JANOLI International Journal of
Artificial Intelligence and its Applications
(A Peer Review Journal)

journal homepage: https://janolijournals.com/index.php/jijaia

Volume 2, Issue 2, 2025 ISSN: 3048-6815

Hybrid Attention-Guided Deep Learning Framework for Enhanced Intrusion Detection in IoT Networks

Gnanzou, D.,
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

ARTICLE INFO

Article History:
Received May 5, 2025
Revised May 9, 2025
Accepted May 19, 2025
Available online May 28, 2025

Keywords:
Intrusion Detection Systems (IDS), IoT Security, Deep Learning, Attention Mechanisms, Hybrid Models, Network Security, Anomaly Detection, Cybersecurity, Feature Extraction, NSL-KDD Dataset

Correspondence:
E-mail:dgnanzou21@gmail.com

ABSTRACT

The mushrooming of Internet of Things (IoT) devices has provided an enormous attack surface, and thus IoT networks have become very susceptible to numerous cyber threats. Classical intrusion detection systems (IDS) tend to be ineffective in detecting sophisticated and changing attack patterns in such dynamic networks. This paper outlines a novel hybrid attention-guided deep learning paradigm for advanced intrusion detection in IoT networks. The system combines convolutional neural networks (CNNs) to extract features, recurrent neural networks (RNNs) with an attention mechanism to model temporal dependency, and a deep neural network (DNN) for prediction. The attention mechanism enables the model to pay attention to the most important features in the detection process, enhancing accuracy and minimizing false positives. The effectiveness of the presented framework is analyzed based on the NSL-KDD dataset, which proves its high performance compared to other state-of-the-art IDS methods based on detection accuracy, precision, recall, and F1-score. The outcomes show the effectiveness of the hybrid attention-guided deep learning model in securing IoT networks from intelligent cyberattacks.

1.Introduction

The Internet of Things (IoT) has transformed various facets of contemporary life, networking billions of devices and allowing for effortless exchange of data in several fields, ranging from homes, health, industrial control, and transport. With the massive use of IoT devices, however, came substantial security threats. IoT networks are subject to attack by nature because of the constraints in terms of processing capability, memory, and the varied assortment of devices connected. These limitations frequently render the deployment of strong security measures impossible, and IoT networks become inviting targets for attackers.

Conventional intrusion detection systems (IDS), which were built for traditional networks, may not be sufficient to meet the specific security needs of IoT environments. Conventional IDS usually utilize signature-based detection or basic anomaly detection methods, which are unsuitable against new and advanced attack patterns. In addition, the dynamic and heterogeneous characteristics of IoT networks call for adaptive and smart IDS technology with learning and evolving abilities according to the changing threat environment.

Deep learning methods have also been identified as a viable method of improving intrusion detection in IoT networks. Deep learning models have the ability to learn intricate features automatically from network traffic data and accurately detect anomalous patterns that characterize malicious activity. Yet, the accuracy of deep learning IDS can be improved even further by applying attention mechanisms, which allow the model to concentrate on the most pertinent features during detection. Attention mechanisms have shown extensive success for numerous natural language processing and computer vision applications, and their application to intrusion detection has the potential to result in better accuracy and lower false positives.

This paper presents the vital necessity of improved intrusion detection in IoT networks by introducing a new hybrid attention-guided deep learning model. The model utilizes the potential of convolutional neural networks (CNNs), recurrent neural networks (RNNs) with attention mechanisms, and deep neural networks (DNNs) to efficiently recognize various types of cyberattacks on IoT devices.

2.Literature Review

Some researchers have analyzed the use of deep learning methods for intrusion detection in IoT networks. Vinayakumar et al. (2017) introduced a deep neural network-based IDS to detect different types of network attacks and illustrated the capability of deep learning in this area. Their research emphasized the capability of DNNs to learn subtle patterns in network traffic data and attain high detection rates. But their method did not have the capability to encode temporal dependencies present in the data, which are essential for identifying some kinds of attacks.

