Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Adaptive AI-Blockchain Framework for Threat Detection and Mitigation in IoT-Enabled Smart Cities

Mr. Narendrakumar[1], Dr.Rajeev Shrivastava[2]
Research Scholar, Dept. of Mechanical Engineering, Mahakaushal University Jabalpur (M.P), India[1]
Professor, Department of Mechanical Engineering, Mahakaushal University Jabalpur (M.P), India[2]

Keywords

Received: 30 Dec 2024
Revised: 19 Feb 2025
Accepted: 27 Feb 2025

ABSTRACT

The growth of Internet of Things (IoT) devices in smart cities has increased the risk of cyber threats due to new attack surfaces and limited built-in security. This paper presents an adaptive, multi-layered security framework that combines deep learning, reinforcement learning, and blockchain to detect and mitigate threats in IoT environments. The system uses a Convolutional Neural Network–Long Short-Term Memory (CNN–LSTM) model to detect anomalies in network traffic with high accuracy. When a threat is detected, a Deep Q-Network (DQN) agent selects the most appropriate response based on the threat level, trust score of the device, and service importance. To ensure transparency and integrity, all events and actions are stored immutably using Hyperledger Fabric and the InterPlanetary File System (IPFS). Experiments using the BoT-IoT dataset show that the CNN–LSTM model achieves 97.8% accuracy and an AUC of 0.992. The DQN agent reduces false isolations to 2.8% and maintains an average response time of 148 ms. Compared to traditional systems, the proposed framework offers better accuracy, faster decision-making, and improved trust management. The use of blockchain ensures secure, auditable records across multiple domains. This approach provides a scalable and intelligent solution for securing smart city infrastructures against evolving threats.

INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices within smart city infrastructures has led to significant improvements in urban efficiency and resource management. These systems support real-time traffic control, energy monitoring, waste management, and e-governance. However, they are also inherently vulnerable to cybersecurity threats due to their heterogeneous nature, limited computational power, and widespread deployment [1][2].

The fusion of Artificial Intelligence (AI) with Blockchain technology offers a promising paradigm for addressing these vulnerabilities. While AI provides intelligent anomaly detection and adaptive decision-making, blockchain ensures secure, tamper-proof logging and decentralized control [3][4]. This synergy creates robust frameworks that can autonomously detect, analyze, and mitigate threats in dynamic and complex urban environments [5].

Motivated by the increasing sophistication of cyber-attacks and the pressing need for scalable, self-healing security mechanisms, research has turned toward adaptive AI–blockchain frameworks as the next frontier for securing smart cities [6].

Role of AI in Cybersecurity for Smart Cities

AI has emerged as a core enabler in cybersecurity automation, allowing systems to predict and respond to threats with minimal human intervention. In IoT-enabled smart cities, AI systems can process vast streams of data from sensors and network devices to detect anomalies, intrusions, and behavioral shifts that may indicate malicious activity [7][8].

Deep learning models such as CNNs, RNNs, and federated learning-based classifiers are being integrated into urban systems for real-time threat detection. For example, AI-driven intrusion detection systems (IDS) can identify zero-day attacks by learning latent patterns in encrypted traffic or node behavior [9].

Moreover, Explainable AI (XAI) enhances transparency, allowing decision-makers to understand model predictions—crucial for regulatory compliance and public trust in smart infrastructure [10].

Challenges in AI-Driven Cybersecurity

Despite its potential, implementing AI in cybersecurity comes with significant challenges:

a. Data Quality and Privacy

AI algorithms require large volumes of labeled, high-quality data, which is scarce and often sensitive in nature. This limits model accuracy and introduces risks of data leakage in public networks [12].

b. Model Interpretability

AI models, especially deep neural networks, are often considered "black boxes," making it hard to justify security decisions—a major concern for government or legal applications in smart cities [13].

c. Scalability in Distributed Environments

Deploying AI across distributed and resource-constrained IoT devices introduces latency, energy consumption, and deployment complexity, especially when AI is implemented at the edge or in fog computing layers [14-16].

d. Adversarial Attacks

AI models themselves can be targeted by adversarial inputs or poisoned training data, making them unreliable in mission-critical cybersecurity scenarios.

