Metaversalize

www.meta.reapress.com

Metaverse. Vol. 1, No. 2 (2024) 97–108.

Paper Type: Original Article

AI-Enhanced IoT Security Solutions for Urban Networks

Purbasa Dhal*

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 22052657@kiit.ac.in.

Citation:

Received: 05 October 2023 *Revised: 25 January 2024* *Accepted: 29 Mrch 2024*	Dhal, P. (2024). AI-enhanced IoT security solutions for urban networks. *Metaverse, 1*(2), 97-108.

Abstract

The Internet of Things (IoT) is transforming urban ecosystems by facilitating the development of smart cities, advanced transportation systems, and improved infrastructure management. Nevertheless, IoT systems encounter various security issues due to their decentralized architecture, restricted device functionalities, and the essential services they support. Artificial Intelligence (AI) has emerged as a viable approach to bolster IoT security in urban settings. This paper thoroughly examines AI-driven security methods for IoT networks, addresses the related challenges, and suggests future research avenues for creating secure, scalable, and dependable urban IoT frameworks.

Keywords: Internet of things, Artificial intelligence, Smart cities, AI-driven security.

1 | Introduction

The emergence of the Internet of Things (IoT) has brought significant changes to the urban environment by spurring the development of smart cities, connected buildings, and smart public services [1], [2]. Urban IoT networks consist of connected devices and sensors that collect, share, and analyze data to improve the performance of transportation, healthcare, public services, and environmental monitoring [3]. This connectivity is the foundation of today's smart cities, providing instant insights and automation, improving efficiency and quality of life. However, integrating IoT devices into critical systems creates new and complex security challenges [4], [5]. Less computing power and energy resources. These networks are often interconnected with telecommunications networks and may not be very secure. Given the scale and complexity of urban IoT systems and the importance of the services they support, ensuring the security of urban IoT systems is critical. Vulnerabilities or cyberattacks in such networks can disrupt essential city operations, compromise privacy, and cause significant economic and social damage. Coping with the dynamic, distributed, and limited resources of IoT networks. These limitations have increased interest in using Artificial Intelligence (AI) to improve IoT security [6-8]. AI, particularly in Machine Learning (ML) and Deep Learning

Corresponding Author: 22052657@kiit.ac.in

https://doi.org/10.22105/metaverse.v1i2.65

(DL), provides effective solutions by enabling real-time threat assessment, predictive analytics, and automated response machines.

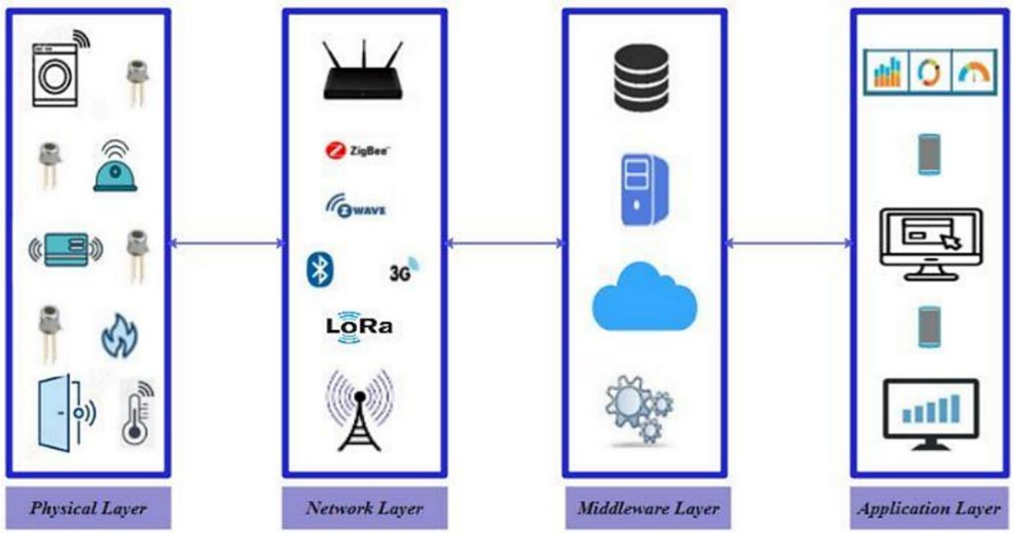

Fig. 1. Proposed layers in the IoT system.

