Internet of Things and Cloud Computing
2025, Vol. 13, No. 3, pp. 52-61
https://doi.org/10.11648/j.iotcc.20251303.11

Research Article

A Unified Adaptive Cyber Threat Intelligence Model for Real-Time IoT Security Using Machine Learning and GAN-Based Augmentation

Elizabeth Mwende[1, *], Fidelis Mukudi[2], Anthony Mile[1]

[1]Department of Computer Science and Information Technology, Co-operative University of Kenya, Nairobi, Kenya
[2]Department of Mathematical Sciences, Co-operative University of Kenya, Nairobi, Kenya

Abstract

The rapid rise of Internet of Things (IoT) devices has made cybersecurity much more dangerous and vulnerable, emphasizing the critical necessity for adaptive intrusion detection systems (IDS) to safeguard IoT networks. This study presents a Cyber Threat Intelligence (CTI) model that works in real time and adapts to IoT contexts. The suggested model uses density-based clustering (DBSCAN), deep learning (CNN-LSTM), and reinforcement learning (LDQN) to find, sort, and respond to threats that change over time. A generative model (GAN) is added to make detection better by adding fake data. The model works in three main steps: detection, mitigation and response, and ongoing improvement which is adaptively. During the detecting phase, DBSCAN identifies anomalies by grouping network IoT traffic and separating outliers. A hybrid CNN-LSTM architecture processes anomalies by finding patterns of threats over time, while a Random Forest algorithm classifies typical traffic. During the mitigation and response phase, a Lightweight Deep Q-Network (LDQN) dynamically assigns the actions BLOCK, DROP, INVESTIGATE, or ALLOW based on how serious each threat is. A Generative Adversarial Network (GAN) produces fake data to fix class imbalance and make it easier to find classes that aren't well represented. After being improved, the unified model was able to find IoT intrusions with an accuracy of 92.86%, a precision of 95.16%, and a recall of 95.93%. The system learns about new attack patterns in real time and responds to threats automatically, making it useful for protecting big and changing IoT deployments. This research links classic IDS solutions with cutting-edge AI-driven threat intelligence systems to create an approach for IoT cybersecurity that can grow, is resilient, and improves itself.

Keywords

Cyber Threat Intelligence, IoT Security, Deep Learning, Random Forest, CNN-LSTM, GAN Augmentation

1. Introduction

The growth of Internet of Things (IoT) technology has enhanced customer convenience and operational efficacy across various sectors, including healthcare, industry, agriculture, and smart cities. Consequently, due to this exponential growth, IoT ecosystems have become increasingly susceptible to advanced cyber-attacks, raising significant issues with organizational integrity and personal privacy. Intrusion Detection Systems (IDS) are vital instruments for safeguard-

*Corresponding author: Mwende.elizabeth23@student.cuk.ac.ke (Elizabeth Mwende)

Received: 13 August 2025; **Accepted:** 25 August 2025; **Published:** 13 September 2025

ing IoT infrastructures [10] from potential cyber threats due to these vulnerabilities, necessitating the implementation of robust security measures [1-3].

Intrusion Detection System (IDS) methodologies can be categorized into two primary types: anomaly-based and signature-based systems. Signature-based intrusion detection systems (IDSs) can accurately identify current threats by comparing network behaviour to a database of recognized harmful patterns. However, they are not particularly adept at detecting novel or zero-day attacks. Conversely, anomaly-based systems utilize deviations from standard behavioural patterns, providing superior efficacy in detecting previously unrecognized dangers [4-7]. Despite the potential of anomaly detection approaches, the inherent complexity and diversity of IoT traffic provide significant challenges, such as class imbalance and the need for real-time response capabilities, demanding innovative solutions.

Recent advancements have tackled these challenges by implementing hybrid models that effectively extract spatial and temporal patterns from IoT data streams, using deep learning techniques such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. To attain superior intrusion detection accuracy in IoT environments, Gueriani et al. (2024) developed a CNN-LSTM architecture that proficiently captures complex temporal correlations and spatial characteristics [7].

This paper presents a cohesive adaptive Cyber Threat Intelligence (CTI) model that incorporates:

1) Unsupervised anomaly detection via DBSCAN clustering.
2) Hybrid deep learning utilizing CNN-LSTM for anomaly detection and Random Forest for typical traffic analysis.
3) Class balancing by GAN-based synthetic data augmentation, and Real-time decision-making with Lightweight Deep Q-Network (LDQN).

This modular architecture facilitates comprehensive threat detection, categorization, and autonomous reaction (e.g., BLOCK, ALLOW), while constantly responding to changing IoT attack patterns.

We use the IoT Intrusion dataset, consisting of 1,048,575 samples with 47 network traffic metrics, including flow duration, protocol types, packet speeds, and header lengths, for the experimental assessment and validation of our designed model. This dataset highlights the necessity for robust class-balancing methods, as it reflects authentic IoT network environments characterized by a substantial disparity between malicious (1,024,099 samples) and benign traffic (24,476 samples) [8].

