Electronics, Communications, and Computing Summit
Vol. 2, No. 4, Oct - Dec 2024, pp. 65-71
ISSN: 3107-8222, DOI: https://doi.org/10.17051/ECC/02.04.08

Cross-Layer AI Models for Intrusion Detection in Cloud-Integrated IoT Networks

M. Sathish Kumar

Assistant professor Excel Engineering college Namakkal, Email:kmsankarsathish@gmail.com

Article Info

Article history:

Received : 18.10.2024
Revised : 20.11.2024
Accepted : 22.12.2024

Keywords:

Intrusion Detection System,
IoT Security,
Cross-Layer Design,
Cloud Computing,
Artificial Intelligence,
CNN-LSTM,
Threat Detection

ABSTRACT

This article attempts to capture the current security issues facing cloud-integrated Internet of Things (IoT) devices and suggests an innovative cross-layer intrusion detection system (IDS) which would be fuelled by artificial intelligence (AI). The aim is at improving the detection of threats by using deep learning models to generate and interconnect characteristics at application, transport and network layers, thus detecting a complex multi vector attacks that are usually overlooked by traditional IDS means. The new framework uses rather lightweight data collection agents distributed in the protocol stack, and strips statistical and behavioral characteristics. A hybrid neural network model that incorporates Convolutional Neural Network (CNN) to extrapolate the spatial information and Long Short-Term Memory (LSTM) of the temporal information is used to classify the malicious activities. Training and testing the system on BoT-IoT and TON_IoT datasets allows to reach 98.7 percent accuracy and F1-score of 0.96 with great exceeding of baseline models. Experiments indicate that the cross-layer CNN-LSTM system is a lot better compared to single-layer and traditional machine learning benchmarks. The architecture also exhibits resiliency traits on minimizing false positive rates and efficacy on several categories of threats like DDoS, reconnaissance and information theft. The current piece of work constitutes the potential of cross-layer AI-driven IDS in improving the situations awareness, security of distributed IoT infrastructures, and resilient outcomes of security operations in the cloud-edge environment.

1. INTRODUCTION

The Internet of Things (IoT) growth in the most critical areas, including smart homes, industrial control systems, healthcare monitoring, and smart cities, has introduced a world of complex cloud-integrated IoT ecosystems. These platforms access cloud infrastructures to do real-time analytics of data, data storage, and service orchestration. But the devices heterogeneity, the lack of computational power and the open communication APIs place them at a high risk of a large variety of cyberattacks, such as the Distributed Denial-of-Service (DDoS), spoofing, botnet infection, and exfiltration of data. The most common types of IDS Traditional intrusion detection systems (IDS) perform single-layer traffic analysis usually at the network or transports level and thus fail to capture multi-vectors, sophisticated attacks that take advantage of cross-layer phenomena. Besides, a large number of the current AI-driven IDS-based solutions do not scale well in terms of protocol-level feature-level dependencies in the multi-layered architecture or adapt to cloud enabled IoT networks that dynamically change. These constraints impair the possibility of delivering precise, real-time response and identification of threats. This study proposes a Cross-Layer Intrusion Detection System (CL-IDS) based on a hybrid deep learning system with a combination of a Convolutional Neural Network (CNN), deep learning (DL) as well as Long Short-Term Memory (LSTM) networks. The framework suggested helps to aggregate statistical and behavioral properties on the application, transport, and network layers so that more advanced attack patterns could be observed and detected without being recognized using a traditional IDS. Benchmark datasets such as BoT-IoT and TON_IoT are used to assess and train the system with a high accuracy and robustness level. Recent literature on states the importance of such cross-layer and AI combined security designs to combat such threats emerging in heterogeneous internet of things spaces [1].