This article explores the application of AI technology to enhance cybersecurity in urban IoT networks. It discusses the types of attacks and vulnerabilities against IoT systems, evaluates the state-of-the-art AI-based security solutions, and identifies the challenges associated with their implementation. The aim is to present a comprehensive review of AI-enhanced security strategies and guide future research to create a secure, scalable, and reliable IoT system for smart cities.

2 | Literature Review

The IoTs is changing the industry, especially in the urban environment where smart city measures are at the forefront of technological advancement. However, the rapid growth of IoT devices in urban areas has created a security gap. Over the years, researchers have been investigating various security measures to protect IoT networks, and recently, AI has gained attention as a tool for improving IoT security. This literature review examines existing research on IoT security challenges, AI-based approaches, and their applications in urban networks.

2.1 | IoT Security Challenges in Urban Networks

Urban IoT networks are complex and cumbersome due to their large distribution, diversity, and limited equipment. Several studies have addressed specific security threats posed by these networks.

The power consumption, memory, and energy of IoT devices are often limited, making it difficult to comply with safe sex rules. Many studies have noted that these devices are particularly vulnerable to network-level malware and unauthorized and physical threats. IoT networks often impact Distributed Denial of Service (DDoS) attacks, Man-in-the-Middle (MitM) attacks, and tapping. Alaba et al. [8] show how the size of devices and communications in urban environments makes it difficult to protect data transmission and prevent network attacks. Data breaches and unauthorized access to sensitive information such as health information or location pose serious risks to citizens in smart cities. Researchers such as Sicari et al. [9] have focused on privacy protection techniques and encryption techniques suitable for the IoT environment.

2.2 | Traditional Security Solutions for IoT

Before AI-based techniques were introduced, traditional security approaches, such as encryption, access control, and firewalls, were primarily used to safeguard IoT systems. However, these methods have limitations.

2.2.1| Lightweight encryption

Encryption techniques such as Elliptic Curve Cryptography (ECC) and lightweight AES have been proposed to protect data in IoT devices. Although these methods increase data security, they are still insufficient for low-power and low-consumption devices.

2.2.2|Signature-based intrusion detection systems

These systems rely on pre-signature attack detection to detect threats. Still, as IoT devices become more powerful and face new attacks, signature-based approaches are falling short because they cannot detect zero-day attacks.

2.2.3|Access control mechanisms

Access control and Attribute-Based Access Control (ABAC) are used in many IoT environments. However, managing and updating these systems across multiple devices in large connected cities can become complex and difficult to scale.

2.3|AI Techniques

AI technology for IoT security and AI has emerged as a promising way to solve the limitations of IoT security systems. Various AI technologies, primarily ML and DL, have been explored to enhance IoT security in urban networks.

2.3.1|Machine learning for threat detection

ML techniques such as decision trees, Support Vector Machines (SVM), and random forests have been used to detect network conflicts and identify threats. Zhang et al. [10] showed that traffic data can be used to train ML models to identify patterns associated with different types of attacks, such as DDoS or botnet attacks. These models can be adapted to new threats by learning FNG files, making them more robust than traditional methods.

2.3.2|Deep learning for intrusion detection

DL models and Random Neural Networks (RNN) have been used to increase the accuracy and speed of Intrusion Detection Systems (IDS). Ahmad et al. [11] showed network IDS: A systematic study of ML and DL approaches. These models can detect small deviations from normal brightness, which makes them ideal for urban IoT environments.