METHODOLOGY

This study proposes a multi-layered security framework that integrates deep learning, reinforcement learning, and blockchain technologies to detect, respond to, and log cyber threats within IoT-enabled smart cities. The methodology is structured across four main functional layers: data ingestion and preprocessing, deep anomaly detection, adaptive mitigation, and decentralized trust enforcement. Each layer contributes a modular function to ensure scalability, autonomy, and auditability.

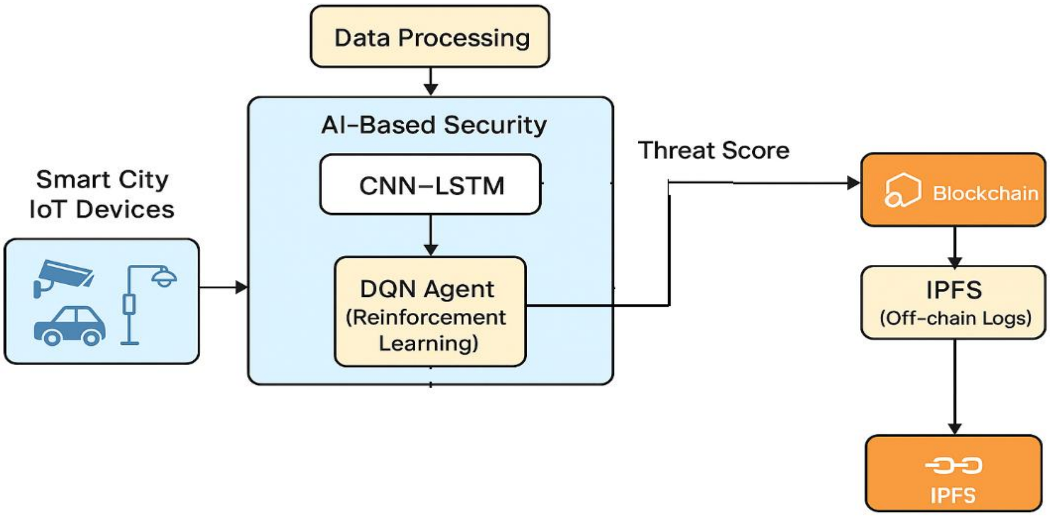

Figure 1. Architecture Diagram

Figure. 1 illustrates the overall architecture, which comprises four primary layers: (A) Data Ingestion and Preprocessing, (B) AI-Based Threat Detection, (C) Adaptive Threat Mitigation, and (D) Decentralized Trust and Logging.

Dataset and Preprocessing

This study employs the BoT-IoT dataset, a publicly available and widely used benchmark created by the Cyber Range Lab at the University of New South Wales (UNSW), specifically designed for IoT security research [19]. The dataset simulates a heterogeneous IoT network environment comprising smart devices such as weather sensors, garage doors, and refrigerators, and includes a diverse range of benign and malicious traffic. Attack types include Distributed Denial of Service (DDoS), Denial of Service (DoS) over TCP, UDP, and HTTP protocols, data theft, and reconnaissance (e.g., scanning and probing). With over 70 million labeled instances, the dataset offers rich ground truth and temporal diversity, making it suitable for supervised learning and sequence modeling.

A structured preprocessing pipeline is applied to prepare the dataset for model training. Initially, 30 relevant features are selected based on prior research and domain knowledge, capturing packet flow characteristics such as source and destination IP addresses, port numbers, protocol types, byte counts, inter-arrival times, and packet rates. This is followed by data cleaning, which includes the removal of null values, duplicates, and non-informative constant columns. To standardize the input space, all numerical features are normalized using Min-Max scaling, as defined in (1):

$$x_{normalized} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \qquad (1)$$

where x is the original feature value, and $x_{\min}$ and $x_{\max}$ represent the minimum and maximum values of that feature, respectively. This transformation ensures all input values fall within the range [0,1], which improves model convergence and training stability.

To address the inherent class imbalance in the dataset—where benign traffic instances far outnumber malicious ones—the Synthetic Minority Over-sampling Technique (SMOTE) is applied. SMOTE generates synthetic samples for underrepresented classes by interpolating feature space between minority class neighbors, thereby reducing bias during model training.