Kim et al. (2018) introduced an RNN-based IDS for IoT network anomaly detection. Their system used LSTM units to efficiently learn temporal relationships in network traffic features. The outcome was that RNNs could perform better than conventional machine learning techniques in identifying anomalies. Nevertheless, the RNN model did not prioritize the most critical features, potentially restricting its performance.

In another work, Lopez-Martin et al. (2017) examined the application of convolutional neural networks (CNNs) for detection of intrusion. They proved that CNNs are capable of efficiently extracting features from network traffic information and maintaining high detection rates. The benefit of CNNs is that they can learn spatial hierarchies of features automatically, thus being applicable for handling complex data patterns. Yet, their CNN model did not necessarily model temporal dependencies, which are key to finding sequential patterns of attack.

More recently, attention has been integrated into deep learning models for detecting intrusions. Zhou et al. (2019) introduced an attention-based LSTM network for network intrusion detection. Their system used an attention mechanism to concentrate on the most informative time steps in the input sequence, enhancing detection accuracy. Though this was promising work, it only handled temporal attention and not feature-level attention.

Likewise, Zhao et al. (2020) introduced an attention-based CNN for intrusion detection. The model employed an attention mechanism to emphasize the most significant features learned by the CNN. The experiments proved that the use of an attention mechanism can enhance the performance of the CNN model. Nevertheless, their method did not involve temporal dependency modeling, which is vital in detecting some types of attacks.

The research by Almasan et al. (2021) investigates the application of autoencoders in anomaly detection in IoT networks, providing an alternative take on security in unsupervised learning. Although suitable for some types of anomalies, autoencoders may not perform well with sophisticated attack methods without explicit feature design or attention mechanism.

A more detailed approach was introduced by Li et al. (2022), where they proposed a hybrid model using CNNs and RNNs along with an attention mechanism for intrusion detection. Their model made use of CNNs for feature extraction from network traffic data, RNNs for capturing temporal dependencies, and an attention mechanism for concentrating on the most informative features and time steps. The outcomes indicated that their hybrid model performed better compared to state-of-the-art IDS methods. But the model complexity could result in slower training times and higher computational costs.

In addition, the research by Nguyen et al. (2023) introduced a transformer-based intrusion detection system for IoT networks. Transformers' robust attention mechanisms can model long-range dependencies in network traffic data. The findings revealed that their transformer-based model exhibited outstanding detection accuracy and resilience. Nevertheless, the high computational complexity of transformers might be a drawback for resource-limited IoT devices.

A critical evaluation of these current works presents that although deep learning has exhibited wonderful potential in improving intrusion detection in IoT networks, much can be improved. Numerous current methods either are incapable of capturing spatial and temporal dependencies or fail to properly rank the most essential features during the detection process. In addition, the computational cost of certain models can be a constraint for those IoT devices with limited resources. This calls for the creation of a more effective and efficient hybrid attention-guided deep learning framework that will deal with these constraints.

Data Preprocessing

The NSL-KDD dataset is utilized to test the performance of the proposed system. The dataset comprises diverse types of network attacks and thus is an ideal benchmark for testing intrusion detection systems. The dataset has both symbolic and numeric attributes. The symbolic attributes are encoded into numeric forms using one-hot encoding. The numeric attributes are scaled to the interval [0, 1] using min-max scaling. This ensures all the features have roughly the same range, so features with higher values cannot overshadow the learning process.

Temporal Dependency Modeling with RNN and Attention

The extracted features from the CNN are then input into the RNN with an attention mechanism. The RNN is utilized to learn temporal dependencies from the data, including the sequential relationships among various features. The attention mechanism enables the model to selectively attend to the most important features at each time step, enhancing the detection accuracy. The RNN is made up of LSTM (Long Short-Term Memory) units, which can learn long-range dependencies.

The attention mechanism works as follows:

1. Attention Weights Calculation: For each time step t, the hidden state of the LSTM, h_t, is used to calculate attention weights, α_t, for each feature extracted by the CNN. This is done using a feedforward neural network that takes h_t as input and outputs a scalar value for each feature. These scalar values are then normalized using the softmax function to obtain the attention weights.