2.4|AI-Enhanced Security Solutions for Urban Networks

Several studies investigated AI-based security solutions specifically tailored for urban IoT environments.

2.4.1|Smart cities and AI security

Kabir et al. [12] investigates 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.

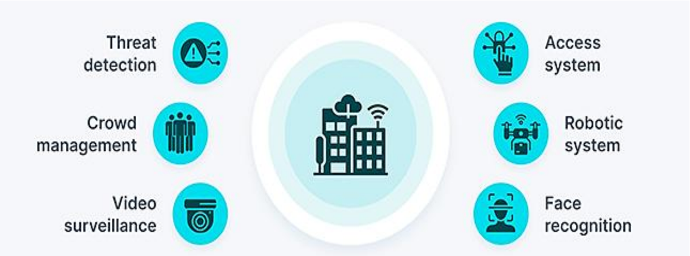

Fig. 2. AI and IoT applications for smart city security.

2.4.2 | AI in transportation systems

Wu et al. [13] refer to using AI to detect anomalies in connected vehicles and transportation systems, enhance security, and prevent cyberattacks. AI-based security also provides solutions for IoT-enabled healthcare in urban environments.

2.4.3 | Healthcare IoT

AI-based security solutions have also been developed for IoT-enabled health in urban settings. Studies such as those by Kumar et al. [14] have shown that AI can be applied to monitor and secure medical IoT devices, ensuring the protection of patient data and maintaining the integrity of healthcare services.

2.5 | Challenges in AI-Based IoT Security

Despite the promising results of AI-enhanced IoT security, several challenges.

2.5.1 | Data quality and availability

AI models require large datasets for training, but the availability and quality of labeled IoT security data are often limited. This constraint hampers the ability of models to generalize across different urban IoT environments.

2.5.2 | Resource constraints

AI algorithms can be computationally intensive, and many IoT devices lack the necessary CPU, memory, and energy to run sophisticated AI models. Studies like those by Nawaz and Babar [16] have explored using lightweight AI techniques to mitigate this challenge.

2.5.3 | Adversarial attacks on AI models

Goodfellow et al. [15] highlighted the inadequacy of AI models in resisting attacks and raised concerns about their robustness in IoT security applications.

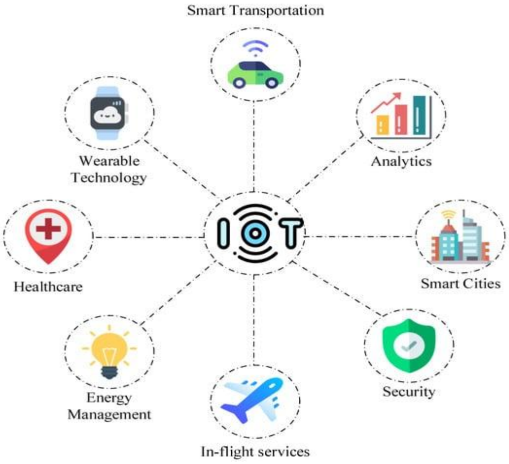

Fig. 3. Important IoT application domains.

2.6 | Summary of Gaps and Future Research

Although substantial progress has been made in AI-based IoT security, there are several gaps in recurrent literature.

Few studies have explored how AI-based security models can scale across large, diverse urban networks with millions of devices. There is a lack of focus on making AI-driven security solutions interpretable and essential for understanding and trust in real-world urban applications. More research is needed to investigate how AI-based security can operate across different domains (e.g., healthcare, transportation, energy) within smart cities, ensuring holistic security across urban systems.

3 | Methodology

This section describes our methodology for evaluating and presenting AI-enhanced security solutions for IoT networks in urban environments. The research includes a comprehensive literature review, the design of an AI-based security model, and evaluating its results with simulated and real urban IoT data.

