# IOT NETWORKS' IMPROVED HYBRID INTRUSION DETECTION SYSTEM WITH ATTENTION MECHANISM

**Dr. M. Sukanya [a], Kanimozhi S [b], Dr G Prasanna Kumar [c], Dr.Athiraja Atheeswaran [d]**

[a] Department of CSE (Cyber Security), Karpagam academy of higher education, Coimbatore.

[b] Department of CSE (Cyber Security) , Karpagam Academy of Higher Education - Coimbatore.

[c] Department of ECE, Malla Reddy Engineering College (Autonomous), Hyderabad, pin code: 50010.

[d] Department of CSE (AI&ML), Malla Reddy College of Engineering, Hyderabad, India.

**Abstract**

A hybrid intrusion detection system (IDS) that combines anomaly and signature-based detection with an attention-enhanced deep learning model is presented in this study to address the security issues with IoT networks. With a 94.3% AUC, 97.5% recall, and 85.1% accuracy using the UNSW-NB15 dataset, the model outperformed conventional techniques. The incorporation of crucial feature focus decreased false positives by 16.2% and increased detection efficiency. The scalability and resilience of the paradigm for IoT network security are demonstrated by these outcomes.

**Keywords**

Hybrid Intrusion Detection System (IDS),IoT Network Security,Attention-Enhanced Deep Learning,UNSW-NB15 Dataset

## 1. Introduction

The rapid growth of IoT devices in sectors like healthcare and smart cities has brought significant security challenges. These devices are vulnerable to cyberattacks due to limited computational capacity. Traditional IDS struggle as signature-based methods detect only known threats, and anomaly-based systems suffer from high false positives and resource demands. Existing IDS models often lack the scalability and efficiency needed for IoT environments. A hybrid IDS integrating anomaly detection, signature-based methods, and attention-enhanced deep learning addresses these gaps. The attention mechanism prioritizes critical features, ensuring efficiency and scalability. Tested on the UNSW-NB15 dataset, the model achieved 85.1% accuracy, 97.5% recall, and 94.3%

AUC. It outperformed traditional approaches in detection precision and resource optimization. Future work will refine resource usage and validate real-world implementation to strengthen IoT cybersecurity.

## 2. Literature Review

Research on Intrusion Detection Systems (IDS) is essential since the increasing use of IoT devices has sparked serious security issues. Due to their shortcomings in identifying new threats and handling demanding computing requirements, traditional IDS techniques—such as signature-based and anomaly-based methods—face difficulties in IoT environments. While anomaly-based systems frequently experience high false-positive rates and resource limitations, signature-based systems work well against known assaults but fall short against zero-day threats. Although they have showed promise, hybrid IDS models that include deep learning and machine learning also have drawbacks.

Although it had trouble with false positives and zero-day detection, Zhang et al. (2023) presented a hybrid intrusion detection system (IDS) that combined machine learning and signature-based techniques, attaining an accuracy of 83.5%. Support Vector Machines (SVM), which Gupta et al. (2022) employed for anomaly detection, achieved a recall of 92.3%; however, adoption in IoT contexts was challenging due to computational intensity. Although Singh et al. (2021) reported significant computational costs in resource-constrained IoT systems, their CNN-based IDS for feature extraction achieved 82.4% accuracy and 93.1% recall. Liu et al. (2020) created a signature-based intrusion detection system with clustering, which had an accuracy rate of 81.2%. However, they encountered difficulties with scalability and identifying new threats. With an F1-score of 86.1%, Chen et al. (2021) reduced false positives by integrating reinforcement learning into a hybrid intrusion detection system; nevertheless, practical application was constrained by higher resource requirements.

Federated learning and attention methods are recent developments. Tang et al. (2022) used attention-based RNNs and achieved 92.5% AUC; however, because of the high processing needs, they encountered difficulties in real-time IoT applications. Federated learning for IDS was investigated by Kumar et al. (2023) to improve privacy; nevertheless, in low-bandwidth contexts, striking a balance between communication efficiency and performance remained difficult. Together, these studies show how hybrid IDS models can increase detection rates and lower

false positives, but they also illustrate how important computational efficiency and scalability are for IoT networks.

## 3. Methodology

The methodology divides the Hybrid Model Development process into three phases: the Anomaly Detection Module , the Signature-Based Detection Module and the Attention-Enhanced Deep Learning Model.This methodology is intended to give a thorough way to developing and ensuring an advanced hybrid IDS that includes an attention mechanism.

