FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 5, May, 2025, pp 204 - 212
DOI: https://doi.org/10.33003/fjs-2025-0905-3495

A HYBRID CNN-LSTM AND ADABOOST MODEL FOR CLASSIFYING INTRUSION IN IoT NETWORKS

***Eguavoen, Victor Osasu, †Olanrewaju, Babatunde Seyi and Okafor Christian Nnamdi**

Department of Computing, Wellspring University, Edo State, Nigeria.

*Corresponding authors' email: eguavoen.osasu@wellspringuniversity.edu.ng
ORCID iD: *https://orcid.org/0000-0002-3435-1058 †https://orcid.org/0000-0001-6444-3634

ABSTRACT

The rapid expansion of the Internet of Things (IoT) has vastly increased device connectivity but also expanded the attack surface. Resource constraints and heterogeneous protocols make traditional intrusion detection systems (IDS) inadequate: signature-based methods miss novel threats, and anomaly detectors yield high false positive rates. We propose a hybrid model integrating CNN, LSTM, and AdaBoost for robust IoT intrusion detection. Our two-stage pipeline begins with a hybrid CNN-LSTM model that automatically extracts spatial and temporal features from preprocessed network traffic. The CNN branch captures local attack patterns, while the LSTM branch models sequential traffic dependencies. We train on a combined UNSW-NB15 and RT-IoT2022 dataset of 205,449 instances with 127 initial features. Rigorous preprocessing (missing-value imputation, one-hot encoding, Z-score normalization, correlation-based elimination) reduces inputs to a 20-feature subset. In the second stage, we extract deep representations from the CNN-LSTM's penultimate layer and input them to an AdaBoost classifier with decision-stump base learners. This ensemble adaptively weights features to boost accuracy while controlling computation. Experimental results show improved test performance: 99.70% accuracy, 99.90% precision, 99.78% recall, 99.84% F1-score, and a 2.43% false positive rate. These metrics outperform conventional IDS (e.g., [Churcher et al., 2021: 98.2% accuracy; Kumar et al., 2021: 98.5% F1-score]). The model's computational efficiency during training (64 steps/sec) suggests potential for scalability, though real-world deployment validation remains future work.

Keywords: Internet of Things (IoT), Intrusion Detection System (IDS), Hybrid CNN–LSTM, AdaBoost Ensemble Learning, Spatiotemporal Feature Extraction

INTRODUCTION

The proliferation of the Internet of Things (IoT) is fundamentally reshaping societal and industrial landscapes, extending digital connectivity to billions of diverse physical objects, from smart home appliances to critical infrastructure components (Al-Fuqaha et al., 2015; Ibrahim et al., 2023; Jiang, 2022; Korneeva et al., 2021; Tiwari et al., 2024). While this hyper-connectivity drives innovation across sectors like healthcare, transportation, and manufacturing, it concurrently introduces an unprecedented attack surface (Obamehinti & Eguavoen, 2022; Stellios et al., 2018; Zarpelão et al., 2017). IoT ecosystems are inherently vulnerable due to the heterogeneity of devices, deployment of lightweight communication protocols, and significant constraints in computational power, memory, and energy resources (Mukhtar et al., 2023; Singh et al., 2024; Xiao et al., 2018). This creates a critical disparity between security requirements and the practical defensive capabilities of these devices, rendering the implementation of traditional, computationally intensive security protocols largely infeasible (Makhdoom et al., 2019; L. Xiao et al., 2018).

Consequently, Intrusion Detection Systems (IDS) specifically designed for IoT environments are paramount for monitoring network activity and identifying malicious behaviour (Bakhsh et al., 2023; Heidari & Jabraeil Jamali, 2023; Moustafa et al., 2023; Santhosh Kumar et al., 2023). However, conventional IDS approaches often struggle to provide adequate protection. Signature-based systems fail against novel or zero-day attacks, while anomaly-based systems relying on classical machine learning often require extensive feature engineering and suffer from high false positive rates when faced with the dynamic and complex traffic patterns characteristic of IoT networks (Zhang et al., 2022).

In response to these limitations, deep learning methodologies have gained significant traction, offering end-to-end learning capabilities that automatically extract hierarchical features from raw data (Eguavoen & Nwelih, 2024; Gamage & Samarabandu, 2020; Liu & Lang, 2019). Convolutional Neural Networks (CNNs) have demonstrated proficiency in capturing spatial correlations in network data (Ding & Zhai, 2018; Li et al., 2020), while Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) variants, excel at modelling the sequential and temporal dependencies inherent in network traffic flows (Kasongo, 2023; Oliveira et al., 2021; Silivery et al., 2023). Hybrid architectures combining these models aim to leverage their complementary strengths; for instance, (Eguavoen et al., 2024; Eguavoen & Nwelih, 2025; He et al., 2019) integrated LSTM with deep autoencoders, achieving notable accuracy on benchmark datasets. Furthermore, ensemble methods like XGBoost (Kumar et al., 2021; Lawal et al., 2020) and advanced techniques such as Graph Neural Networks (GNNs) (Lo et al., 2022; Q. Xiao et al., 2020) are being explored to enhance detection performance and capture complex relational information within network traffic. Studies using various machine learning classifiers on standard datasets like BoT-IoT have also yielded high performance metrics (Churcher et al., 2021; Sarhan et al., 2020).