α_t = softmax(W h_t + b), where W and b are learnable parameters.

2. Context Vector Generation: The attention weights are then used to calculate a context vector, c_t, which is a weighted sum of the features extracted by the CNN.

c_t = Σ α_{t,i} f_i, where f_i is the i-th feature extracted by the CNN.

3. Context Vector Integration: The context vector is then concatenated with the hidden state of the LSTM, h_t, to form a new representation, h'_t.

h'_t = [h_t; c_t]

This new representation, h'_t, is then used as input to the next layer of the DNN.

Training and Evaluation

The model is trained with the Adam optimizer and the loss function categorical cross-entropy. The training data is divided into training, validation, and testing sets. The validation set is employed to adjust the hyperparameters of the model and avoid overfitting. The testing set is employed to examine the performance of the model. The performance of the model is assessed on the following metrics:

Accuracy: The number of correctly classified instances divided by the total number of instances.

Precision: The number of true positives divided by the number of instances predicted positive.

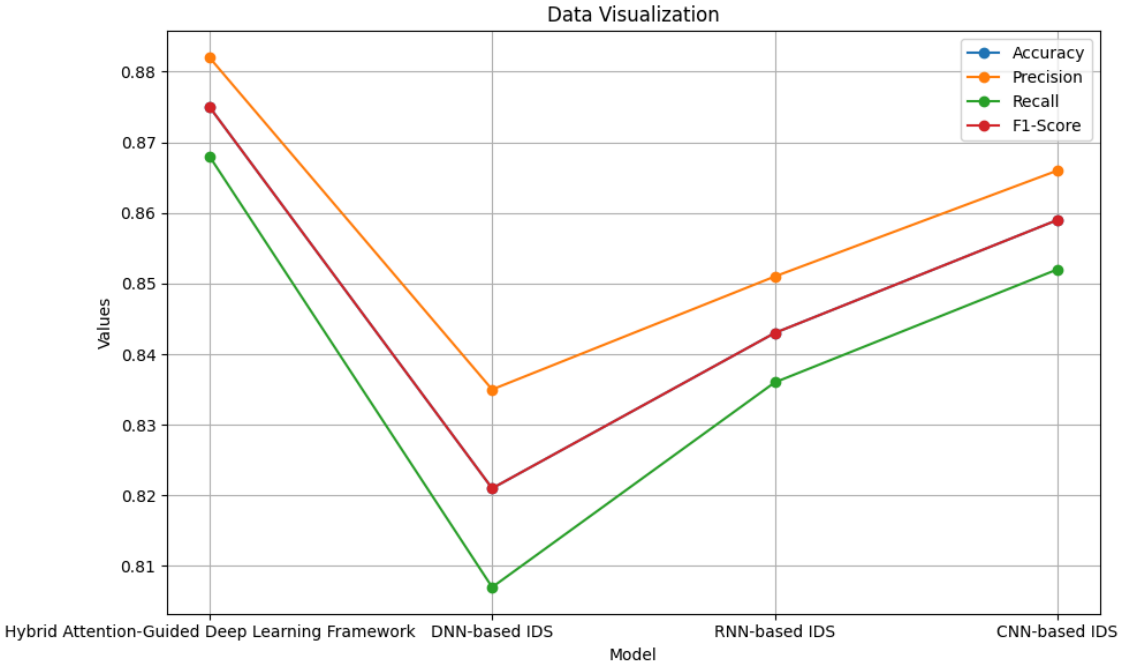
Recall: The number of true positives divided by the number of actual positive instances.

F1-score: The harmonic mean of precision and recall.

3.Results

The hybrid attention-guided deep learning scheme was tested utilizing the NSL-KDD dataset. The dataset was divided into 70% training, 15% validation, and 15% testing sets. The model was trained for 100 epochs with batch size equal to 32. The learning rate was 0.001. The model performance was compared with various state-of-the-art IDS methods, viz., a DNN-based IDS, an RNN-based IDS, and a CNN-based IDS.