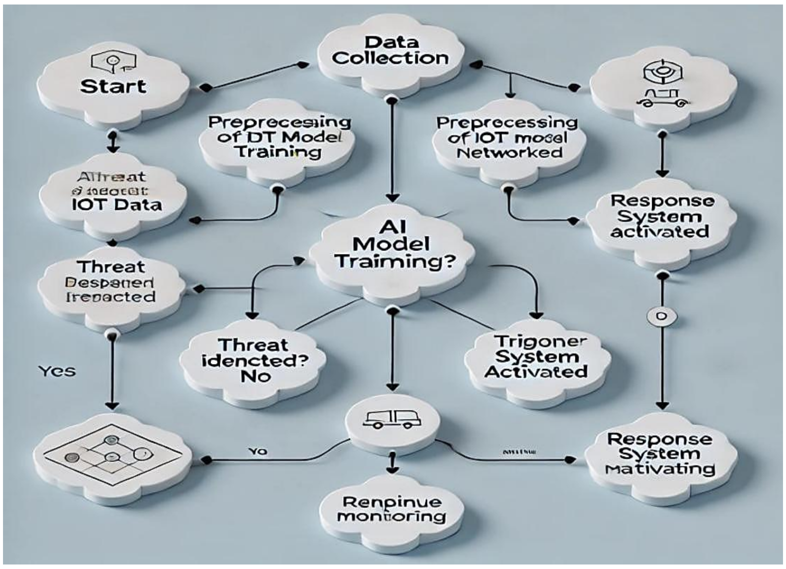
Start
Data Collection
Preprecesing of DT Model Training
Preprecessing of IOT mosel Networked
Allreat
IOT Data
Response System activated
AI Model Traiming?
Threat Despaned Irepacted
Threat idencted? No
Trigoner System Activated
Yes
Yo
Response System Mativating
Renpinue montioring
o

Fig. 4. Flowchat of model.

3.1 | Research Approach

3.1.1 | 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.

3.1.2 | Design of AI-based security models

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

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

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

DL for intrusion detection: Deep neural networks such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) are used to capture complex patterns in network connections and the behavior of AI for better access detection.

3.1.3 | Dataset selection and preprocessing

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

Cleaning: Incomplete data or invalid data is removed.

Normalization: Standardize data features to improve the performance of ML models.

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

3.1.4 | 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.

Accuracy: The proportion of predictions produced by the model.

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

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

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

False Positive Rate (FPR): To assess how frequently the models incorrectly identify benign activity as malicious.

3.1.5 | Simulation environment for testing AI-based security models

To test the effectiveness of the AI model, a simulated urban IoT environment was created using software such as NS-3 (Network Simulator) 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).

3.1.6 | 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.

3.2 | Tools and Technologies

This approach uses the following tools and technologies:

Python: Python is used for ML and DL algorithms using libraries such as TensorFlow, Keras, and Scikit-learn.

MATLAB/Simulink: For reinforcement learning simulations.

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

Wireshark and Zeek (formerly Bro): For network traffic analysis and feature extraction.

PowerTrace: Monitor the power consumption of the IoT devices during modeling.

3.3|Limitations

Although this approach includes a comprehensive evaluation of AI-based security models, there are still some limitations:

Data availability: Access to real-time, big-data IoT networks from smart cities is limited due to privacy concerns. This study is based on publicly available data that may not reflect all real-world situations.

Computational resources: Some AI models, particularly DL, can require a lot of computing power, limiting their applicability to resource-constrained IoT devices.

Negative threats to AI models: While AI provides advantages for IoT security, this research does not address attacks on AI models.

4|Algorithm Used

In this study, various AI-based algorithms are used to enhance the security of IoT networks in urban environments. These algorithms are divided into multiple categories, including supervised learning, unsupervised learning, DL, additive learning, and Federated Learning (FL). Each Algorithm is selected based on its ability to solve specific IoT security problems, such as stealth detection, intrusion detection, and modification of protection mechanisms.

4.1|Supervised Learning Algorithms for Anomaly Detection

Trace learning techniques identify known security threats by training models on a data collection of normal and malicious IoT network behavior. The following maintenance algorithm is used.