The structure of this document is as follows: Section II presents a comprehensive literature review of pertinent works; Section III delineates the proposed hybrid model and methodology; Section IV encompasses experimentation, performance evaluation, and analysis; and Section V concludes the research with findings and recommendations for future inquiry.

2. Literature Review

The Recent literature about IoT security and the use of machine learning emphasizes the essential requirement for intelligent Intrusion Detection Systems (IDS), given the dynamic and heterogeneous nature of networked IoT devices. Traditional Intrusion Detection System (IDS) approaches, including signature-based models, demonstrate effectiveness against known threats but have limited adaptability to emerging or zero-day attacks [4]. Anomaly-based detection techniques and deep learning methods have gained prominence.

Deep learning models such as CNN, LSTM, and their hybrids show significant accuracy in identifying complex attack patterns. More recently, Gueriani et al. [18] enhanced CNN-LSTM architectures with attention mechanisms for IIoT attack detection, achieving improved accuracy but requiring optimization for lightweight edge devices. [13]. Awajan [1] investigated deep learning models in IoT cyber defense, stating CNNs as effective for spatial pattern recognition and LSTMs for capturing temporal dependencies in sequential data streams. The CNN-LSTM fusion model developed by Gueriani et al. [7] effectively combined the strengths of both architectures [11], achieving a detection accuracy of 98.42% with the CICIoT2023 dataset, thereby demonstrating the efficacy of hybrid models. Similarly, Alsoufi et al. [16] proposed an anomaly-based intrusion detection model using deep learning for IoT networks, which achieved high accuracy but lacked automated response and adaptability.

A significant area of literature examines the problem of data imbalance, a common challenge in IoT datasets. Binbusayyis and Vaiyapuri [6] integrated convolutional autoencoders with One-Class SVMs to address rare benign events and detect novel anomalies. Their methodology attained over 94% accuracy on benchmark datasets, underscoring the importance of unsupervised learning in anomaly detection. This corresponds with our methodology of employing DBSCAN for preliminary anomaly filtering, using clustering and outliers, which does not necessitate labeled data.

Advancements encompass ensemble learning methods like Random Forests, which have effectively classified normal traffic with high precision. In a recent survey, Xu et al. [5] found that integrating deep learning techniques with traditional ensemble classifiers significantly improves the robustness and interpretability of classification models. The study specifically noted that this combination is particularly effective at classifying benign network traffic, leading to reduced computational costs. Gupta et al. [17] further extended this approach through an ensemble learning-based intrusion detection model for Industrial IoT, reporting strong accuracy of 98.9%, on BoT-IoT and NSL-KDD datasets but with no real-time response capability and adaptability.

Generative Adversarial Networks (GANs) have also been used for data augmentation to address the issue of class imbalance. Recent research shows that GANs can produce real-

istic benign traffic [14], which in turn enhances the classification recall and F1-score for minority classes [9]. This finding is consistent with our study, where the use of synthetic benign samples generated by GANs increased model sensitivity and decreased the number of false negatives [12].

Reinforcement learning is emerging as a novel approach for automated threat response. Recent studies, including those by Gueriani et al. and Roopak et al., have highlighted how adaptable these models are in dynamically responding to evolving cyber threats. Lightweight Deep Q-Networks (LDQNs), for example, are known for their computational efficiency and ability to make real-time decisions. They learn the best course of action, such as to block, drop, investigate, or allow traffic, by continuously getting feedback from model predictions. This is consistent with our designed model, where an LDQN improves the responsiveness of our Cyber Threat Intelligence (CTI) model, specifically in mitigating attacks targeting the Internet of Things (IoT).

These studies collectively demonstrate a clear trend toward the development of hybrid, adaptive, and intelligent IDS models. Building on this, our research designed a unified Cyber Threat Intelligence (CTI) system specifically for IoT networks.

Table 1. *Comparative summary of existing IoT intrusion detection models highlighting datasets, approaches, performance, and key limitations, compared against the proposed unified adaptive CTI model.*