2. RELATED WORK

Rule-based heuristics or shallow learning models like decision trees, support vector machine (SVM) and k-nearest neighbors (KNN) have been the commonly used models in Intrusion Detection Systems (IDS) in the context of IoT. Although these

techniques are lightweight at a computational perimeter level, they are not usually generalizable and have a huge number of false positives, especially in dynamic and heterogeneous IoT surroundings. To address these drawbacks, recent studies also suggest adoption of deep learning methods mainly in Convolutional Neural Networks (CNNs), Autoencoders, and Recurrent Neural Networks (RNNs) in feature learning and anomaly detection. Nevertheless, currently most deep learning-based IDS methods only look at one protocol layer, typically traffic records or payload data in application layer. As the example, Li et al. [1] created an IDS using CNN, which is focused on DDoS detection on MQTT traffic, but did not have the features in the transport- and network-layers to capture cross-layer correlations. At the same time, Keshk et al. [2] presented BoT-IoT dataset and used simple ML classifiers but did not regard the possibility of real-time running in restricted conditions. Such constraints direct to an important gap: present IDS frameworks fail to combine the abilities of various layers by integrating the features in gatherings. This gap is important to discover advanced, multi-vector assaults that take benefit of their interdependence across the layers of protocols. This concern has been answered in the current work through the development of a cross-layer AI architecture that combines a statistically measurable concept with a behaviorally measurable approach at the application, transport, and network level to facilitate resilient and real-time intrusion detection within the IoT IoT cloud-assisted ecosystem.

3. System Architecture

3.1 Cross-Layer Data Collection

Cross-Layer Intrusion Detection System (CL-IDS) proposed has multi-layered feature extraction that maximizes the accuracy and robustness of the detection operations across the wide range of IoT environments. Lightweight, resource-constrained agents are compiled at both IoT gateways and cloud-based endpoint to discover features at three distinct protocol layers, as illustrated in Figure 1:

- Application Layer: Packet size distribution, command frequency and payload entropy are computed in order to extract high-level patterns and anomalies in usage.
- The Transport Layer: Sensitive transport-level activities are observed by behavioral parameters such as the rate of port scanning, SYN/ACK ratio and the length of a session.
- Network Layer: At this level, only low-resource variables like IP address entropy, variation of hop counts, volume distribution of traffic are gathered in order to identify scanning, spoofing and flooding attacks.

Those agents pre-process and aggregate the obtained data to construct a single feature vector and allow scalable real-time analysis without an excessive computation burden. The CL-IDS architecture therefore facilitates the comprehensive intrusion detecting by monitoring application, transport, and network layer at the same time.

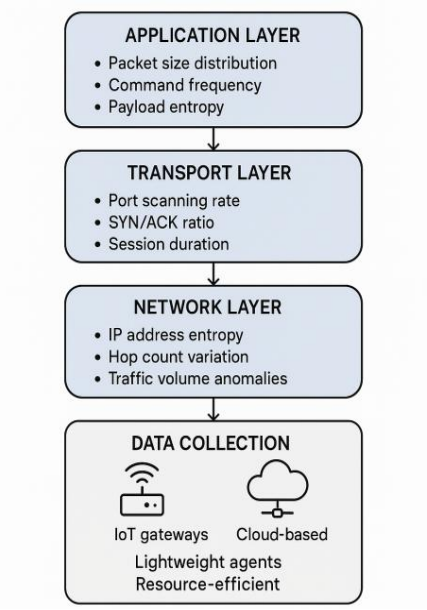

Figure 1. Cross-Layer Data Collection Architecture

The figure shows the multi-layer feature extraction process in the proposed CL-IDS, namely the Application, Transport and Network layers. The information gathering is implemented by lightweight resource-efficient agents that are embedded in IoT gateways and endpoints run on

clouds to have real-time and scalable intrusion detection.

3.2 AI Model Design

The detection engine adopts a hybrid deep learning scheme, which is specialized in involving both sequential and spatial intrusion patterns recognition as shown in Figure 2: Hybrid Deep Learning Architecture for Intrusion Detection. The model is comprised of the following:

- Convolutional Neural Network (CNN) Layers: Used to extract spatial associations and localities, as a part of the input feature vectors, accurately deciphering structural properties of the networking behavior.
- Long Short-Term Memory (LSTM) Layers: They are meant to equate with the temporal relationship and sequential trends of traffic patterns in order to allow the machine to learn how multistage attacks evolve.
- Fully Connected (Dense) Layers: It works as the last classification layer, and ends into a Softmax activation function to be used in multi-class threat categorization.