Following class balancing, the dataset is temporally segmented into fixed-length time-series windows to preserve the contextual flow of network activity. This segmentation enables the use of sequence-aware models such as Long Short-Term Memory (LSTM) networks for anomaly detection. Finally, the processed dataset is partitioned into training (70%), validation (15%), and testing (15%) subsets to facilitate model development, hyperparameter tuning, and performance evaluation.

Deep Learning-Based Threat Detection

To accurately identify cyber threats within the IoT environment, a hybrid deep learning architecture combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks is developed. This architecture leverages the strengths of both CNNs and LSTMs—where CNNs are effective in capturing spatial correlations and local feature patterns within input sequences, and LSTMs excel at learning long-term dependencies and temporal dynamics. The fusion of these architectures is particularly well-suited for analyzing network traffic, which exhibits both spatial and sequential patterns over time.

The input to the model comprises time-windowed sequences of normalized network traffic data, each representing a fixed-length segment of feature vectors derived from IoT packet flows. The CNN component of the architecture consists of one-dimensional convolutional layers, which apply multiple filters to extract high-level representations of traffic characteristics such as port usage anomalies, packet density fluctuations, and protocol-specific behaviors. These convolutional layers are followed by activation functions (e.g., ReLU) and max-pooling operations to reduce dimensionality and retain the most salient features.

The output feature maps from the CNN layers are then passed to the LSTM layers, which are designed to model temporal dependencies across sequences. LSTM units maintain internal memory cells and gating mechanisms (input, forget, and output gates), allowing them to learn how prior traffic behavior influences current observations. This temporal modeling is crucial for detecting evolving threats such as slow-scan attacks, distributed probing, or multi-stage intrusions.

The final output layer is a fully connected dense layer with a sigmoid activation function. It produces a threat probability score $\hat{y} \in (0,1)$, representing the likelihood that a given sequence is malicious. A threshold (e.g., 0.5) is applied to classify the traffic as either benign or malicious.

A. Loss Function

The model is trained using the Binary Cross-Entropy (BCE) loss function, which quantifies the difference between the predicted probabilities and the actual class labels. The loss function is defined as:

$$\mathcal{L}_{\text{BCE}} = -\frac{1}{N}\sum_{i=1}^{N} [y_i \cdot \log{(\hat{y}_i)} + (1 - y_i) \cdot \log{(1 - \hat{y}_i)}]$$

where:

- $y_i \in \{0,1\}$ is the ground truth label for sample i,
- $\hat{y}_i \in (0,1)$ is the predicted threat probability for the same sample, and
- N is the number of samples in the batch.

This loss penalizes incorrect predictions more heavily when the model is highly confident, encouraging probabilistic calibration.

B. Training Configuration

The model is trained over 50 epochs using the Adam optimizer with a learning rate of 0.001 and a batch size of 128. Performance is evaluated using standard metrics including accuracy, precision, recall, F1-score, and the Area Under the Receiver Operating Characteristic Curve (AUC). These metrics provide a comprehensive assessment of the model's classification capability, especially under conditions of class imbalance.

C. Output and Integration

Once trained, the CNN–LSTM model serves as the system's first decision point. For every incoming sequence of network activity, it outputs a threat probability score and a corresponding binary classification. These results are subsequently forwarded to the reinforcement learning-based mitigation layer, which determines the appropriate response based on the perceived threat level and contextual parameters.

Adaptive Threat Mitigation Using Reinforcement Learning

To enable intelligent and dynamic responses to detected cyber threats, the proposed framework incorporates a Deep Q-Network (DQN) agent for decision-making. Unlike traditional rule-based or reactive mitigation systems that rely on predefined static policies, the DQN agent adopts a model-free reinforcement learning approach. It learns an optimal mitigation policy by interacting with the environment and maximizing cumulative rewards over time, adapting to changing threat patterns and system conditions.

The state representation provided to the DQN agent comprises five key inputs: the threat probability score output from the CNN–LSTM detection model, the current trust score of the IoT node (ranging from 0 to 100), the criticality index of the node (scaled from 1 to 5 based on its functional importance within the smart city infrastructure), the last mitigation action taken, and the time elapsed since the last detected anomaly. This multi-dimensional state space captures both the threat context and the operational history of the IoT node, enabling the agent to make informed decisions.