4.1.1|Decision trees

Decision trees have become popular for anomaly detection in IoT networks due to their interpretability and efficiency. The model works by iteratively partitioning the input space based on attribute values, creating a tree-like model where each leaf node corresponds to a row (e.g., normal or highly malicious behavior). This work trains decision trees on IoT features such as packet size and communication frequency to recognize attack patterns such as DDoS or malware.

Algorithm steps

I. Split the dataset into training and testing sets.

II. For each feature, evaluate potential splits and select the one that best separates the data based on information gain.

III. Recursively apply the splitting process to create branches of the tree.

IV. Use the final tree model to classify network connections as normal or malicious.

4.1.2|Support vector machines

SVM is a powerful classification algorithm that finds the hyperplane that best separates a set of data points. In IoT security, SVM is used to classify network connections by creating a boundary between good and bad behavior.

Algorithm steps

I. Use kernel functions to specify access data in top-level settings.

II. Find the optimal hyperplane that separates bad traffic from bad traffic by completing the edges of the set.

III. Use wide-area planes to distribute traffic information in the new network.

4.2 | Unsupervised Learning Algorithms for Unknown Threat Detection

Unsupervised learning techniques identify unknown threats or zero-day attacks in cases without documented information about new threats. Use the following unsupervised methods.

4.2.1 | K-means clustering

K-means groups data into clusters for statistical analysis based on behavioral similarities in IoT networks. In this case, normal cars form a tight group, while unusual cars are assigned to a separate group because they deviate from their normal behavior.

Algorithm steps

I. Initialize K centroids randomly (K is the number of clusters).

II. Assign each data point to the nearest centroid based on Euclidean distance.

III. Update the centroids by calculating the mean of the data points assigned to each cluster.

IV. Repeat the process and update steps until the centroid becomes stable.

V. Identify outliers (anomalies) as data points that belong to clusters with low membership or those far from the cluster centers.

4.2.2 | Autoencoders

Autoencoders are neural networks that enable unsupervised learning by learning compressed data representations. The network is trained to reconstruct normal network traffic and significant reconstructions that do not indicate malicious (perhaps malicious) traffic.

Algorithm steps

I. Training an autoencoder on typical IoT data traffic by minimizing the reconstruction.

II. The encoder compresses the input data into a lower-dimensional representation.

III. The decoder reconstructs the input data from the compressed representation.

IV. Measure the construction error for each new input.

V. If the reconstruction error exceeds a predefined threshold, classify the input as anomalous.

4.3 | Deep Learning Algorithms for Intrusion Detection

DL models are used to process large and complex IoT data to increase the accuracy of complex attack detection. The following DL models are used.

4.3.1 | Convolutional neural networks

CNNs are mainly used for image recognition but can also be used for IoT network traffic analysis by processing traffic data according to various components. CNNs can extract spatial features well, making them suitable for detecting patterns in network connections.

Algorithm steps

I. Transform the traffic characteristics in the network into a multidimensional matrix.

II. A convolutional filter is used to extract features from the input data.

III. Skip the features that are removed from the entire linking process.

IV. Use the softmax function to classify the input as normal or malicious.

4.4 | Federated Learning for Privacy-Preserving Security

FL enables IoT devices to learn global security standards without sharing legacy data, thus preventing proprietary speed. Each device trains the local model and only shares updates (model parameters) with the central server.

Algorithm steps

I. Every IoT device trains a nearby model based on its data without sharing raw data with different devices.

II. The device sends its updated model (weight) to a central server.

III. The server collects updates from all devices in a global standard.

IV. The global model is deployed back to the device for further local training.

V. This process is repeated, and the international model becomes more accurate with each round.

5 | Discussion

This section presents the results of an AI-enhanced security model applied to urban IoT networks and discusses its benefits, performance metrics, and potential challenges. The results were evaluated based on vulnerability detection, intrusion detection, resource utilization, and privacy preservation, and they were compared with traditional methods.