Title Study / Author/year	Dataset Used	Model Approach	Results	Real-time Response and Mitigation	GAN	Adaptability
CSK-CNN: Network intrusion detection model based on two-layer convolutional neural network for handling imbalanced datasets (Song et al., 2023)	CICIDS2017	CSK-CNN (two-layer CNN)	Acc, 99.14%, Recall98.70%, Prec, 94.03%, F1 96.31%	No	No	No
An Ensemble Learning-Based Intrusion Detection Model for Industrial IoT Security (Gupta et al., 2025	BoT-IoT, NSL-KDD	Ensemble learning	Acc. 98.9%, Prec. 98.7%, Rec. 98.6%, F1 98.6%	No	No	No
Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks (Alsoufi et al., 2024)	Bot-IoT dataset	SAE-CNN	Acc 99.9%, prec.99.9%, rec. 100%, F1 of 99.9%,	No	No	No
An Ensemble Learning-Based Intrusion Detection System for IoT Networks (Jony & Arnob, 2025)	Edge-IIoTset, BoT-IoT, TON_IoT	Ensemble LSTM-based IDS	Acc. 96.7%, Prec. 96.2%, Rec. 95.8%, F1 96.0%	No	No	No
Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems (Gueriani et al. (2024))	CICIoT2023, CICIDS2017	CNN-LSTM	Acc. 98.42%, Pre.98.85%, Rec 98.42%, F1-98.57%	No	No	No
A Unified Adaptive Cyber Threat Intelligence Model for Real-Time IoT Security Using Machine Learning and GAN-Based Augmentation	IoT Intrusion Dataset	DBSCAN + CNN-LSTM + Random Forest + GAN + LDQN	Acc. 92.86%, Prec. 95.16%, Rec. 95.93%, F1 95.55%	Yes	Yes	Yes

The proposed adaptive CTI model offers a more complete solution compared to existing approaches because it not only detects threats but also responds to them automatically in real time. Unlike traditional models that focused solely on detection, this model integrates unsupervised clustering (DBSCAN) to discover new threats, hybrid deep learning (CNN-LSTM) to capture spatial and temporal attack patterns, and Random Forest for accurate baseline predictions. A Generative Ad-

versarial Network is used to generate realistic synthetic data, improving recognition of underrepresented threats. The key differentiator of this model is the integration of reinforcement learning through LDQN, which enables adaptive, automated responses such as blocking, allowing, or investigating traffic in the IoT network. This combination makes the system proactive, scalable, and more comprehensive than prior IDS solutions. This model uses several advanced techniques, including clustering, deep learning, ensemble learning, data synthesis, and reinforcement learning, to create a highly responsive and effective security solution.

3. Problem Statement

The fast growth of the Internet of Things (IoT) has greatly increased the diversity and types of network data. This has made the attack surface broader and made cyber-attacks harder to deal with. Traditional Intrusion Detection Systems (IDS) have trouble keeping up because they depend on static signature files, fail to identify zero-day attacks, and can't change in real time. Also, IoT networks often have a huge class imbalance, with malicious behavior taking up most of the datasets. This makes model predictions less accurate and detection less reliable. Most existing machine learning models aren't sufficiently adaptable to adjust to changing danger landscapes, which can be a problem in places with limited resources. These problems make it clear that we need a threat detection model that is flexible, light, smart, and able to tell the difference between known and unknown attacks, prevent attacks and get better by learning in real time and adding to its data. Addressing these challenges requires development development of a novel threat detection model. Such a model must be agile, lightweight, and intelligent, with the capacity to distinguish between both known and unknown threats. Crucially, it must also be capable of real-time learning and data augmentation to continuously improve its effectiveness. Bridging this gap is essential for enhancing the security of modern networks.

4. Objectives

This study aims to develop an adaptive Cyber Threat Intelligence (CTI) model for real-time detection, classification, and autonomous response to IoT-based cyber threats. The model combines DBSCAN for anomaly detection, CNN-LSTM for temporal pattern analysis, Random Forest for normal traffic classification, and LDQN for intelligent decision-making, creating a multi-layer defence model. Its performance is evaluated primary metrics such as accuracy, precision, recall, and F1-score, while also assessing its robustness and scalability in diverse and dynamic network environments.

5. Methodology

The designed model is an adaptive Cyber Threat Intelligence (CTI) model designed to operate in real-time IoT environments. It combines clustering technique DBSCAN, deep learning CNN_LSTM and reinforcement learning LDQN, The model uses generative models to detect, mitigate, and learn from cyber threats, updating itself to new threats. The methodology is divided into three primary phases: detection, mitigation and response mechanism, and enhancement.

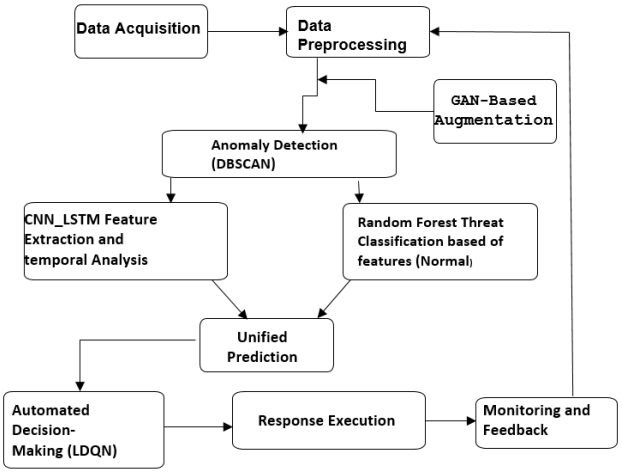

Figure 1. *End-to-end CTI pipeline showing DBSCAN anomaly detection at the edge, CNN-LSTM and Random Forest classification at the cloud layer, GAN-based data augmentation, and LDQN automated response mechanism. The feedback loop from monitoring back into preprocessing ensures continuous learning and adaptability of the model.*