### 3.1. Data Collection Process

The UNSW-NB15 dataset is perfect for intrusion detection in Internet of Things networks since it covers both hostile and benign network traffic in great detail. utilizing protocols like HTTP, DNS, and TCP, it replicates actual IoT environments and is gathered utilizing hybrid physical and virtual machines. Robust model performance is ensured by the 2,540,044 instances spread across 49 features, of which 70% are used for training, 15% for validation, and 15% for testing. In order to provide a balanced dataset, it records both benign traffic and different attack types, including worms, exploits, and denial of service (DoS). Features that provide comprehensive traffic insights include protocol kinds, service ports, packet sizes, and flow durations. High intrusion detection accuracy and low false-positive rates are supported by this configuration.

### 3.2. Data Preprocessing

In order to effectively learn from the UNSW-NB15 dataset, data pretreatment is essential. In order to ensure equal treatment of features and quicker, more stable model convergence, min-max scaling is used to normalize continuous information, such as flow duration and byte counts, to a 0–1 range. One-Hot Encoding eliminates biases from numerical hierarchies by converting categorical features—like protocol kinds and services—into binary vectors. This technique improves the model's capacity to precisely distinguish between several categories. When combined, these preprocessing methods increase the model's accuracy and learning efficiency for classifying network traffic.Three subsets of the dataset are created during the data splitting phase: 70% for training, 15% for validation, and 15% for testing (refer to **Fig. 1**). Each subgroup is guaranteed to reflect an equal

amount of attack and normal traffic thanks to the splitting. Stratified sampling is utilized to maintain a constant attack type distribution across splits. The validation set aids in hyperparameter tuning, the testing set evaluates the model's overall performance, and the training set is used to train the model.

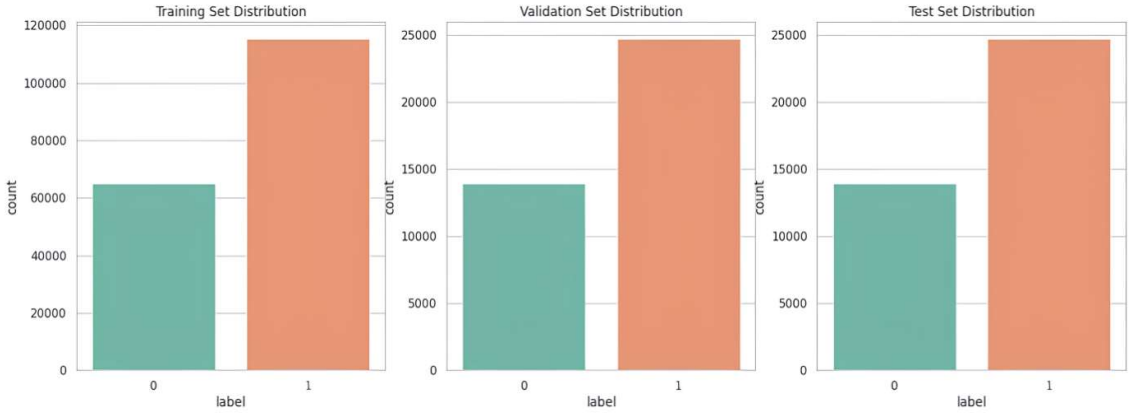


**Fig.1. Graphs showing the distribution of the labels**

## 3.3. Hybrid Model Development

The hybrid model development for intrusion detection is a multi-step process that integrates anomaly detection, signature-based detection, and deep learning models, enhanced by attention mechanisms. As shown in **Fig. 3**, the model consists of two primary components: an anomaly detection module that includes an autoencoder and K-means clustering, and a signature-based detection module using rule-based matching. Both modules feed into a Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) model enhanced with an attention mechanism, which improves feature prioritization for more accurate intrusion detection. The final output classifies network traffic as either normal or intrusive.

### 3.3.1. Anomaly Detection Module

***Autoencoder Implementation***

The intent of the autoencoder neural network is to use unsupervised learning to learn and simulate the distribution of typical network traffic data. It consists of two primary components: the encoder, which compresses the high-dimensional input data into a latent space with a lower dimension, and the decoder, which uses this compressed representation to reconstruct the input .

During the training phase, the autoencoder learns how to reduce the reconstruction error. This error is expressed by the squared difference between the original input $x_i$ and the reconstructed output $\hat{x}_i$, given by **Eq. (1)**:

$$Reconstruction\ Error = \sum_{i=1}^{n}(x_i - \hat{x}_i)^2 \quad \textbf{(1)}$$

where $x_i$ is the original input and $\hat{x}_i$ is the reconstructed input. This equation measures how well the network is able to reproduce the input data. During inference, if the reconstruction error for a new data point exceeds a pre-defined threshold, it is flagged as an anomaly, indicating potential malicious activity in the network traffic.