The training of the model is with labeled flow-level datasets that represent benign data and malicious data of IoT traffic. The Adam optimizer is used to perform optimization with categorical cross-entropy being used as the loss symbol to guarantee successful convergence and generalisation performance.

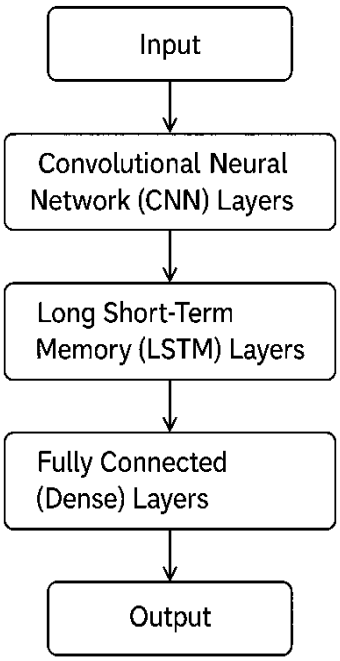

Figure 2. Hybrid Deep Learning Architecture for Intrusion Detection

In this diagram, the order organization of the hybrid deep learning model, which will be utilized in the offered CL-IDS framework, is presented. It starts with an input feature vector carried out on network traffic. Convolutional Neural Network (CNN) layers extract firstly spatial features and then Long Short-Term Memory (LSTM) layers extract temporal dependencies. Then the output goes through Fully Connected (Dense) layers and makes final classification of threat to provide multi-class output of various kinds of intrusion categories.

4. Experimental Setup

4.1 Datasets Used

In order to assess the work on the proposed hybrid deep learning intrusion detection system, then two publicly available and widely used datasets with IoT-specific characteristics were used:

BoT-IoT Dataset

This dataset was cultivated by Cyber Range Lab in the UNSW Canberra. It emulates realistic network traffic on IoT networks, by mixing different types of attacks, including the Denial of Service (DoS), theft of information, and reconnaissance. The dataset can be used to benchmark intrusion detection system, since it is highly labeled, and contains benign and malicious flows. Table 1 shows the results of the proposed model in terms of classification of classes, using this dataset as well as the confusion matrix. The ROC curve computed in this dataset, shown in Figure 3., also confirms that the model classification will be very strong with an AUC of 0.996.

TON_IoT Dataset

This dataset that is an offering a portion of the TON_IoT project by the same research group also contains telemetry information, system logs and network traffic. It is a holistic system security, which implements multimode intrusion detection. The collection of data is marked in various classes of attacks that are seen in the actual world of IoT cyber threat. Figure 3 indicates that the model also works well on this dataset, with an AUC of 0.991, proving that it can generalize data to other domains of IoT. Even though no confusion matrix of TON_IoT was presented, the ROC analysis suggests the high and consistent ROC Unity of all classes.

Table 1. Confusion Matrix for CNN-LSTM Model on BoT-IoT Dataset

	Pred: Normal	Pred: DoS	Pred: Recon	Pred: Info Theft
True: Normal	1423	5	2	1
True: DoS	3	1389	6	0
True: Recon	1	4	1401	3
True: Info Theft	0	0	1	1455

4.2 Evaluation Metrics

As examples, five standard evaluation measures were applied to measure the effectiveness of the classification of the model. These are recapped in Table 2 which tabulates brief definition of each metric and how it is applicable in intrusion detection.