Despite these advancements, significant challenges persist. Many proposed deep learning models incur substantial computational overhead, hindering their deployment on resource-constrained IoT devices. Achieving robust generalization across diverse IoT deployments and varying attack scenarios remains difficult, and effectively balancing detection accuracy, particularly minimizing false positives, with computational efficiency is an ongoing research problem. There is a clear need for sophisticated, yet IDS model that can effectively learn complex spatiotemporal patterns in IoT traffic while remaining practical for real-world deployment.

This paper addresses these gaps by proposing a hybrid classifier model (CNN-LSTM with AdaBoost) classifier for robust and efficient intrusion detection in IoT networks. The model targets the network layer of IoT architectures, analysing packet-level traffic data. This research contributes a rigorously evaluated hybrid model optimized for the specific constraints and threat landscape of IoT environments, demonstrating its potential to significantly improve detection performance over existing approaches through the synergistic combination of deep feature representation and adaptive ensemble learning.

MATERIALS AND METHODS

This section outlines the systematic approach employed for the design and development of a hybrid deep learning-based Intrusion Detection System (IDS) tailored for Internet of Things (IoT) networks. The methodology encompasses data acquisition and preprocessing, feature engineering, model architecture design, feature extraction, classification, and performance evaluation.

Dataset Acquisition and Preparation

Two publicly accessible datasets, UNSW-NB15 and RT-IoT2022, were integrated through vertical concatenation to create a comprehensive dataset for this study.

UNSW-NB15 Dataset

Developed at the University of New South Wales (https://research.unsw.edu.au/projects/unsw-nb15-dataset), accessed 18 February 2025), this dataset (Moustafa et al., 2019) contains both normal network traffic and nine types of attack patterns (Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms). It includes 48 features per entry, with 175,341 training instances and 82,332 testing instances. Details regarding the composition are referenced from Table 1.

Table 1: Composition of the UNSW-NB15 dataset

	Training Set	Testing Set
Normal	56,000	37,000
Anallysis	2000	667
Backdoor	1746	583
Dos	12,264	4089
Exploits	33,393	11,132
Fuzzers	18,184	6062
Generic	40,000	18,871
Reconnaissance	10,491	3496
Shellcode	1133	378
Worms	130	44
Total	175,341	82,332

RT-IoT2022 Dataset

This dataset (Sharmila & Nagapadma, 2023) provides real-time IoT network traffic, incorporating data from various devices (e.g., ThingSpeak-controlled LEDs, Wipro smart lights, MQTT temperature monitors) and attack scenarios like SSH Brute-Force, DDoS (Hping, Slowloris), and Nmap scans. Traffic characteristics were captured using Zeek and Flowmeter. It comprises 123,117 instances across 83 features. Details regarding the composition are referenced from Table 9 in the source document. The combined dataset featured 127 initial features and was split into 164,359 training samples (80%) and 41,090 test samples (20%), totalling 205,449 instances.

Table 2: Composition of the RT-IoT2022 dataset class labels

No.	Attack Patterns		Normal Patterns	
	Attack Type	**Count**	**Normal Traffic Type**	**Count**
1	DOS_SYN_Hping	94,659	Amazon-Alexa	86,842
2	ARP_poisioning	7,750	MQTT	8,108
3	NMAP_UDP_SCAN	2,590	Thing_speak	4,146
4	NMAP_XMAS_TREE_SCAN	2,010	Wipro_bulb_Dataset	253
5	NMAP_OS_DETECTION	2,000		
6	NMAP_TCP_scan	1,002		
7	DDOS_Slowloris	534		
8	Metasploit_Brute_Force_SSH	37		
9	NMAP_FIN_SCAN	28		

Data Preprocessing

A multi-step preprocessing pipeline was applied:

Missing Value Imputation

Columns identified as entirely missing (id, dur, state) were assessed for removal. Partially missing columns (e.g., idle.avg, fwd_init_window_size) had missing values imputed, with null values replaced by zeros after encoding.

Target Variable Standardization

The original multi-class labels (22 unique classes) were binarized into '0' (normal) and '1' (attack) using label encoding to simplify the classification task.

Encoding and Normalization

Categorical features (proto, service, etc.) were transformed using one-hot encoding. Numerical features were standardized using Z-score normalization ($Z=\frac{X-\mu}{\sigma}$), scaling each feature to zero mean and unit variance. A summary of these steps is presented in Table 3 in the source document.