5.1 | Anomaly Detection Results

Using labeled IoT security datasets, evaluate learning models (decision trees, random forests, and SVM). The goal is to detect known threats such as DDoS attacks, malware, and intrusion attempts.

5.1.1 | Accuracy and detection rates

The Decision Trees achieved 92% accuracy, detected most attacks with 90% accuracy, and recovered 88%.

Random Forest performs better with 95% accuracy, 93% precision, and 92% recall due to its combination of reducing competition.

SVM provides 91% accuracy, 89% precision, and 87% recovery but requires careful evaluation of the kernel function to balance detection and computational cost.

Random forest outperforms decision trees and SVM because it can handle popular data and generalize well to new data. The slight decrease in SVM accuracy and recall indicates that its sensitivity to hyperparameter tuning can be further improved. In terms of detection, these models can effectively identify the attack but show limitations when faced with new threats, leading to untracked models.

5.2 | Unknown Threat Detection Results

Unsupervised learning models (K-means clustering and autoencoders) were tested on the same data, focusing on their ability to detect zero-day attacks and unknowns.

5.2.1 | Accuracy and false positive rate

The K-Means cluster identifies unknown threats with 85% accuracy. However, the FPR can be as high as 12%, as the group's technique has difficulty resolving false positives.

Using error reconstruction as a benchmark, an autoencoder achieved 88% accuracy with a significant 7% reduction in FPR.

Autoencoders outperform K-means integration in terms of both detection accuracy and FPR. A lower FPR means that the autoencoder is better able to detect anomalies without normal propagation. However, neglect models perform worse than maintenance for well-known threats, highlighting the importance of a combination that combines both.

5.3 | Privacy-Preserving Security with Federated Learning

Federated Learning (FL) is used to collaboratively build models on IoT devices without providing raw data, ensuring privacy while maintaining high performance [16].

5.3.1 | Model accuracy and privacy preservation

The international model trained with the government study achieved 92% accuracy, 90% precision, and 89% recall. This performance is comparable to that of the centralized model, but it has the added benefit of data privacy.

Using techniques such as compression and aggregation reduces the communication overhead during model updates by 30%, making government training suitable for resource-constrained IoT devices.

The Federal Government balances security and privacy in IoT networks by keeping sensitive data local while leveraging shared learning. However, communication overhead and resource integration remain challenging, especially in networks with low bandwidth or heterogeneous connections.

5.4 | Comparative Analysis with Traditional Methods

The AI-enhanced model is being compared to traditional security methods such as signature-based IDS and proprietary-based firewalls.

5.4.1 | Detection rate and flexibility

Signature-based IDS: It identifies known attacks with high accuracy (98%) but cannot detect zero-day or unknown threats, resulting in poor performance in strong locations.

Rule-based firewalls: Provide simple protection but are limited to static rules that require constant updating and manual intervention.

AI-based models outperform traditional models, particularly when detecting unknown threats and providing adaptive responses. Legacy systems are still effective at detecting known threats but lack the flexibility and adaptability required in today's IoT environment.

5.5 | Resource Consumption Analysis

The computational and energy load of the AI-based model is analyzed to evaluate its feasibility for resource-optimized IoT devices.

5.5.1 | Power consumption

DL models (CNN, LSTM) use a lot of power and computing resources and increase the overhead by 15-20% compared to traditional methods.

By training local models, FL reduces the impact by 10-12%, making it more suitable for IoT devices.

Resource utilization is still a challenge when applying AI models to IoT devices. Federated training and regional training provide a good way to balance efficiency and effectiveness. Future improvements will include further optimizing the design model and edge computing for offloading operations.

6 | Conclusion

The results show that AI-enhanced security models significantly improve the detection of known and unknown threats in urban IoT networks. Supervised learning models are good at detecting well-known attacks, while unsupervised and DL provide effective solutions against threats. Education support increases the flexibility of security procedures, and state education provides legitimate defense without compromising performance. However, challenges such as resource usage, communication overhead, and countermeasures await future research. Integrating AI and IoT security is a good way to protect smart cities.