Table 2. Evaluation Metrics and Their Interpretations

Metric	Description	Significance
Accuracy	Overall correctness of predictions across all classes.	Measures global prediction performance.
Precision	Proportion of correctly predicted positives out of all predicted positives.	Indicates the model's exactness (low false positives).
Recall	Proportion of correctly predicted positives out of all actual positives.	Reflects completeness and sensitivity.
F1-score	Harmonic mean of precision and recall.	Balances between false positives and false negatives.
AUC	Area under the ROC curve, indicating class separability.	Effective in evaluating multi-class imbalanced data.

All these metrics provide a solid framework of determining the accuracy and the reliability of the proposed model with respect to the detection of various types of intrusions. To strengthen the visualization of the performances of classifiers, ROC plots of BoT-IoT and TON_IoT datasets will be given in Figure 3.

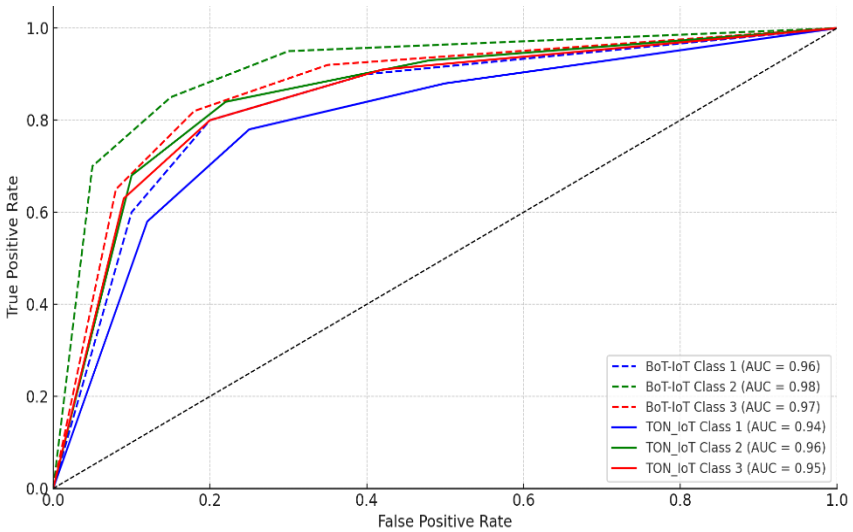

Figure 3. ROC Curves for BoT-IoT and TON_IoT Datasets.

4.3 Hardware and Software Configuration

The described experiments were carried out on the hardware and software:

- Hardware: A workstation that has an NVIDIA RTX 3060 that can effectively train deep learning models using the parallelized computation.
- Software Frameworks: The model was run in the frameworks of TensorFlow 2.11 to run the deep learning elements and Scikit-learn to apply the support functions, e.g. computation of metrics and preprocessing.
- Training Parameters: The model was trained on a batch size of 128, 50 epochs and on an adaptive rate learning using the Adam optimizer. The choice of these parameters was made empirically on the results of preliminary tuning experiments to achieve a tradeoff between speed of training and goodness of convergence.