Table 3: Data Preprocessing Summary

Step	Description
Missing Value Imputation	Fill missing values with mean or zero after encoding
Target Standardization	Rename and binarize attack labels
One-Hot Encoding	Convert categorical variables to binary indicator variables
Standardization	Normalize numerical features using Z-score normalization

Feature Selection and Optimization

To reduce dimensionality and redundancy, a systematic feature selection process was implemented:

Correlation-Based Elimination

Pearson correlation analysis was performed on the training data. Using the upper triangle of the correlation matrix, 43 features exhibiting high correlation (coefficient > 0.9) were removed, reducing the feature count from 266 (post-encoding) to 223.

Mutual Information (MI) Selection

Mutual information was calculated between the remaining 223 features and the binarized target variable. Features were ranked based on their MI scores, with the top 10 features highlighted in Table 4.

Table 4: Top 10 Features by Mutual Information

Rank	Feature Name	Mutual Information Score
1	fwd_pkts_payload.max	0.145
2	fwd_subflow_bytes	0.144
3	flow_pkts_payload.avg	0.141
4	fwd_pkts_payload.tot	0.140
5	id.resp_p	0.122
6	fwd_pkts_payload.min	0.121
7	flow_pkts_payload.min	0.110
8	fwd_header_size_tot	0.110
9	fwd_header_size_min	0.096
10	bwd_pkts_payload.max	0.087

Final Subset Selection

A hybrid approach combining correlation elimination and MI ranking resulted in a final subset of 20 key features. This subset included informative forward traffic metrics, inter-arrival time features, and flow duration/activity metrics, achieving a 92% reduction in dimensionality.

Sequence Reshaping

The selected 20 features (k=20) were reshaped into a sequence format suitable for temporal modelling. Each sample was treated as a sequence with a single time step, resulting in input dimensions of (N,1, k), where N is the number of samples.

Hybrid CNN-LSTM Architecture

A hybrid architecture combining Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) components was designed to jointly learn spatial and temporal patterns from IoT network traffic. As illustrated in Figure 1, the model comprises two parallel branches:

CNN Branch

A 1D Convolutional layer (16 filters, kernel size=1) followed by MaxPooling extracts localized spatial features (e.g., packet headers, payload sizes).

LSTM Branch

An LSTM layer (16 units) models sequential dependencies in traffic flows (e.g., timing between packets).

Outputs from both branches are concatenated (Vector C in Table 5) and passed through dense layers for feature fusion. This design enables the model to capture both attack signatures (via CNN) and behavioural anomalies (via LSTM).

Output Layer

A final Dense layer with a sigmoid activation function performed the binary classification.