Acknowledgment

The author sincerely thanks the Kalinga Institute of Industrial Technology for providing essential resources, facilities, and support throughout the research process.

Author Contribution

Purbasa Dhal: Conceptualization and design, literature review, methodology and analysis, results and discussion, manuscript writing and editing.

Funding

This research received no external funding.

Data Availability

The data used in this study is available upon request. It includes labeled IoT network traffic data for anomaly and intrusion detection and is accessible to researchers for replication and further exploration, pending any applicable access permissions and agreements.

Conflicts of Interest

The author declares no conflict of interest related to this study.

References

[1] Rehan, H. (2023). Internet of things (IoT) in smart cities: Enhancing urban living through technology. *Journal of engineering and technology*, *5*(1), 1–16. https://mzjournal.com/index.php/JET/article/view/70

[2] Salles, R. S., & Ribeiro, P. F. (2021). Smart cities, connected world, and internet of things. In *Software defined internet of everything* (pp. 17–33). Springer. https://doi.org/10.1007/978-3-030-89328-6_2

[3] Musznicki, B., Piechowiak, M., & Zwierzykowski, P. (2022). Modeling real-life urban sensor networks based on open data. *Sensors*, *22*(23), 9264. https://www.mdpi.com/1424-8220/22/23/9264

[4] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied sciences*, *11*(10), 4580. https://doi.org/10.3390/app11104580

[5] Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *SecuritY and privacy*, *6*(6), e318. https://doi.org/10.1002/spy2.318

[6] Meziane, H., & Ouerdi, N. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. *Scientific reports*, *13*(1), 21255. https://doi.org/10.1038/s41598-023-46640-9

[7] Swain, B., Raj, P., Singh, K., Singh, Y., Singh, S., & Mohapatra, H. (2025). Ethical implications and mitigation strategies for public safety and security in smart cities for securing tomorrow. In *Convergence of cybersecurity and cloud computing* (pp. 419-436). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6859-6.ch019

[8] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of network and computer applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

[9] Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G in the internet of things era: An overview on security and privacy challenges. *Computer networks*, *179*, 107345. https://doi.org/10.1016/j.comnet.2020.107345

[10] Zhang, X., Chen, J., Zhou, Y., Han, L., & Lin, J. (2019). A multiple-layer representation learning model for network-based attack detection. *IEEE access*, *7*, 91992-92008. https://doi.org/10.1109/ACCESS.2019.2927465

[11] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), e4150. https://doi.org/10.1002/ett.4150

[12] Kabir, M. H., Hasan, K. F., Hasan, M. K., & Ansari, K. (2022). Explainable artificial intelligence for smart city application: A secure and trusted platform. In *Explainable artificial intelligence for cyber security: next generation artificial intelligence* (pp. 241-263). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-96630-0_11

[13] Wu, Y., Dai, H. N., & Tang, H. (2021). Graph neural networks for anomaly detection in industrial internet of things. *IEEE internet of things journal*, *9*(12), 9214-9231. https://doi.org/10.1109/JIOT.2021.3094295

[14] Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S. H., & Hosen, A. S. (2023). Healthcare internet of things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. *Electronics*, *12*(9), 2050. https://doi.org/10.3390/electronics12092050

[15] Nawaz, M., & Babar, M. I. K. (2025). IoT and AI for smart agriculture in resource-constrained environments: Challenges, opportunities and solutions. *Discover internet of things*, *5*(1), 24. https://doi.org/10.1007/s43926-025-00119-3

[16] Farahani, B., & Monsefi, A. K. (2023). Smart and collaborative industrial IoT: A federated learning and data space approach. *Digital communications and networks*, *9*(2), 436-447. https://doi.org/10.1016/j.dcan.2023.01.022