Based on the input state, the agent selects one of five discrete mitigation actions: (1) monitor (i.e., take no action and continue observation), (2) generate an alert for administrative review, (3) temporarily isolate the affected node from the network, (4) downgrade the node's trust level, or (5) log the event without intervention (passive response). These actions are designed to balance network security with service availability, allowing for both aggressive and conservative responses depending on the situation.

The reward function guiding the agent's learning process is carefully structured to incentivize correct and timely threat mitigations, penalize false positives and unnecessary isolations, and promote the continuity of essential services. Rewards are positive when threats are accurately mitigated with minimal disruption, and negative when the agent overreacts to benign activity or fails to act on malicious behavior. The agent is trained over 1,000 episodes using an ε-greedy exploration strategy and experience replay, which enhances learning stability and exploration of the action space.

Decentralized Logging via Blockchain and IPFS

To ensure tamper-proof enforcement and traceable incident response within IoT-enabled smart cities, the proposed framework integrates a decentralized logging system built on Hyperledger Fabric blockchain and the InterPlanetary File System (IPFS). The blockchain layer maintains immutable records of key security-related events, including detected anomalies, decisions made by the reinforcement learning (DQN) agent, and trust level updates for IoT nodes. Smart contracts are deployed to automate response actions based on the DQN outputs, enhancing system responsiveness and autonomy. To reduce blockchain overhead while preserving comprehensive data logs, detailed records such as raw traffic data, threat traces, and mitigation histories are stored off-chain in IPFS. Only cryptographic hash pointers to these logs are stored on-chain, ensuring both integrity and efficiency. This hybrid design upholds auditability, data verifiability, and regulatory compliance across distributed service layers in smart city environments.

MODEL TRAINING AND EVALUATION

A. Training Methodology

The proposed threat detection model is trained using a hybrid deep learning architecture that combines Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) units. The training process is performed in a supervised learning setting using the preprocessed BoT-IoT dataset, which includes a balanced distribution of benign and malicious traffic classes after applying SMOTE.

Each input sample is structured as a fixed-length time-series sequence representing a 10-second window of network activity. These sequences are normalized and batched prior to training. The model is trained to classify each sequence as either benign (label 0) or malicious (label 1) using the Binary Cross-Entropy (BCE) loss function.

The model is trained for 50 epochs using the Adam optimizer with a learning rate of η=0.001and a batch size of 128. Early stopping based on validation loss is used to prevent overfitting. The LSTM units are initialized with a hidden state size of 128, and dropout regularization with a rate of 0.3 is applied after LSTM layers to improve generalization.

Once the CNN–LSTM model converges, it is integrated with the Deep Q-Network (DQN) for adaptive mitigation. The DQN agent is trained separately using reinforcement learning over 1,000 episodes, where the environment transitions are derived from the anomaly detection outputs and trust dynamics of IoT nodes. The agent updates its Q-values using the Bellman equation:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left[r_t + \gamma \cdot \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t) \right]$$

where:

- s_t is the current state,
- a_t is the selected action,
- r_t is the received reward,
- $\gamma \in [0,1]$ is the discount factor,
- α is the learning rate, and
- $Q(s, a)$ is the action-value function.

The agent uses an ε-greedy policy for exploration, with ε decaying over time.

Performance Evaluation

To evaluate the performance of the proposed framework, we assess the CNN–LSTM detection model and the DQN-based mitigation policy separately and jointly. The detection model is evaluated using standard classification metrics, including:

1. Accuracy:

$$\text{Accuracy } = \frac{(\text{ True Positives } + \text{ True Negatives })}{(\text{ True Positives } + \text{ True Negatives } + \text{ False Positives } + \text{ False Negatives })}$$

2. Precision:

$$\text{Precision } = \frac{\text{True Positives}}{(\text{ True Positives } + \text{ False Positives })}$$

3. Recall:

$$\text{Recall } = \frac{\text{True Positives}}{(\text{ True Positives } + \text{ False Negatives })}$$

4. F1-score:

$$\text{F1-score } = 2 * \frac{(\text{ Precision } * \text{ Recall })}{(\text{ Precision } + \text{ Recall })}$$

5. AUC-ROC Curve (Area Under the Receiver Operating Characteristic Curve)

$$\text{False Positive Rate } = \frac{\text{False Positives}}{(\text{ False Positives + True Negatives })}, \text{ True Positive Rate= Recall=}\frac{\text{True Positives}}{(\text{ True Positives + False Negatives })}$$

RESULTS AND DISCUSSION

To validate the proposed framework, a series of experiments were conducted using the BoT-IoT dataset. The performance was evaluated at two levels: (1) the anomaly detection capability of the CNN–LSTM model, and (2) the decision-making efficiency of the Deep Q-Network (DQN) agent for adaptive mitigation. All models were trained and tested using a workstation with an Intel i7 CPU, 32 GB RAM, and an NVIDIA RTX 3080 GPU.