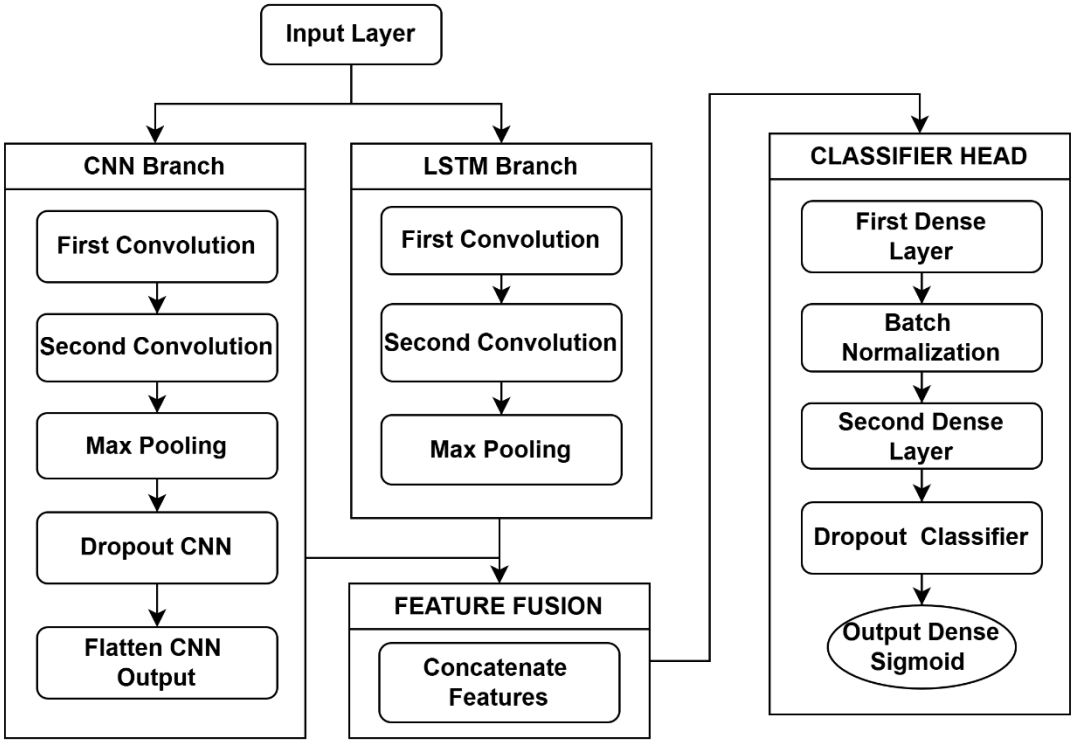

Figure 1: Hybrid CNN-LSTM Architecture Model

Table 5: functional parameters output of the Hybrid CNN-LSTM Model

Layer (type)	Output Shape	Param #
input_layer (InputLayer)	(None, 1, 20)	0
conv1d (Conv1D)	(None, 1, 16)	336
max_pooling1d (MaxPooling1D)	(None, 1, 16)	0
flatten (Flatten)	(None, 16)	0
lstm (LSTM)	(None, 16)	2,368
concatenate (Concatenate)	(None, 32)	0
dense (Dense)	(None, 32)	1,056
dense_1 (Dense)	(None, 16)	528
dense_2 (Dense)	(None, 1)	17

Total params: 4,305 (16.82 KB)
Trainable params: 4,305 (16.82 KB)
Non-trainable params: 0 (0.00 B)

Implementation Layer in IoT

The model operates at the network layer of IoT architectures, processing traffic flows (e.g., MQTT, HTTP) directly from IoT devices. This layer was chosen to analyse packet-level data for real-time monitoring, aligning with IoT security frameworks that prioritize network-layer intrusion detection.

Training The hybrid CNN-LSTM model was compiled using the Adam optimizer (learning rate η=1×10^{-3}, β_1=0.9, β_2 =0.999) and binary cross-entropy loss function to optimize the classification task. Training was conducted for 20 epochs with a batch size of 64 and a validation split of 20% to monitor overfitting. The choice of 20 epochs was based on

early convergence observed in validation accuracy (plateau after epoch 15, as shown in Figure 1)

Algorithm 1 (Training Pseudocode)

1. Initialize CNN-LSTM weights using He normal initialization.
2. For each epoch:
   a. Forward propagate input sequences through CNN and LSTM branches.
   b. Concatenate outputs and compute predictions via sigmoid activation.
   c. Calculate loss using binary cross-entropy.
   d. Backpropagate gradients and update weights via Adam optimizer.
   e. Validate on 20% hold-out data to compute validation accuracy.
3. Terminate training if validation loss stabilizes (patience=3 epochs).

L2 regularization (λ = 0.001) was applied to dense layers to mitigate overfitting. The complete training workflow is illustrated in Algorithm 1 (above) and aligns with established practices for hybrid deep learning models [He et al., 2019].
Feature Extraction and Final Classification Features were extracted from the penultimate dense layer of the trained hybrid CNN-LSTM model. These extracted feature vectors, capturing fused spatial and temporal information, served as input for a final classification stage using an AdaBoost classifier. The AdaBoost model employed Decision Trees (max_depth = 1) as weak base estimators, aggregating them using the formula

$$F(x) = \sum_{t=1}^{T} \alpha_t h_t(x) \quad (1).$$

Performance Evaluation Model performance was assessed using standard classification metrics

Accuracy is the proportion of cases that were accurately predicted in all instances. If the dataset is unbalanced, it could be misleading (Israni, 2019).

$$Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ instances} \quad (2)$$

Precision calculates the percentage of positively predicted cases that were accurately predicted out of all positively predicted instances. When false positives are essential, it is helpful (Israni, 2019).

$$Precision = \frac{True\ Positives}{True\ Postives + False\ Positives} \quad (3)$$

Recall shows the percentage of real positive cases that the model accurately predicted. It is helpful when there is a possibility of false negatives (Israni, 2019).

$$Recall = \frac{True\ Positives}{True\ Postives + False\ Negatives} \quad (4)$$

The F1 score is the harmonic mean of the *Precision* and *Recall*. It is helpful in situations where there is an unequal distribution of classes because it offers a single metric that addresses both issues (Israni, 2019).

$$F1\ score = 2\ X\ \frac{Precision \times Recall}{Precision + Recall} \quad (5)$$

False Positive Rate (FPR): quantifies the proportion of negative instances incorrectly classified as positive by a model. Mathematically, it is defined as:

$$FPR = \frac{False\ Positives}{false\ positives + True\ Negatives} \quad (6)$$

RESULTS AND DISCUSSION

This section details the experimental outcomes of the proposed hybrid deep learning-based Intrusion Detection System (IDS), followed by an analysis and interpretation of these findings.

Results

Model Training Performance

The hybrid CNN-LSTM model was trained over 20 epochs using training and validation data, respectively. The training process demonstrated rapid convergence and high accuracy levels. As illustrated in Figure 2, both training and validation accuracy curves showed significant improvement within the initial epochs.