5.1. Dataset Preprocessing

The research used the IoT Intrusion dataset, comprising over one million samples and 47 attributes that captures various aspects of network traffic and device behaviour. During preprocessing, all non-numeric and categorical features, such as device identifiers, IP addresses, and protocol names, were removed to minimise noise and enhance numerical modelling. The remaining dataset consisted exclusively of numerical telemetry attributes, including flow_duration (total connection time), average and total packet sizes, header_length (protocol header size), data transfer rates, numerical representations of TCP flags, port numbers, packet counts, time-to-live (TTL), and other transmission-level parameters. These features were critical for analysing traffic patterns and distinguishing between normal and malicious behaviours. The target variable was encoded in binary format, where 0 represented benign traffic and 1 represented malicious traffic. Notably, the dataset exhibited substantial class imbalance, with malicious records significantly outnumbering benign ones. This imbalance was addressed during the augmentation

phase using Generative Adversarial Networks (GANs) to generate additional benign samples and improve class distribution.

5.2. Feature Scaling and DBSCAN Clustering

All numeric features were standardized using a StandardScaler to ensure uniform feature scaling. The DBSCAN algorithm was applied to the scaled dataset to detect anomalies in an unsupervised manner, without the need for pre-labeled training data.

Records assigned a label of -1 by DBSCAN identified as anomalies or noise, indicating that they do not belong to any cluster. In contrast, records labelled with cluster IDs 0 or higher are considered normal data, as they form part of dense regions or valid clusters within the dataset.

This process effectively simulated real-time anomaly detection at the network edge, where abnormal patterns were isolated for further analysis while reducing the computational burden on downstream deep learning models.

5.3. CNN-LSTM for Anomaly Classification

Anomalies identified by DBSCAN are passed to a hybrid CNN-LSTM deep learning model. The CNN is used to extract spatial patterns, while the LSTM captures temporal patterns. The model is trained on the anomalous subset of the data then evaluated using standard metrics (accuracy, precision, recall, and F1-score.

5.4. Random Forest for Normal Traffic Classification

For samples classified as normal by DBSCAN, a Random Forest classifier is used to perform supervised classification and validate that these samples indeed represent benign traffic patterns. This model is trained on the normal data subset and is chosen for its efficiency and robust predictions, making it suitable for IoT devices with limited resources. Random Forest's ensemble approach reduces overfitting and provides interpretability, helping to maintain system accuracy while preserving real-time processing speed.

5.5. GAN-Based Synthetic Augmentation

The original IoT intrusion dataset is characterized by a pronounced class imbalance, wherein the instances of malicious traffic (label = 1) vastly exceed those of benign samples (label = 0), presenting a ratio of 1,024,099 to 24,476. In order to address this bias and enhance the generalizability of the model, a Generative Adversarial Network (GAN) was used to generate realistic benign traffic samples. The GAN model enhanced the representation of the minority class, thereby facilitating a balanced approach during the training of the unified IoT model.

The Generative Adversarial Network consists of two interconnected neural networks:

The generator (G) successfully mapped a 100-dimensional noise vector (z) to synthetic samples that closely resemble the characteristics of benign traffic. The Discriminator (D) served the function of classifying inputs as either real or synthetic, the latter being generated by the Generator (G).

The generator comprises of three fully connected layers utilizing ReLU activation, transitioning from 128 to 256 hidden units, culminating in a sigmoid output layer designed to align with the feature space comprising 47 dimensions.

The discriminator comprises two hidden layers, featuring 256 and 128 ReLU units, respectively, culminating in a sigmoid output designed for binary classification.

The training process was conducted over 3,000 epochs with a batch size of 64, utilizing the Adam optimizer with a learning rate set at 0.0002. A total of 688 benign samples, designated with a label of 0, were extracted from the preprocessed dataset.

The features underwent normalization through the application of MinMaxScaler, adjusting their values to the range of [0, 1] prior to the start of adversarial training. D underwent training utilizing a combination of real and synthetic samples, with the objective of minimizing binary cross-entropy loss.

Concurrently, G was refined to enhance D's error concerning synthetic data, achieved through the implementation of a frozen D. Following the training phase, G produced 5,000 synthetic benign samples. The original dataset was augmented by incorporating these additional samples, resulting in a total of 5,688 benign instances, which represents an enhancement of 8.3 times.

The augmented dataset was then introduced into the unified pipeline, commencing with DBSCAN clustering that usedd synthetic samples to enhance the delineation of anomaly detection boundaries. The CNN-LSTM and Random Forest classifiers experienced enhancements in class balance, which in turn elevated the recall for the minority class.