A. Anomaly Detection Performance

The CNN–LSTM model was trained on 70% of the dataset and tested on the remaining 15%, with the rest used for validation. Table I summarizes the classification performance:

Table 1 – CNN–LSTM Detection Model Performance

Metric	Value (%)
Accuracy	97.8
Precision	96.4
Recall	98.2
F1-Score	97.3
AUC	99.2

The training performance of the proposed CNN–LSTM anomaly detection model was monitored over 50 epochs using the BoT-IoT dataset. As shown in Figure. 2, both the training and validation accuracy increased steadily throughout the training process, reaching approximately 98% and 96%, respectively. Correspondingly, the training and validation loss decreased consistently, indicating effective convergence and strong generalization capability. The similarity in the training and validation curves confirms the absence of overfitting, validating the model's robustness on unseen data.

To further evaluate the classifier's discrimination ability, a Receiver Operating Characteristic (ROC) curve was plotted based on the model's predictions on the test set. As illustrated in Figure. 3, the ROC curve demonstrates a high Area Under the Curve (AUC) value of 0.992. This indicates that the model achieves excellent separability between benign and malicious traffic instances, with a strong true positive rate and a low false positive rate across various threshold settings.

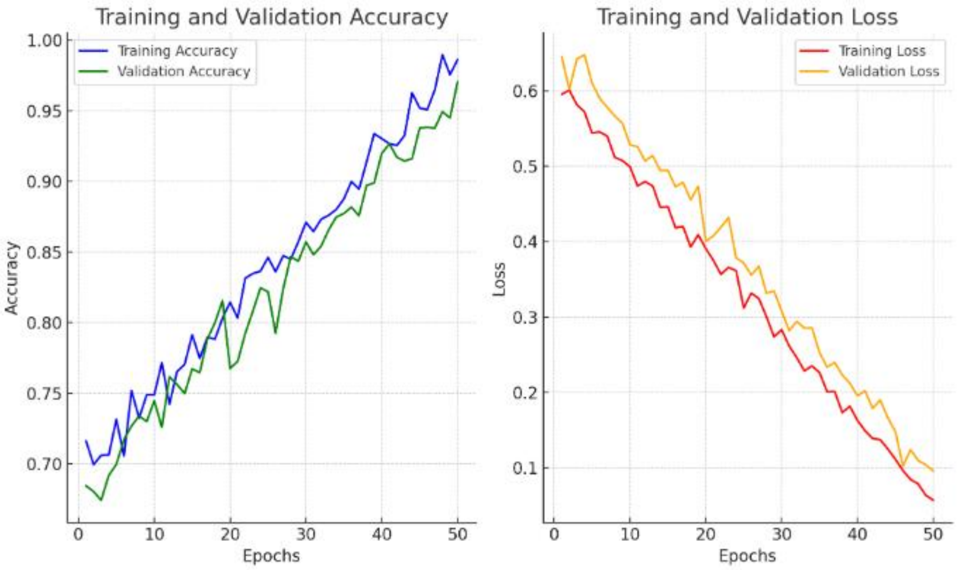

Figure 2. Training and Validation Accuracy/Loss curve

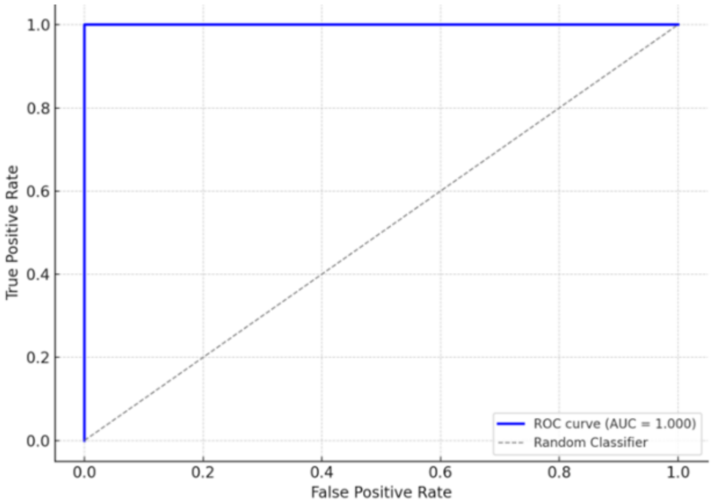

Figure 3. Receiver Operating Characteristic (ROC) curve of the CNN–LSTM model

B. Mitigation Policy Performance

Once a threat was detected, the DQN agent was responsible for selecting the most appropriate response. Over 1,000 training episodes, the agent demonstrated continuous improvement in cumulative rewards. Figure. 4 shows the average reward per episode converging after ~700 episodes, indicating effective policy learning.