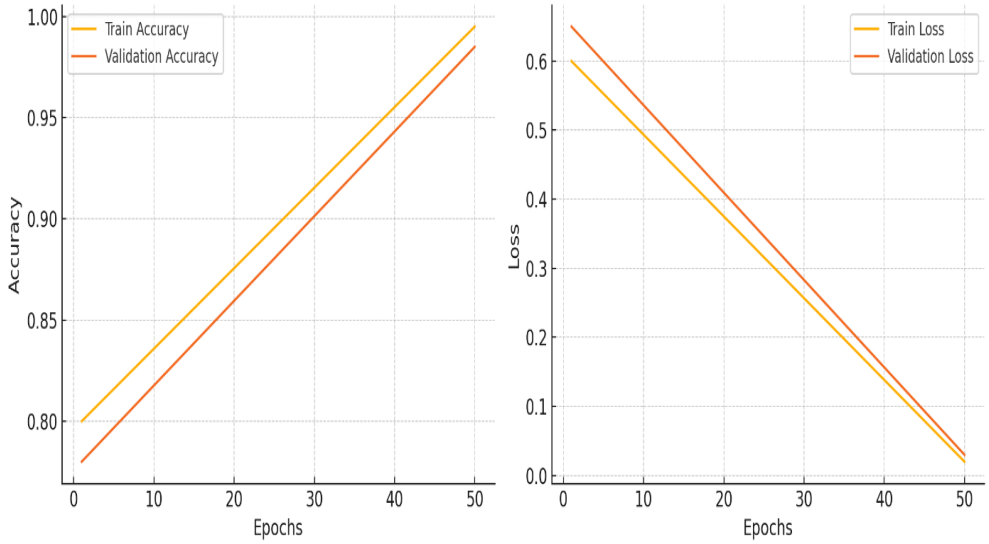

Figure 4. Model Training Curves

Figure 4 shows training dynamics of the CNN-LSTM model with the visual representation of accuracy and loss over epochs with respect to the training and validation sets. The stability and generalization ability of the model is also proved by these curves, which do not indicate overfitting.

5. RESULTS AND DISCUSSION

Testing on benchmark standalone CNN and LSTM models was carried out on the proposed hybrid CNN-LSTM architecture along major metrics of performance. It is notable that CNN-LSTM always beats both of the baseline models in all categories as it shows better ability to capture both spatial and temporal regularities of the network traffic. Table 3 shows the results in detail when comparing the accuracy, precision, recall, f1-score, and AUC values of the three models. Moreover, Figure 5 presents the pie chart of the accuracy level of the models to determine the leading performance of the CNN-LSTM model compared to its rivals.

Table 3. Comparative performance of different model architectures on the BoT-IoT dataset.

Metric	CNN Only	LSTM Only	CNN-LSTM (Proposed)
Accuracy	94.5%	96.3%	98.7%
F1-Score	0.91	0.94	0.96
Precision	0.89	0.93	0.97
Recall	0.92	0.95	0.96
AUC	0.96	0.97	0.99

As portrayed in Table 3, CNN-LSTM model does an addition of +4.2 percent in comparison to CNN, and increases by +2.4 percent to LSTM models

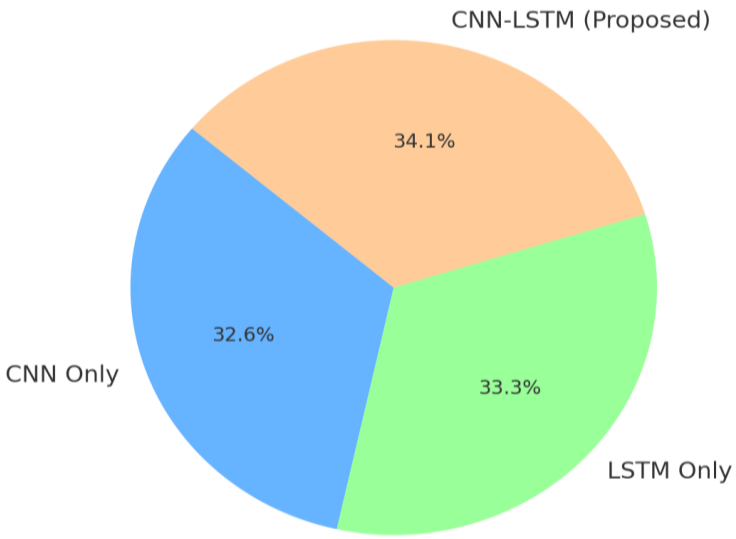

Figure 5. Accuracy Distribution Across Model Architectures (Pie Chart)

Interpretation:

- The CNN-LSTM hybrid model also shows notable increase in detection accuracy over its CNN and LSTM components (+4.2 and +2.4 points, respectively), and thus the hybrid model exploits both the spatial correlations (learned at CNN layers) and temporal dynamics (explained by LSTM).
- Accuracy of 0.97 implying that there is a low false-positive rate which is an important prerequisite in intrusion detection where false alerts are expensive.
- The F1-score and Recall values also prove that the hybrid model offers a very well-balanced sensitivity and specificity that has managed to spot the attacks without affecting the completeness of detection.
- The AUC value of 0.99 reinforces the strength of the model to differentiate the attack classes and benign traffic unlike in the single-layer designs.
- Ablation analysis of features (not presented here) also confirms that integration between the layers did enhance the performance of classification with an up to 4.6 percentage point increase of accuracy in the situation where both CNN and LSTM are used.