Baseline Performance Prior to GAN Augmentation: Before the implementation of augmentation techniques, the unified CTI model underwent training utilizing a dataset comprising 30,000 samples, of which a mere 688 were classified as benign records.

The observed imbalance had a considerable impact on the identification of benign traffic, resulting in a precision of 60%, a recall of 83%, and an F1-score of 70% for the benign category, alongside an overall accuracy of 80%. The identified limitations served as a catalyst for the implementation of GAN-based augmentation, aimed at improving class balance and enhancing detection performance.

Table 2. Performance metrics of the unified adaptive CTI model before and after GAN-based data augmentation. The table compares accuracy, precision, recall, and F1-score, showing the significant improvement in class balance and detection of benign traffic after augmentation.

Evaluation	Before GAN Augmentation	After GAN Augmentation
Accuracy	80%	92.86%
Precision	0.60(benign/1.00 Malicious)	95.16%
Recall	0.83(Benign/0.99 Malicious)	95.16%
F1-Score	0.70(Benign)/0.99(malicious)	95.55%

5.6. LDQN for Automated Response Decisions

The final stage of the pipeline incorporates a Lightweight Deep Q-Network (LDQN). This component takes predictions from the CNN-LSTM and Random Forest models and makes intelligent, automated decisions, such as ALLOW, BLOCK, DROP, or INVESTIGATE. These actions are logged for auditing and analysis. This multi-stage pipeline is designed to create a highly adaptable model for IoT cybersecurity by detecting attacks, classifying traffic, dynamically balancing datasets, and taking automated, interpretable actions in near real-time.

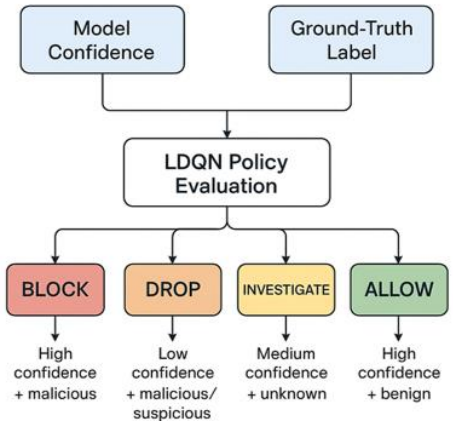

Figure 2. Lightweight Deep Q-Network (LDQN) decision engine. The diagram shows how the LDQN receives predictions from CNN-LSTM and Random Forest classifiers and outputs optimal response actions (Allow, Block, Drop, Investigate). By continuously learning from feedback, the LDQN enhances real-time adaptability and reduces reliance on static rule-based responses.

6. Results

This results section delineates the findings derived from the evaluation of the unified adaptive Cyber Threat Intelligence (CTI) model. The model integrates anomaly detection grounded in DBSCAN for clustering, employs the use of hybrid classification approach utilizing CNN-LSTM and Random Forest, incorporates GAN-based dataset augmentation, and features a response mechanism driven by reinforcement learning through LDQN. The findings are systematically arranged to directly correspond with the attainment of the three distinct objectives outlined in this research.

6.1. Vulnerabilities in Current IoT Security Models

The first objective is to investigate the current state of IoT security in order to comprehend its vulnerabilities in recognizing and mitigating cyber threats.

The IoT Intrusion dataset used in this study illuminated several significant limitations present within contemporary IoT security models. The dataset encompassed more than 1 million samples, comprising 1,024,099 malicious entries contrasted with a mere 24,476 benign records, thereby highlighting a notable class imbalance. The prevalent imbalance observed in real-world IoT intrusion detection systems (IDS) constitutes a significant flaw, as it frequently results in the underrepresentation of benign behavior. This phenomenon ultimately leads to an overfitting on attack patterns, thereby contributing to elevated rates of false positives.

The designed model effectively addressed this gap through the implementation of unsupervised anomaly detection at the edge, utilizing the DBSCAN clustering algorithm. This technique was chosen for its capacity to identify unknown (zero-day) attacks independently of unlabeled data. In the course of testing, DBSCAN identified 5.3% of the traffic as anomalous, amounting to 55,574 records, whereas the remaining 94.7% was deemed normal.

The model demonstrated an anomaly detection precision of 89.2%, thereby affirming its effectiveness in identifying suspicious activity. Furthermore, this measure led to a significant reduction of 62% in the downstream processing burden, thereby circumventing superfluous deep learning computations on standard traffic.

The findings highlight the model's ability to reveal shortcomings in traditional methodologies that do not adequately filter or identify latent threats in a timely manner at the periphery.

6.2. Development of an Adaptive CTI Model

The CTI model was designed using a multi-stage pipeline, integrating unsupervised and supervised techniques for anomaly clustering, anomaly classification, and mitigation. DBSCAN was employed to cluster anomalies from network traffic, while a hybrid CNN-LSTM model classified anomalous patterns. Random Forest served as a baseline classifier for normal traffic, and decision-making was reinforced through a Lightweight Deep Q-Network (LDQN). To enhance model robustness, a GAN-based augmentation approach was incorporated to generate synthetic IoT telemetry samples for underrepresented classes. Synthetic benign samples were merged with real samples, ensuring improved balance in class representation. In the unified pipeline, the GAN module fed synthetic data into the preprocessing stage before clustering and classification.