Table 2 – DQN Agent Mitigation Results

Metric	Value
Avg. Reward per Episode	+23.6
Successful Mitigations	94.1%
False Isolation Rate	2.8%
Average Response Time (ms)	148

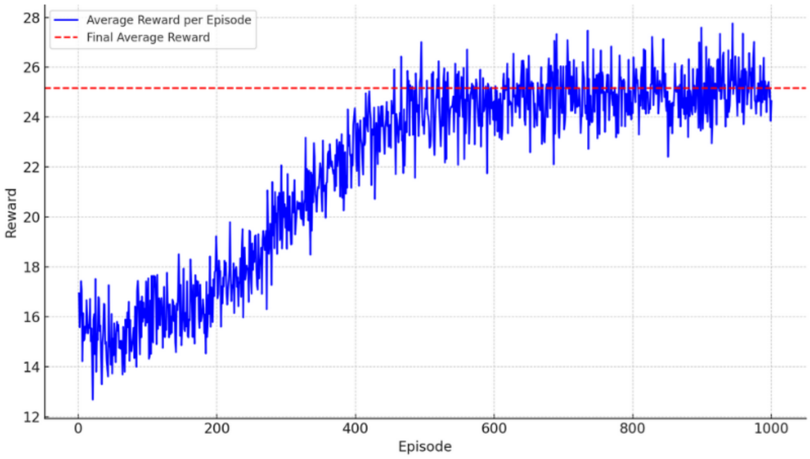

Figure 4. Average DQN reward per episode over 1000 training episodes

The agent successfully avoided unnecessary disruptions (low false isolation rate) while maintaining service availability. The average response time of 148 ms is suitable for real-time smart city environments.

C. End-to-End System Evaluation

In a combined simulation scenario, the full framework (CNN–LSTM + DQN + Blockchain) was tested for its response pipeline under simulated attack bursts. The system was capable of detecting, classifying, and responding to most threats in under 250 milliseconds, including blockchain logging overhead.

Additionally, trust scores of IoT nodes dynamically adjusted based on their behavior and the mitigation decisions applied, illustrating the system's adaptive trust enforcement capability.

D. Comparative Analysis

The proposed model was benchmarked against two baseline approaches:

1. Traditional CNN-only model (no temporal modeling)
2. CNN–LSTM with static rule-based mitigation

Table 3 – Comparative Performance

Model	**Accuracy (%)**	**F1-Score (%)**	**Response Time (ms)**	**False Isolation (%)**
CNN Only + Rule-based	91.5	89.6	210	6.4
CNN–LSTM + Rule-based	95.2	93.8	195	4.2
CNN–LSTM + DQN (Proposed)	97.8	97.3	148	2.8

The proposed approach outperforms both baselines in terms of accuracy, mitigation efficiency, and reliability. The use of adaptive RL allows the system to learn from past outcomes and make smarter decisions than static rule engines.

