecting new attacks and exploits is difficult [13].

4.4 | Tools and Technologies

This approach uses the following tools and technologies:

I. Python: For machine learning and deep learning algorithms using libraries such as TensorFlow, Keras, and Scikit-learn

II. MATLAB/Simulink: For reinforcement learning simulations

III. NS-3 and cooja: Simulate IoT networks and evaluate the performance of the proposed model in smart city environments

IV. Wireshark and zeek (Formerly bro): For network traffic analysis and feature extraction

V. Power trace: Monitor the power consumption of the IoT devices during modeling

5 | Conclusion

Integrating AI and IoT into efficient traffic management and public safety has profound implications that translate into the direction of safe, accessible, and efficient transportation systems. AI analytics allows real-time monitoring of traffic patterns so that adaptive traffic signal controls and smart routing are enabled. That congestion is dramatically reduced while travel times are reduced. Other technologies, such as connected vehicles and smart infrastructure, create critical data that aid in situational awareness and enhance the likelihood of more informed decision-making by authorities in traffic management.

In addition to advancing public health, AI and IoT solutions also progress proactive surveillance and emergency response capabilities in public safety. Advanced analytics can pick up abnormal behaviors on smart surveillance systems, leading to early police intervention, which could even thwart the commission of a crime. Sensors around the environment monitor such aspects as air quality and decibel levels to improve public health within the community.

Notwithstanding such promising developments, issues such as privacy over data, infrastructure demands, and the need for effective interoperability have to be appropriately addressed to maximize the potential of these technologies. Their successful implementation would depend on public acceptance and trust in such systems.

Implementing AI and IoT solutions in traffic management and public safety improves operational efficiencies and simultaneously contributes to safe, intelligent, and sustainable lifestyles in urban spaces. Whether this can be achieved while implementing the technological piece lies in the future of the smart city. Future initiatives will ensure participant coordination, infrastructure investment to enforce the proper and responsible use of AI and IoT, and effective policies.

Acknowledgments

I would like to express my sincere appreciation to all those who assisted me in researching and writing this paper.

First and foremost, I am deeply thankful to my academic advisors and mentors for their invaluable support and encouragement. Their knowledge and insights were crucial in enhancing my understanding of the intricate issues related to AI and IoT solutions for efficient public service delivery to smart cities. I also want to recognize the constructive feedback from my peers and colleagues. Their engaging discussions and critical viewpoints significantly enriched the quality of my research. I am particularly grateful to the institutions and scholars whose work I cited in this paper. Their commitment to expanding knowledge in IoT, machine learning, waste management, and transportation systems has profoundly influenced my research.

Finally, I acknowledge the steadfast support of my family and friends. Their encouragement and patience were essential as I faced the various challenges of this research. I hope this paper adds value to the ongoing discussions in this vital field and encourages future advancements in secure and efficient transportation systems.

Data Availability

I advocate for transparency in research by promoting public access to data. However, this study did not generate any new data. The results presented in this paper are derived from a thorough review of existing literature and publicly accessible datasets about IoT-enabled smart transportation networks.

The datasets examined in this research can be located in the following publicly available archives:

I. UCI machine learning repository: This repository offers a variety of datasets pertinent to smart transportation systems that are suitable for further investigation.

II. Kaggle datasets: Kaggle features numerous datasets related to transportation, IoT, and security, which can yield valuable insights for future research.

III. Transportation Research Board (TRB) publications: TRB provides access to many publications and datasets focused on transportation research.

IV. It is important to note that specific datasets that include sensitive user information have not been disclosed due to privacy and ethical considerations. The data utilized in this paper adheres to all relevant ethical standards and data protection regulations.

Conflicts of Interest

The author declares no conflict of interest. I affirm that no personal circumstances or interests could be perceived as having an inappropriate influence on the presentation or interpretation of the research findings reported in this paper. Furthermore, funders played no role in the design of the study, in the collection, analysis, or interpretation of the data, in the writing of the manuscript, or in the decision to publish the results.

References

[1] Musa, A. A., Malami, S. I., Alanazi, F., Ounaies, W., Alshammari, M., & Haruna, S. I. (2023). Sustainable traffic management for smart cities using internet-of-things-oriented intelligent transportation systems (ITS): Challenges and recommendations. *Sustainability*, *15*(13), 9859. https://doi.org/10.3390/su15139859

[2] Lee, C. P., Leng, F. T. J., Habeeb, R. A. A., Amanullah, M. A., & ur Rehman, M. H. (2022). Edge computing-enabled secure and energy-efficient smart parking: A review. *Microprocessors and microsystems*, *93*, 104612. https://doi.org/10.1016/j.micpro.2022.104612

[3] Wang, T., Miao, Z., Chen, Y., Zhou, Y., Shan, G., & Snoussi, H. (2019). AED-Net: An abnormal event detection network. *Engineering*, *5*(5), 930–939. https://doi.org/10.1016/j.eng.2019.02.008

[4] Faggiano, V., McNall, J., & Gillespie, T. T. (2011). *Critical incident management: A complete response guide*. CRC Press. https://books.google.com/books

[5] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *Institution of engineering and technology networks*, *9*(4), 145–155. https://doi.org/10.1049/iet-net.2019.0155

[6] Papageorgiou, M., Ben-Akiva, M., Bottom, J., Bovy, P. H. L., Hoogendoorn, S. P., Hounsell, N. B., … ., & McDonald, M. (2007). ITS and traffic management. *Handbooks in operations research and management science*, *14*, 715–774. https://doi.org/10.1016/S0927-0507(06)14011-6

[7] Muthuramalingam, S., Bharathi, A., Rakesh Kumar, S., Gayathri, N., Sathiyaraj, R., & Balamurugan, B. (2019). IoT based intelligent transportation system (IoT-ITS) for global perspective: A case study. *Internet of things and big data analytics for smart generation*, *21*(3), 279–300. https://doi.org/10.1007/978-3-030-04203-5_13

[8] Mohapatra, H. (2021). Socio-technical challenges in the implementation of smart city. *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 57–62). IEEE. https://doi.org/10.1109/3ICT53449.2021.9581905

[9] Hancer, E., Xue, B., & Zhang, M. (2020). A survey on feature selection approaches for clustering. *Artificial intelligence review*, *53*(6), 4519–4545. https://doi.org/10.1007/s10462-019-09800-w

[10] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE access*, *7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

[11] Mohanty, S. P., Yanambaka, V. P., Kougianos, E., & Puthal, D. (2020). PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE). *IEEE consumer electronics magazine*, *9*(2), 8–16. https://doi.org/10.1109/MCE.2019.2953758

[12] Gupta, B. B., & Wu, J. (2025). Integration of IoT with robotics and drones. In *AI developments for industrial robotics and intelligent drones* (pp. 33–54). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-2707-4.ch003

[13] Siau, K., & Rossi, M. (2011). Evaluation techniques for systems analysis and design modelling methods-a review and comparative analysis. *Information systems journal*, *21*(3), 249–268. https://doi.org/10.1111/j.1365-2575.2007.00255.x