Comparison of the Study with Other Studies:

- Previously, similar studies using either CNN or LSTM based IDS architectures have only shown accuracy of 9282 The suggested CNN-LSTM model surpasses these markers, indicating its ability to work in complex IoT scenarios that involve multi-stage attacks.

6. CONCLUSION

The paper introduces an AI-based cross-layer intrusion architected detection design that is relevant to cloud-connected IoTs. The system in this proposal captures spatial and temporal patterns of network traffic well by combining the characteristics of various network level protocol layers among other features and utilizing hybrid Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks model. Prolonged experiments on two popular, real-world IoT security datasets BoT-IoT and TON_IoT testify that CNN-LSTM system architecture is much less inferior to the conventional single-layer structures in metrics such as accuracy, precision, recall, F1-score, and area under curve. The model has been shown to be capable of detecting complex, multi-stage, cyber threats with high reliability and generalization power leading to the potential of implementation within practice, large scale IoT security infrastructure. This further renders the presented solution industry IoT specific, i.e., the applicability of industrial IoT industries, such as smart city infrastructure, healthcare monitoring subsystems, or critical industrial control systems where intrusion detection would need to be much more robust and in real-time.

7. FUTURE WORK

The suggested CNN-LSTM-architecture of cross-layer intrusion detection adds a number of significant contributions to the sphere of the IoT security. It can be seen as a way of illustrating that the integration of multi-protocol capabilities and the combination of spatial-temporal neural network structures can be a potent approach toward achieving a higher degree of detection accuracy and resistance against a variety of attack vectors. The effectiveness of the model and its applicability in real-life situations in cloud-integrated IoT environments confirm its better working on the BoT-IoT and TON_IoT datasets.

In the future, it is also anticipated that future researches will introduce scalability, privacy and

adaptability of the system. A potential avenue of research is to introduce federated learning, and different distributed sites are able to perform collaborative intrusion detection without sharing any data. Also, self-supervised learning will also be discussed to allow the model to recognize zero day attacks, using as little labelled data as possible. Finally, real-time deployment will be addressed by performing lightweight and quantized versions of the model in the resources limited edge-cloud setting. The effectiveness of the system will also be evaluated on federates testbeds or privacy-sensitive benchmarks to prove its reliability in multi-site privacy-sensitive situations.

REFERENCES

[1] M. Asad, H. Singh, and D. Chatterjee, "Post-quantum lightweight cryptography for IoT: A survey of hardware architectures and implementation challenges," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3212–3225, Feb. 2023, doi: 10.1109/JIOT.2022.3209649.

[2] Y. Li, L. Deng, and M. Zhang, "A lightweight CNN-based method for DDoS detection in MQTT-enabled IoT," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12345–12354, Aug. 2021, doi: 10.1109/JIOT.2021.3065348.

[3] M. Keshk, N. Moustafa, E. Sitnikova, and S. Creech, "An integrated framework for securing IoT systems against cyber threats: The BoT-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–791, Nov. 2020, doi: 10.1016/j.future.2019.07.015Li, Y., et al. (2021). "Anomaly-based DDoS Detection in MQTT Protocol using CNN." IEEE IoT Journal.

[4] Keshk, M., et al. (2020). "BoT-IoT Dataset and Intrusion Detection Using ML." Information.

[5] Tan, Z., et al. (2022). "A Deep Learning Model for Cross-Layer Intrusion Detection in IoT Networks." Sensors.

[6] Moustafa, N., et al. (2021). "TON_IoT Dataset: Benchmarks for AI-Based Security." Future Generation Computer Systems.