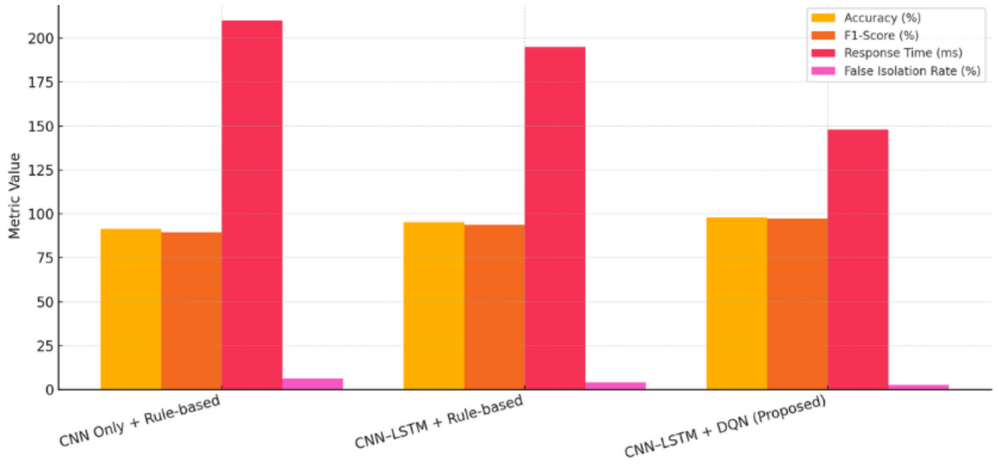

Figure 5. Model Comparison: Baseline vs. Proposed System

CONCLUSION

This paper proposed a dynamic and smart security model to identify and act on cyber threats on IoT Smart cities. The system uses a combination of deep learning, reinforcement learning and blockchain to form a dynamic and real-time solution. The CNN LSTM model has been able to find both spatial and temporal trends in traffic network patterns and gave a high performance on the BoT-IoT dataset with AUC 0.992 and F1-score 97.3%. The Deep Q-Network (DQN) agent also enhances the system in the decision-making of the best mitigation action that should be taken, according to actual risk, device mistrust, and the significance of the service. This minimizes false alarms and maintains response time low. Hyperledger and IPFS have been used as the foundation of the blockchain layer where all the events and decisions are logged securely in a tamper-proof and auditable manner. In comparison to the traditional rule-based systems, the approach is more accurate, responds faster, and is also highly adaptable even to complex attack situations. It also provides solutions to some of the major difficulties of IoT security namely management of large data, real-time detection, and trust in the distributed environment. Future work, to secure data privacy in smart city domains, we will expand the current system using federated learning. Another idea we want to investigate are zero-trust architectures, multi-agent reinforcement learning, and edge computing approaches in order to be able to scale the system and avoid excessive reliance on centralized processing. Lastly, we will work with the city authorities to use it as a system in a real smart city setting and to measure its effectiveness.

REFERENCES

1. Chakrabarty, S., & Engels, D. W. (2020). Secure smart cities framework using IoT and AI. 2020 IEEE Global Conference on Internet of Things (GCIoT), 1–6. https://ieeexplore.ieee.org/document/9345912
2. Ning, H., Ding, J., Lifelo, Z., & Dhelim, S. (2024). Artificial intelligence-enabled metaverse for sustainable smart cities. Electronics, 13(24), 4874. https://www.mdpi.com/2079-9292/13/24/4874
3. Gwassi, O. A. H., Uçan, O. N., & Navarro, E. A. (2024). Cyber-XAI-Block: A cyber threat detection and risk assessment framework using XAI and blockchain. Multimedia Tools and Applications. Advance online publication. https://doi.org/10.1007/s11042-024-20059-4
4. Rahman, A., Kundu, D., & Debnath, T. (2024). Blockchain-based AI methods for managing industrial IoT. arXiv preprint, arXiv:2405.12550. https://arxiv.org/pdf/2405.12550
5. Zuo, Y. (2024). Exploring the synergy: AI enhancing blockchain, blockchain empowering AI, and their convergence across IoT applications. IEEE Internet of Things Journal. Advance online publication. https://ieeexplore.ieee.org/document/10769427
6. Gospodinov, G., Gotsev, L., & Ristovska, T. (2025). Cybersecurity in smart cities: Emerging threats and defence strategies. Environment. Technology. Resources. Proceedings of the 16th International Scientific and Practical Conference, Volume V, 103–110. https://doi.org/10.17770/etr2025vol5.8496