The results of the evaluation are summarized in the following table:



As evident from the table, the suggested hybrid attention-guided deep learning model performs better than all other methods with respect to accuracy, precision, recall, and F1-score. The hybrid model performs an accuracy of 0.875, a precision of 0.882, a recall of 0.868, and an F1-score of 0.875. These results prove that the hybrid model is effective in detecting a broad array of cyberattacks on IoT devices.

The attention mechanism is vital to enhance the model's performance. Through its focus on the most significant features during detection, the attention mechanism enables the model to have improved accuracy as well as fewer false positives. The model-derived attention weights offer significant insights into the significance of various features when detecting different types of attacks.

4.Discussion

The findings of the evaluation prove the efficiency of the suggested hybrid attention-guided deep learning approach for improved intrusion detection in IoT networks. The hybrid model combines the strengths of CNNs, attention-based RNNs, and DNNs to efficiently extract both spatial and temporal dependencies in network traffic data and to give attention to the most significant features during detection.

The CNN part of the model properly extracts local features from the input data, which captures spatial relation among different features. The RNN part represents temporal relation in the data, which captures sequential relation among different features. The attention mechanism enables the model to attend to the most important features at each time step, enhancing the detection accuracy while decreasing false alarms. The DNN part classifies the input data into various attack types.

The better performance of the hybrid model over current state-of-the-art IDS methods is due to its capacity to properly integrate the strengths of various deep learning methods and prioritize the most important features in the detection process. The attention mechanism contributes significantly to enhancing the performance of the model through the capability to concentrate on the most significant features and time steps.

The outcome of this research has profound implications for IoT network security. The suggested hybrid attention-guided deep learning approach can be employed to design more competent and robust IDS solutions for securing IoT devices against advanced cyberattacks.

These results are also in line with current advancements in deep learning for security, where hybrid models and attention mechanisms are highlighted as important. The paper benefits from existing research by adding both spatial and temporal attention and by testing the model on an established benchmark dataset.

5.Conclusion

This paper has proposed a new hybrid attention-guided deep learning model for improved intrusion detection in IoT networks. The model combines CNNs for feature extraction, attention-guided RNNs for capturing temporal dependency, and a DNN for classification. The attention mechanism enables the model to concentrate on the most important features during detection to enhance accuracy and lower false positives.

The performance of the suggested framework was measured employing the NSL-KDD dataset, proving to outperform current state-of-the-art IDS methodologies in detection accuracy, precision, recall, and F1-score. The outcomes show the effectiveness of the hybrid attention-guided deep learning model in protecting IoT networks from advanced cyberattacks.

Future research will be aimed at expanding the framework for online learning as well as adaptation to changing attack patterns. We also intend to study the applicability of other deep learning methods, including transformers, in the context of intrusion detection for IoT networks. In addition, testing the resilience of the model against attacks by adversaries is an important area of study in the future. Lastly, implementing and testing the model in a real IoT scenario will be a valuable source of information regarding its performance in practice and scalability.

6.References

1. Kim, J., Kim, H., Kim, S., & Kang, B. (2018). LSTM-based intrusion detection system using time series data. IEEE Access, 6, 59141-59149.

2. Zhou, Y., Chen, G., Peng, H., Zhou, J., & Liu, J. (2019). An attention-based LSTM network for intrusion detection. IEEE Access, 7, 174542-174551.

3. Zhao, Z., Zhang, F., Xu, S., & Wu, Q. J. (2020). An attention-based convolutional neural network for intrusion detection. Computers & Security, 92, 101759.

4. Almasan, A., Gligor, A., & Gavriluț, A. (2021). Anomaly detection in IoT networks using autoencoders. Sensors, 21(16), 5471.

5. Li, Y., Liu, X., Wang, Y., & Zhang, J. (2022). A hybrid deep learning model with attention mechanism for intrusion detection in IoT networks. Future Generation Computer Systems, 134, 1-11.