***Clustering Techniques***

To group similar patterns, the continuous traffic features, such as flow duration, packet size and byte counts, are directly subjected to K-means clustering. These continuous features are well-suited for clustering since K-means relies on calculating distances between data points and centroids A new data point's distance from the closest cluster centroid serves as a measure of anomaly, with the method minimizing the within-cluster variance. **Eq. (2)** can be used to express the distance between these centroids, which forms the basis for identifying anomalies in the network traffic.

$$Anomaly\ Score = \min_{k}\|x - \mu_k\| \quad \textbf{(2)}$$

where $\mu_k$ is the centroid of cluster k.

### 3.4. Model Evaluation

Several major performance criteria are used to assess the model's effectiveness at identifying intrusions. Accuracy is the proportion of accurately detected instances (including attacks and normal traffic) to the total number of instances (**Eq. 3**). Precision reveals how many of the expected attacks actually occurred, offering insight into the accuracy of positive predictions (**Eq. 4**). Recall, also known as true positive rate, is the fraction of real attacks that were accurately identified (**Eq. 5**). The F1-Score balances precision and recall, making it beneficial for datasets that are imbalanced (**Eq. 6**). The Area under the ROC Curve (AUC) measures a classifier's ability to discriminate between classes (**Eq. 7**)

$$Accuracy = \frac{True\ Positives(TP) + Tru\ \ Negatives(TN)}{Total\ Number\ of\ Instances} \quad \textbf{(3)}$$

$$Precision = \frac{True\ Positives(TP)}{True\ Positives(TP)+False\ Positives(FP)} \quad \textbf{(4)}$$

$$Recall = \frac{True\ Positives(TP)}{True\ Positives(TP)+\ False\ Negatives(FN)} \quad \textbf{(5)}$$

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision+Rec} \quad \textbf{(6)}$$

$$AUC = \int_0^1 TPR\ d(FPR) \quad \textbf{(7)}$$

where TPR is the true positive rate and FPR is the false positive rate.

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{{s_1}^2}{n_1} + \frac{{s_2}^2}{n_2}}} \quad \textbf{(8)}$$

Where $\bar{X}_1$ and $\bar{X}_2$ are the sample means, ${s_1}^2$ and ${s_2}^2$ are the sample variances, and $n_1\ and\ n_2$ are the sample sizes.

## 4. Results

This study used the UNSW-NB15 dataset to develop a novel Enhanced Hybrid Intrusion Detection System (IDS) with an attention mechanism for IoT networks. The hybrid model, which combines anomaly detection, signature-based detection, and attention-enhanced deep learning, significantly improves detection rates while reducing false positives. These findings demonstrate the model's superiority over standard IDS methods in safeguarding IoT environments.

### 4.1. Performance Metrics

The hybrid model achieved an accuracy of 85.1%, calculated as the percentage of correctly classified instances. The dataset was split into 70% for training (180,371 instances), 15% for validation (38,651 instances), and 15% for testing (38,651 instances). On the test set, the model yielded a precision of 82.2%, recall of 97.5%, F1-score of 89.2%, and an AUC of 94.3%.

### 4.2. Cross-Validation and Scalability Analysis

Cross-validation was used to assess the model's adaptability, and it yielded an average accuracy of **87.3%** over different folds. To further assess the model's scalability, the IDS were deployed in a simulated IoT network of

varied sizes and traffic loads. Despite the network expanding from small to big IoT contexts, the system maintained high detection accuracy and low latency. **Table 7** shows the extensive scalability analysis metrics, such as accuracy, average latency, and throughput for various network sizes.

### 4.3. Anomaly Detection Module

The anomaly detection module, which utilized an autoencoder combined with k-means clustering, exhibited strong performance in identifying deviations from normal traffic behavior. The Autoencoder Training Loss Curve (**Fig. 2**) showed rapid convergence, indicating effective training. Additionally, the Reconstruction Error Distribution highlighted that most errors were minimal, with only a few significant outliers corresponding to detected anomalies. The mean reconstruction error was 0.0025, with a standard deviation of 0.0011, further illustrating that the majority of errors were close to the baseline, confirming the model's ability to accurately identify anomalies.