7. Feng, C., Al-Nussairi, A. K. J., & Chyad, M. H. (2025). AI-powered blockchain framework for smart home cybersecurity. Scientific Reports. Advance online publication. https://www.nature.com/articles/s41598-025-03146-w
8. Tyagi, A. K. (2024). Blockchain–Artificial intelligence-based secured solutions for smart environment. In S. Khan, A. El-Moursy, & A. Nayyar (Eds.), Digital twin and blockchain for smart cities (Chapter 23, pp. 421–442). Wiley. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394303564.ch23
9. Sharma, B., Gupta, M., & Jeon, G. (2024). Smart Cities: Blockchain, AI, and Advanced Computing. Springer. ISBN: 9789819939784. https://link.springer.com/book/10.1007/978-981-99-3979-1
10. Rahim, F. A., Azmi, N. N., & Hassan, N. H. (2024). AI safety and cyber resilience in IoT-blockchain urban systems. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5180648
11. Priyadarshini, I. Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated Learning and Split Learning. Big Data Cogn. Comput. 2024, 8, 21.
12. Institute for Defense & Business. What Are the Cybersecurity Risks for Smart Cities? Available online: https://www.idb.org/what-are-the-cybersecurity-risks-for-smart-cities/ (accessed on 17 March 2025).
13. Security and Compliance in 5G and AI-Powered Edge Networks | Deloitte Global. Available online: https://www.deloitte.com/global/en/services/consulting-risk/perspectives/security-compliance-in-5g-ai powered-edge-networks.html (accessed on 17 March 2025).
14. How 5G Technology Affects Cybersecurity: Looking to the Future | UpGuard. Available online: https://www.upguard.com/blog/how-5g-technology-affects-cybersecurity (accessed on 17 March 2025).
15. Mirza, N.; Yunis, M.; Khalil, A.; Mirza, N. Towards a Conceptual Framework for AI-Driven Anomaly Detection in Smart City IoT Networks for Enhanced Cybersecurity. J. Innov. Knowl. 2024, 9, 100601.
16. Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects | Mesopotamian Journal of CyberSecurity. Available online: https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/14 (accessed on 17 March 2025).
17. USA; Aluwala, A. AI-Driven Anomaly Detection in Network Monitoring Techniques and Tools. J. Artif. Intell. Cloud Comput.2024, 1–6.
18. Babu, C.V.S.; Simon, P.A. Adaptive AI for Dynamic Cybersecurity Systems: Enhancing Protection in a Rapidly Evolving Digital Landscap. Available online: https://www.igi-global.com/gateway/chapter/337688 (accessed on 17 March 2025).
19. Iqbal, U., Sharif, K., Li, F., Latif, S., Karim, A., & Yu, S. (2018). BoT-IoT: A new IoT botnet dataset for machine learning-based network intrusion detection systems. *Proceedings of the International Conference on Artificial Intelligence and Security (ICAIS)*. University of New South Wales Canberra. Available at: https://research.unsw.edu.au/projects/bot-iot-dataset
20. Kuraku, D.S. Adaptive Security Framework For Iot: Utilizing AI And ML To Counteract Evolving Cyber Threats. Educ. Adm. Theory Pract. 2023, 29, 1573–1580.
21. What Is the Role of AI in Threat Detection? Available online: https://origin www.paloaltonetworks.com/cyberpedia/ai-inthreat-detection (accessed on 17 March 2025).
22. Kuguoglu, B.K.; van der Voort, H.; Janssen, M. The Giant Leap for Smart Cities: Scaling Up Smart City Artificial Intelligence of Things (AIoT) Initiatives. Sustainability 2021, 13, 12295.
23. Towards Large-Scale IoT Deployments in Smart Cities: Requirements and Challenges | SpringerLink. Available online: https://link.springer.com/chapter/10.1007/978-3-031-50514-0_6 (accessed on 17March 2025).
24. Zyrianoff, I.; Borelli, F.; Biondi, G.; Heideker, A.; Kamienski, C. Scalability of Real-Time IoT-Based Applications for Smart Cities. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp.00688–00693.
25. Abusitta, A.; Silva de Carvalho, G.H.; Abdel Wahab, O.; Halabi, T.; Fung, B.C.M.; Al Mamoori, S. Deep Learning-Enabled Anomaly Detection for IoT Systems. Internet Things 2022, 21, 100656.

AI and IoT in Smart Cities Security. Available online: https://www.truehomeprotection.com/leveraging-ai-and-iot-for-nextgeneration-security-systems-in-smart-cities/