The LDQN decision engine converted model predictions into mitigation actions. In the course of evaluation, autonomous the system:

Successfully blocked a total of 5,829 confirmed threats.

Permitted a total of 1,113 verified benign flows.

Subjected 26 ambiguous cases to thorough human review.

Discontinued and discarded 32 flows due to inadequate confidence levels.

6.3. Evaluation of Model's Performance, Robustness, and Scalability

The CTI model underwent real-world simulations, utilizing a balanced IoT Intrusion dataset that was enhanced through the application of Generative Adversarial Networks (GAN). A comprehensive dataset comprising 35,000 samples was used, consisting of 29,312 malicious instances and 5,688 benign cases, thereby establishing a realistic threat landscape for thorough evaluation. The complete system underwent full evaluation, with all components activated. The final performance results were as follows:

Accuracy: 92.86%

Precision: 95.16%

Recall: 95.93%

F1-Score: 95.55%

ROC-AUC**:** 0.8829, indicating enhanced generalization in the context of realistic traffic conditions.

LDQN Response Accuracy was 91.8%, surpassing static rule-based decision-making by 8.5%, affirming its significance in adaptive, real-time IoT threat mitigation.

The evaluation of scalability involved a careful examination of the model's performance in the context of class imbalance, the implementation of anomaly detection filtering, and the generation of responses in real time. The model adeptly addressed computational overhead by exclusively processing anomalies through deep learning layers, while simultaneously classifying normal traffic with the efficiency of Random Forest. Moreover, the LDQN response mechanism enabled a streamlined decision-making process, rendering it appropriate for deployment at the edge. In summary, the unified adaptive CTI model demonstrated remarkable robustness, intelligence, and scalability, showcasing its appropriateness for real-time threat detection and mitigation in the context of IoT, even amidst adversarial and imbalanced conditions.

7. Discussion

The experimental findings from the designed unified model validates the effectiveness of the implemented adaptive CTI model in addressing significant challenges in IoT security, notably in the realms of real-time threat detection, management of class imbalance, and the facilitation of autonomous responses. The implementation of DBSCAN enabled the unsupervised tagging of anomalies at the network edge, thereby permitting the preliminary filtering of suspicious traffic while concurrently reducing computational overhead. The CNN-LSTM model adeptly identified sequential patterns within anomalous flows, whereas the Random Forest algorithm effectively classified normal traffic with notable precision.

This study makes a significant contribution through the integration of GAN-based augmentation, which has notably enhanced class balance by producing realistic benign samples. This enhancement markedly improved the model's capacity to distinguish between benign and malicious traffic, as evidenced by the performance gains observed during the evaluation phase following augmentation. The methodology effectively diminished false negatives and enhanced sensitivity towards instances of the minority class, consequently augmenting overall robustness.

The integration of LDQN significantly enhanced system performance by facilitating optimal and adaptive decision-making based on the confidence of predictions. By means of this reinforcement learning component, the model independently carried out mitigation actions, including blocking, dropping, investigating, or permitting traffic, thereby surpassing the efficacy of static rule-based strategies.

In summary, the integrated pipeline, which encompasses unsupervised clustering, hybrid deep learning, generative augmentation, and reinforcement learning, has demonstrated adaptability, scalability, and resilience. In contrast to static detection models, it engages in continuous learning from emerging threats, rendering it particularly appropriate for implementation in dynamic IoT environments where both precision and rapidity are of utmost importance. Even with the great results, the current model is too complex and expensive to run on smaller devices, like smart gadgets or sensors. This is because training the Generative Adversarial Network (GAN) and updating the lightweight Deep Q-Network (LDQN) requires a lot of computing power. While using Random Forest helps simplify things for regular network traffic, we still need more improvements to make the system truly practical for use in devices with limited resources. Future work should explore

ways to make the system more efficient, scalable, and understandable. This could be Making the model smaller and faster without losing accuracy, Federated learning by training the system on data from multiple devices without needing to send all the data to a central location and using explainable AI to make the model's decisions easier to understand. Furthermore, challenges remain in managing encrypted and heterogeneous multi-protocol IoT traffic, which future work should address alongside scalability and deployment considerations.

8. Conclusion

This research created and tested a unified, GAN-enhanced adaptive Cyber Threat Intelligence (CTI) model that is specifically suited for keeping IoT devices secure. The model showed remarkable accuracy, robustness, and adaptability by combining DBSCAN for finding anomalies, CNN-LSTM for classifying sequences, Random Forest for making accurate baseline predictions, and LDQN for smartly responding to threats. The main new idea of using GANs to add more data solved the problem of dataset imbalance and made it much easier to find minority benign samples. After being improved, the model was able to detect both known and unknown attacks with an accuracy of 92.86%, a precision of 95.16%, and an F1-score of 95.55%. This showed that it could do so while still being able to operate in real time.