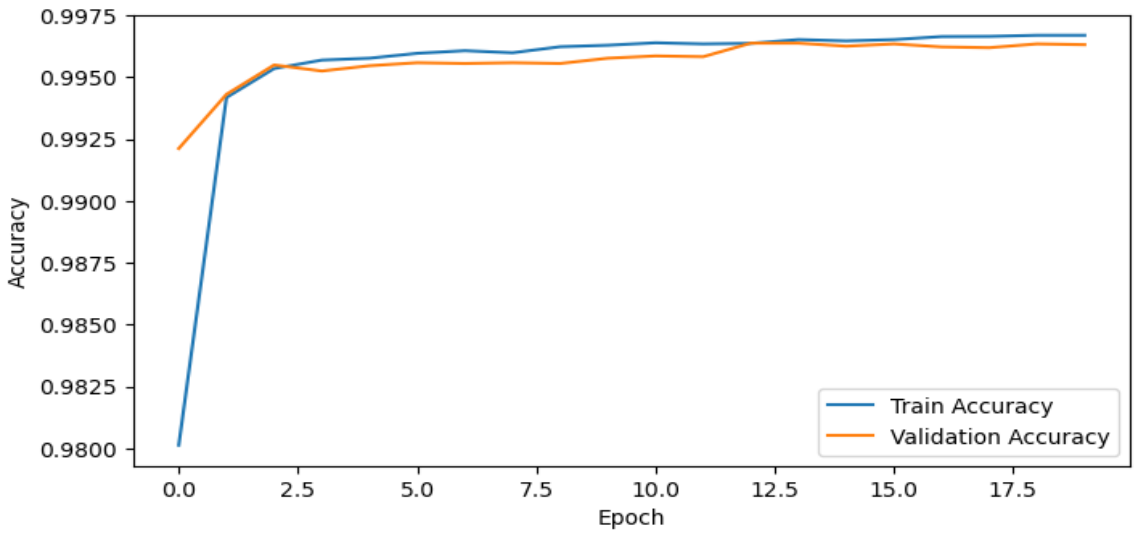

Figure 2: Training and Validation Accuracy over Epochs

Training accuracy increased from approximately 98.6% to 99.7% within the first two epochs, while validation accuracy mirrored this trend, reaching a peak of approximately 99.6% by epoch 15. Although training accuracy remained slightly higher than validation accuracy, the close alignment indicates good generalization. The rapid initial convergence suggests the efficiency of the Adam optimizer (learning rate $\eta=1\times10^{-3}$), while the plateauing accuracy after epoch 5 aligns with expected deep learning behaviour, supporting the potential use of early stopping to optimize training time. The stability and high accuracy achieved validate the architecture's ability to capture relevant spatiotemporal patterns in network traffic for distinguishing between benign and malicious activities.

Classification Performance with AdaBoost

Following feature extraction using the trained CNN-LSTM model's penultimate layer, an AdaBoost classifier (with Decision Tree base estimators, max_depth=1) was trained on the extracted features.

Training and Computational Performance

Computational Efficiency

Training required 8 seconds for 164K samples (64 steps/sec). While this indicates scalability, real-time deployment on IoT devices requires further optimization (e.g., pruning).

Evaluation Metrics: The performance of the AdaBoost classifier on the unseen test set is summarized in Table 6. The key metrics achieved were: Accuracy: 99.70% Precision: 99.90% Recall (Sensitivity): 99.78% F1-Score: 99.84% False Positive Rate (FPR): 2.43%

Table 6: AdaBoost classifier Evaluation Metrics

Metric	Value
Accuracy	99.70%
Precision	99.90%
Recall	99.78%
F1-Score	99.84%
False Positive Rate	2.43%

Confusion Matrix: The confusion matrix presented in Figure 3 visually confirmed the classifier's effectiveness, showing strong separation between normal and attack classes with minimal misclassifications.