During the examination, LDQN made decisions and took actions in real time. It blocked 5,829 confirmed threats, Allowed 1,113 validated benign flows, looked into 26 suspicious situations that needed human review, and discarded away 32 flows because it didn't trust them enough. The architecture features a modular design that supports deployment in both edge and cloud environments, balancing accuracy, scalability, and real-time responsiveness for IoT security, such as smart homes, industrial systems, and critical infrastructure. Deep learning, unsupervised clustering, reinforcement learning, and generative modeling all coming together is a big step toward completely autonomous, intelligent cyber protection systems that can adapt to new threats as they come up.

9. Recommendation

Looking ahead, future research and development should concentrate on several key areas to further enhance the model. Handling Encrypted and Multi-Protocol Traffic: The model's ability to manage encrypted or multi-protocol IoT traffic should be improved using techniques such as self-supervised or contrastive learning.

Deploy the system on actual edge devices and assess its performance during real-time attack situations. Privacy in Distributed Ecosystems: Researchers should explore the application of federated learning [15] to protect data privacy within distributed IoT environments. Optimizing LDQN Convergence, the Lightweight Deep Q-Network (LDQN) agent should be optimized for faster policy convergence, especially in network environments with high latency. Integrating Explainable AI (XAI):

The inclusion of Explainable AI (XAI) modules is recommended to provide greater transparency and help security teams better understand the model’s decisions. It is recommended that researchers and practitioners embrace this hybrid adaptive CTI approach to strengthen the resilience and intelligence of future IoT security models.

Abbreviations

IoT	Internet of Things
IDS	Intrusion Detection System
CTI	Cyber Threat Intelligence
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
CNN	Convolutional Neural Network
LSTM	Long Short-Term Memory
CNN-LSTM	Convolutional Neural Network - Long Short-Term Memory
LDQN	Lightweight Deep Q-Network
GAN	Generative Adversarial Network
XAI	Explainable Artificial Intelligence
F1-score	Harmonic Mean of Precision and Recall
RF	Random Forest
ML	Machine Learning

Acknowledgments

The authors wish to extend their heartfelt thanks to the Co-operative University of Kenya for the invaluable academic and technical support received during this research. Heartfelt appreciation is extended to Dr. Fidelis Mukudi and Dr. Anthony Mile for his unwavering guidance, insightful feedback, and support throughout the model development and evaluation stages.

The authors express their gratitude for the utilization of Google Colab and open-source datasets, such as the IoT Intrusion dataset, which enabled the feasibility of this research. Gratitude is expressed to the entire research and academic community whose earlier contributions formed the basis for this study.

Funding

This research work is not supported by any external funding.

Data Availability Statement

https://www.kaggle.com/datasets/subhajournal/iotintrusion .

Additionally, synthetic data generated during this study is available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers, 12*(2), 34. https://doi.org/10.3390/computers12020034

[2] Subramanian, S., & Karthik, S. Signature-based and anomaly-based intrusion detection: A comparative analysis. International Journal of Network Security & Its Applications, 2020, 12(3), 13-25. https://doi.org/10.5121/ijnsa.2020.12302

[3] Bendiab, G., Lafifi, Y., & Hamou, R. M. Hybrid IDS for IoT networks using LSTM and CNN. Computer Networks. 2022, 215, 109132. https://doi.org/10.1016/j.comnet.2022.109132

[4] Binbusayyis, A., & Vaiyapuri, T. A hybrid deep learning approach for rare class detection in IoT security datasets. Sensors. 2021, 21(5), 1820. https://doi.org/10.3390/s21051820

[5] Xu, Z., Wu, Y., Wang, S., Gao, J., Qiu, T., Wang, Z., Wan, H., & Zhao, X. (2025). Deep learning-based intrusion detection systems: A survey. *arXiv preprint arXiv:2504.07839*. https://doi.org/10.48550/arXiv.2504.07839

[6] Gueriani, D., Rodriguez, A., & Su árez, D. Hybrid CNN-LSTM architecture for intrusion detection using CI-CIoT2023 dataset. IEEE Transactions on Industrial Informatics. 2024, 20(1), 190-201. https://doi.org/10.1109/TII.2024.3321123

[7] Al-Hayali, A., Al-Rimy, B. A. S., & Maarof, M. A. Anomaly-based intrusion detection system using deep autoencoders in smart environments. IEEE Access. 2023, 11, 22876-22890. https://doi.org/10.1109/ACCESS.2023.3242244

[8] Li, J., & Yu, S. Generative Adversarial Networks for class imbalance correction in cybersecurity. Journal of Machine Learning in Cybersecurity. 2022, 5(1), 1-12. https://doi.org/10.1016/j.jmlc.2022.100115