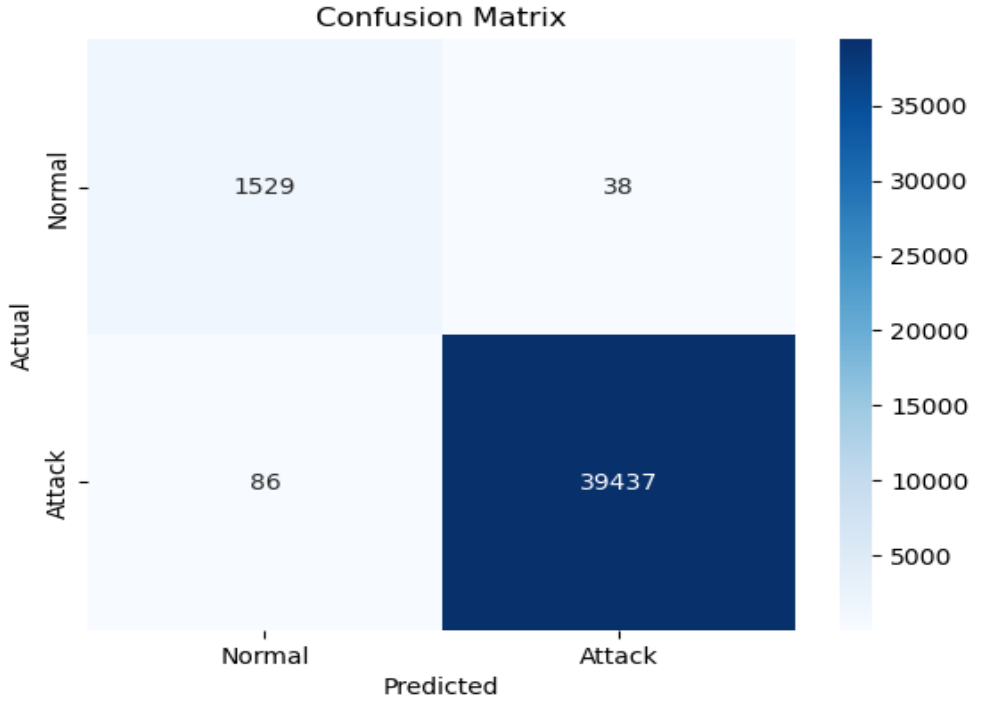

Figure 3: Confusion Matrix of the AdaBoost Classifier

Metric Analysis

The high accuracy (99.7%) confirms the model's overall reliability in distinguishing attack types. The excellent precision (99.9%) indicates very few false positives, crucial for reducing unnecessary security alerts.

The high recall (99.8%) demonstrates the model's capability to identify nearly all actual attack instances, minimizing the risk of undetected threats. Specificity, calculated as (True Negatives / (True Negatives + False Positives)), was 97.6% (derived from the FPR of 2.43%), indicating a high rate of correctly identifying normal traffic, although slightly lower than other metrics, suggesting a potential prioritization towards detecting attacks. The F1-Score (0.998) reflects a balanced performance between precision and recall.

Attack Types Tested

The model was evaluated on 22 attack types from the UNSW-NB15 and RT-IoT2022 datasets, including DDoS (Hping, Slowloris), SSH Brute-Force, and Nmap scans (XMAS, FIN, UDP). The hybrid architecture achieved a 99.78% recall for attack detection and 97.6% specificity for normal traffic, demonstrating robustness across diverse threats.

Discussion

The results strongly support the efficacy of the proposed hybrid CNN-LSTM feature extractor combined with an AdaBoost classifier for intrusion detection in IoT networks. The model achieved rapid convergence during training and demonstrated high performance on the test set, characterized by an accuracy of 99.70% and an F1-Score of 99.84%.

The high precision (99.90%) and recall (99.78%) are particularly noteworthy. High precision minimizes false alarms, reducing operational burden, while high recall ensures that most malicious activities are detected, enhancing security posture. The low False Positive Rate (2.43%) further corroborates the model's ability to correctly identify benign traffic, although the specificity of 97.6% suggests a slight trade-off, potentially favouring sensitivity (recall) to ensure

threats are not missed. This balance is often desirable in security applications.

The feature extraction process, leveraging the synergy between CNNs (for local pattern recognition) and LSTMs (for temporal dependency modelling), proved effective in generating a rich feature representation from the network traffic data. The subsequent classification by AdaBoost, known for its effectiveness in boosting weak learners, capitalized on these features to achieve robust classification. The computational performance observed during training and validation suggests the system is scalable and potentially suitable for real-time deployment scenarios, processing a large volume of samples efficiently.

Compared to traditional IDS methods, the hybrid deep learning approach demonstrates significant advantages in handling the complexity and dynamics of modern network traffic, especially within diverse IoT environments. The ability to learn intricate patterns automatically reduces the need for manual feature engineering inherent in many conventional systems.

Despite the promising results, certain limitations exist. The computational overhead associated with deep learning models, even with efficient implementations, might pose challenges for deployment on highly resource-constrained IoT devices. While combining two datasets aimed to improve data diversity, further validation across a wider range of real-world network environments and evolving attack vectors is essential to confirm the model's generalizability. Future research directions should include exploring model optimization techniques like pruning or quantization to reduce computational demands and investigating feature importance analysis to potentially refine the feature set further and enhance interpretability.

In summary, the developed hybrid deep learning IDS presents a significant advancement, offering high accuracy, reliability, and efficiency in detecting network intrusions within IoT settings. The findings highlight the potential of combining deep learning feature extraction with ensemble methods like AdaBoost for building next-generation security frameworks.