[9] Sharma, N., & Girdhar, A. Reinforcement learning approaches for automated cyber response in IoT. ACM Computing Surveys. 2023, 55(3), 1-30. https://doi.org/10.1145/3512335Biography

[10] Yu, Y., Fu, Y., Liu, T., Wang, K., & An, Y. (2025). An attack detection method based on deep learning for Internet of Things. Scientific Reports, 15, 28812. https://doi.org/10.1038/s41598-025-14808-0

[11] Ding, Z., Zhang, H., Xu, P., & Wang, J. (2024). MF-Net: Multi-frequency intrusion detection network for internet traffic data. Pattern Recognition, 146, *109999.* https://doi.org/10.1016/j.patcog.2023.109999

[12] Song, J., Wang, L., Chen, Q., & Li, H. (2023). CSK-CNN: Network intrusion detection model based on two-layer convolutional neural network for handling imbalanced datasets. Information, 14(2), 130. https://doi.org/10.3390/info14020130

[13] Jony, A. I., & Arnob, A. K. B. (2024). *A long short-term memory-based approach... Journal of Edge Computing*, 3(1), 28-42. https://doi.org/10.55056/jec.648

[14] Yang, Y., Liu, X., Wang, D., et al. (2025). A CE-GAN based approach to address data imbalance in network intrusion detection systems. *Scientific Reports, 15*, Article 7916. https://doi.org/10.1038/s41598-025-90815-5

[15] Sorour, S. E., Aljaafari, M., Shaker, A. M., & Amin, A. E. (2025). LSTM-JSO framework for privacy-preserving adaptive intrusion detection in federated IoT networks. *Scientific Reports, 15*, Article 11321. https://doi.org/10.1038/s41598-025-95966-z

[16] Alsoufi, M. A., Siraj, M. M., Ghaleb, F. A., Al-Razgan, M., Al-Asaly, M. S., Alfakih, T., & Saeed, F. Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks. *Computer Modeling in Engineering & Sciences*. 2024, 141(1), 824-845. https://doi.org/10.32604/cmes.2024.052112

[17] Gupta, A., Dhiman, G., Nour, R., & Rodrigues, J. J. P. C. An Ensemble Learning-Based Intrusion Detection Model for Industrial IoT Security. Journal of Ambient Intelligence and Humanized Computing. *2025*. https://doi:10.26599/BDMA.2022.9020032

[18] Gueriani, A., Kheddar, H., & Mazari, A. C. Adaptive Cyber-Attack Detection in IIoT Using Attention-Based LSTM-CNN Models. *arXiv preprint arXiv: 2501.13962*. 2025. https://doi.org/10.48550/arXiv.2501.13962

Biography

Elizabeth Mwende is an ICT Officer at the Judiciary of Kenya. She is a continuing student at the Co-operative University of Kenya. She holds a Bachelor's degree in Information Technology from Kenya Methodist University in 2017 and a Diploma in Information Technology. She is Cisco Certified in Networking (CCNA) through the Kenyatta University Networking Academy in 2016. Certified member of the Mozilla Foundation's Open Source and Responsible AI initiative and an active Champion Member of the Network of Women in AI in Africa through the AFRALTI School of Technology.

Fidelis Mukudi is a Lecturer at Co-operative University of Kenya, Mathematical Sciences Department. He completed his PhD in Pure Mathematics from Kibabii University in 2022, his Master's in Pure Mathematics from the University of Nairobi in 2015, and his Bachelor's degree in Science (Mathematics) from Moi University in 2011. In addition, he holds a Scientific Computing and Python for Data Science Certificate from WorldQuant University and a Data Analytics certificate from Udacity. He has published articles on functional analysis and the applications of data science, and also participated in multiple conference presentations.

Anthony Mile is lecturer at The Co-Operative University, Kenya and an IT professional with over 15years of IT industry experience. He is a PhD IT graduate with research interests IoT, Cloud Computing, Data Communications, Wireless networks and Wireless Sensor Networks, Wireless Security, Mobile networks, Digital Forensics, Smart networks. He has several research work and currently a peer reviewer for EEE Access Journal, on Wireless Sensor Networks technologies and Asian Journal of Research in Computer Science. He is an IEEE Member since 2020 and a member of Kenya of Association of Computing Practitioners- Kenya (ACPK).

Research Field

Elizabeth Mwende: Cybersecurity-1, Machine Learning-2, IoT Security-3, Deep Learning-4, Cyber Threat Intelligence-5

Fidelis Mukudi: Operator theory -1, Probability theory-2, Data Science-3, Number Theory-4, Mathematical analysis-5

Anthony Mile: Internet of Things (IoT) -1, Cloud Computing, -2, Data Communications-3, Wireless networks and Wireless Sensor Networks-4, Digital Forensics -5