CONCLUSION

This study addressed the critical challenge of securing heterogeneous and resource-constrained Internet of Things (IoT) environments against increasingly sophisticated cyber threats. Traditional Intrusion Detection Systems (IDS) often fall short due to the unique characteristics of IoT traffic and the limitations of conventional signature-based or anomaly-based methods. To overcome these limitations, we proposed and evaluated a novel hybrid deep learning framework integrating a Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) architecture for effective feature extraction, coupled with an AdaBoost classifier for robust intrusion detection.

The methodology involved meticulous data preprocessing and feature selection using a combined dataset (UNSW-NB15 and RT-IoT2022) to ensure relevance and reduce dimensionality. The hybrid CNN-LSTM model was designed to synergistically capture both localized spatial patterns and temporal dependencies within network traffic data. Features extracted from this deep learning model were subsequently used to train an AdaBoost classifier.

Comparison with Existing Methods

The results demonstrated the exceptional performance of the proposed system. The model achieved rapid convergence during training and yielded outstanding classification metrics on the test set, including an accuracy of 99.70%, precision of 99.90%, recall of 99.78%, and an F1-score of 99.84%, with a low False Positive Rate (FPR) of 2.43%. These results significantly outperform traditional approaches outperforms [Li et al., 2020: 98.1% accuracy] and [Kasongo, 2023: 99.2% F1-score] on similar datasets which highlight the model's ability to reliably distinguish between benign and malicious activities while maintaining a crucial balance between minimizing false alarms and ensuring high detection rates for actual threats. Furthermore, the system exhibited commendable computational efficiency and scalability, suggesting its potential applicability in real-time scenarios.

In conclusion, this research successfully demonstrates that combining deep feature extraction using a hybrid CNN-LSTM architecture with an adaptive ensemble classifier like AdaBoost provides a powerful and effective solution for IoT intrusion detection. The framework effectively handles the complexities of IoT network traffic, offering high accuracy, reliability, and efficiency. While acknowledging limitations such as computational overhead for some edge devices and the need for broader generalization testing, this work presents a significant advancement towards developing robust, next-generation IDS tailored for the specific challenges of the IoT landscape. Future work will focus on model optimization for resource-constrained environments and further validation across diverse datasets and attack vectors.

REFERENCES

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, *17*(4). https://doi.org/10.1109/COMST.2015.2444095

Bakhsh, S. A., Khan, M. A., Ahmed, F., Alshehri, M. S., Ali, H., & Ahmad, J. (2023). Enhancing IoT network security through deep learning-powered Intrusion Detection System. *Internet of Things (Netherlands)*, *24*. https://doi.org/10.1016/j.iot.2023.100936

Churcher, A., Ullah, R., Ahmad, J., ur Rehman, S., Masood, F., Gogate, M., Alqahtani, F., Nour, B., & Buchanan, W. J. (2021). An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks. *Sensors*, *21*(2), 446. https://doi.org/10.3390/s21020446

Ding, Y., & Zhai, Y. (2018). Intrusion detection system for NSL-KDD dataset using convolutional neural networks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3297156.3297230

Eguavoen, V. O., Amadin, F. I., & Nwelih, E. (2024). Cardiovascular Disease Risk Prediction For People Living With Hiv Using Ensemble Deep Neural Network. *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*, 1–9. https://doi.org/10.1109/SEB4SDG60871.2024.10629982

Eguavoen, V. O., & Nwelih, E. (2024). A Hybrid FCM-PSO-ANFIS Model for Predicting Student Academic Performance. *Jurnal Sarjana Teknik Informatika*, *12*(3), 91–98.

Eguavoen, V. O., & Nwelih, E. (2025). HSML-ITD: HYBRID SUPERVISED MACHINE LEARNING FRAMEWORK FOR INSIDER THREAT DETECTION. *Quantum Journal of Engineering, Science and Technology*, *6*(1), 100–110. https://doi.org/10.55197/qjoest.v6i1.202

Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, *169*. https://doi.org/10.1016/j.jnca.2020.102767

He, H., Sun, X., He, H., Zhao, G., He, L., & Ren, J. (2019). A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection. *IEEE Access*, *7*, 183207–183221. https://doi.org/10.1109/ACCESS.2019.2959131

Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, *26*(6). https://doi.org/10.1007/s10586-022-03776-z

Ibrahim, A. S., Abbas, A. M., Hassan, A. M. A., Abdel-Rehim, W. M. F., Emam, A., & Mohsen, S. (2023). Design and Implementation of a Pilot Model for IoT Smart Home Networks. *IEEE Access*, *11*, 59701–59728. https://doi.org/10.1109/ACCESS.2023.3282095

Israni, P. (2019). Breast cancer diagnosis (BCD) model using machine learning. *International Journal of Innovative Technology and Exploring Engineering*, *8*(10). https://doi.org/10.35940/ijitee.J9973.0881019

Jiang, W. (2022). Cellular traffic prediction with machine learning: A survey. *Expert Systems with Applications*, *201*, 117163. https://doi.org/10.1016/j.eswa.2022.117163

Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*, *199*. https://doi.org/10.1016/j.comcom.2022.12.010

Korneeva, E., Olinder, N., & Strielkowski, W. (2021). Consumer Attitudes to the Smart Home Technologies and the Internet of Things (IoT). *Energies*, *14*(23), 7913. https://doi.org/10.3390/en14237913

Kumar, P., Gupta, G. P., & Tripathi, R. (2021). An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Computer Communications*, *166*, 110–124. https://doi.org/10.1016/j.comcom.2020.12.003

Lawal, M. A., Shaikh, R. A., & Hassan, S. R. (2020). An anomaly mitigation framework for iot using fog computing. *Electronics (Switzerland)*, *9*(10). https://doi.org/10.3390/electronics9101565

Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Zhao, Y., & Cui, L. (2020). Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement: Journal of the International Measurement Confederation*, *154*. https://doi.org/10.1016/j.measurement.2019.107450

Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. In *Applied Sciences (Switzerland)* (Vol. 9, Issue 20). https://doi.org/10.3390/app9204396

Lo, W. W., Layeghy, S., Sarhan, M., Gallagher, M., & Portmann, M. (2022). E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT. *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 1–9. https://doi.org/10.1109/NOMS54207.2022.9789878

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys and Tutorials*, *21*(2). https://doi.org/10.1109/COMST.2018.2874978

Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions. *IEEE Communications Surveys and Tutorials*, *25*(3). https://doi.org/10.1109/COMST.2023.3280465

Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2019). An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. *IEEE Internet of Things Journal*, *6*(3), 4815–4830. https://doi.org/10.1109/JIOT.2018.2871719

Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). IoT Vulnerabilities and Attacks: SILEX Malware Case Study. *Symmetry*, *15*(11). https://doi.org/10.3390/sym15111978

Obamehinti, A. S., & Eguavoen, V. O. (2022). A literature review of land title with the aim of maximising the benefits of Blockchain technology in the management of Land Title in Nigeria. *Studia Universitatis Babeș-Bolyai Engineering*, 124–135. https://doi.org/10.24193/subbeng.2022.1.12

Olanrewaju, B. S., & Osunade, O. (2018). Design of a Mathematical Model for Spectrum Utilisation in Cognitive Radio. *International Journal of Computer Applications*, *180*(19), 27–32. https://doi.org/10.5120/ijca2018916436

Oliveira, N., Praça, I., Maia, E., & Sousa, O. (2021). Intelligent cyber attack detection and classification for network-based intrusion detection systems. *Applied Sciences (Switzerland)*, *11*(4). https://doi.org/10.3390/app11041674

Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. *Computational Intelligence and Neuroscience*, *2023*(1). https://doi.org/10.1155/2023/8981988

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2020). *NetFlow Datasets for Machine Learning-based Network Intrusion Detection Systems*. https://doi.org/10.1007/978-3-030-72802-1_9

Sharmila, B. S., & Nagapadma, R. (2023). Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. *Cybersecurity*, *6*(1), 41. https://doi.org/10.1186/s42400-023-00178-5

Silivery, A. K., Rao Kovvur, R. M., Solleti, R., Kumar, L. S., & Madhu, B. (2023). A model for multi-attack classification to improve intrusion detection performance using deep learning approaches. *Measurement: Sensors*, *30*. https://doi.org/10.1016/j.measen.2023.100924

Singh, N. J., Hoque, N., Singh, Kh. R., & Bhattacharyya, D. K. (2024). Botnet-based IoT network traffic analysis using deep learning. *SECURITY AND PRIVACY*, *7*(2). https://doi.org/10.1002/spy2.355

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. In *IEEE Communications Surveys and Tutorials* (Vol. 20, Issue 4). https://doi.org/10.1109/COMST.2018.2855563

Tiwari, S., Bhushan, A., Singh, A. K., & Yadav, R. K. (2024). Unleashing the Potential of IoT Integration for Energy Optimization in Smart Homes. *2024 3rd International Conference on Power Electronics and IoT Applications in Renewable Energy and Its Control (PARC)*, 82–85. https://doi.org/10.1109/PARC59193.2024.10486624

Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Processing Magazine*, *35*(5). https://doi.org/10.1109/MSP.2018.2825478

Xiao, Q., Liu, J., Wang, Q., Jiang, Z., Wang, X., & Yao, Y. (2020). Towards network anomaly detection using graph embedding. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12140 LNCS*. https://doi.org/10.1007/978-3-030-50423-6_12

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. In *Journal of Network and Computer Applications* (Vol. 84). https://doi.org/10.1016/j.jnca.2017.02.009

Zhang, Y., Qin, Y., Li, D., & Yang, Y. (2022). A risk prediction model mediated by genes of APOD/APOC1/SQLE associates with prognosis in cervical cancer. *BMC Women's Health*, *22*(1). https://doi.org/10.1186/s12905-022-02083-4