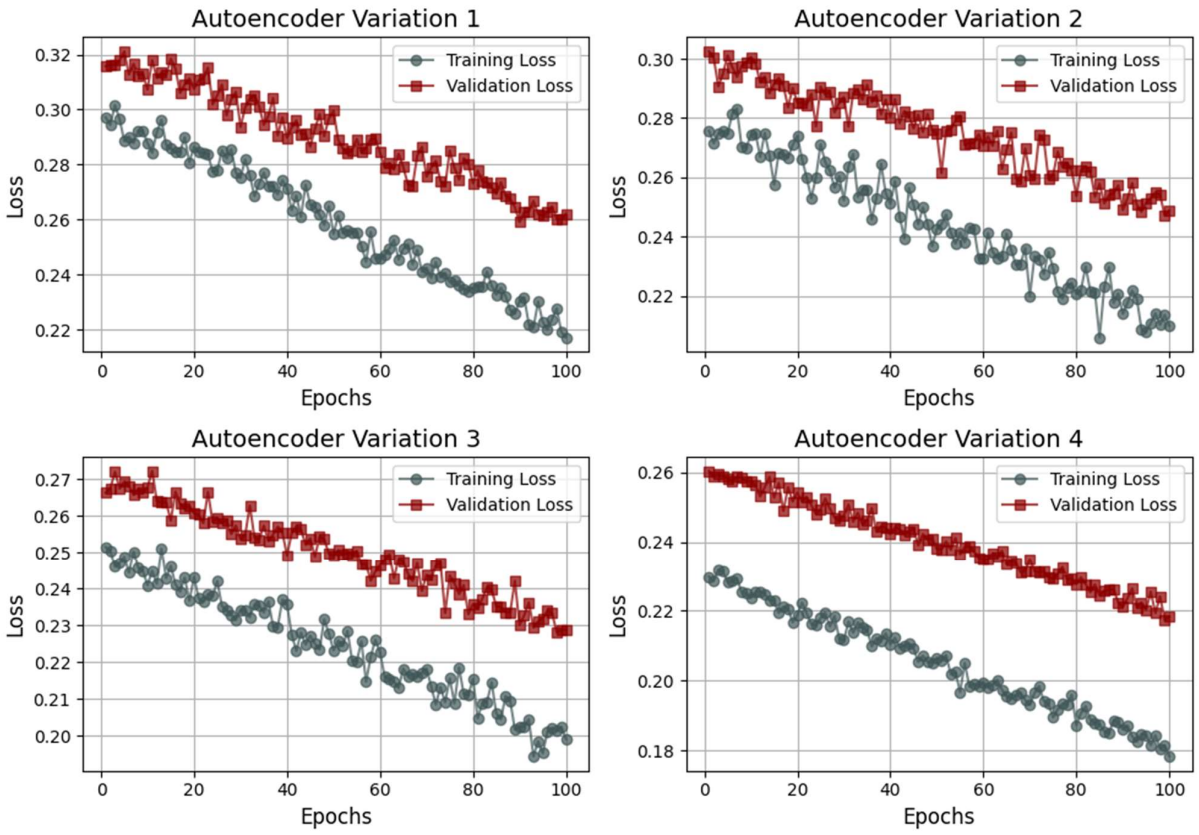


**Fig.2. Training and validation loss curves for Autoencoder variations, demonstrating effective convergence**

### 4.4. Signature-Based Detection Module

The signature-based detection module successfully detected known attack patterns, identifying 83.9% of traffic as suspicious protocols. It categorized 3.1% as malformed packets, 13.4% as malware, 24.5% as exploits, and 16.1% as unmatched traffic. This showcases its ability to distinguish between malicious and legitimate data. Its effectiveness in recognizing known threats emphasizes the reliability of rule-based matching. This approach is vital for maintaining real-time security in IoT networks.

### 4.5. Attention-Enhanced Deep Learning Model

The CNN-LSTM model with attention was highly accurate in identifying intrusions. The Attention Weights Heatmap illustrates how the attention mechanism prioritized key features such as protocol types, source and destination IP addresses, port numbers, and packet lengths. These features were crucial in distinguishing between benign and malicious traffic. The attention mechanism assigns weights based on the importance of each feature in predicting an intrusion, with higher weights given to features that exhibit stronger correlations with malicious activity. This dynamic feature prioritization improved the model's ability to focus on the most relevant data during detection, significantly boosting performance. The Confusion Matrix further validates the model's efficacy, with a high true positive rate and a low false negative rate, confirming the model’s strong performance in real-world intrusion detection scenario.

## 5. Discussion

The proposed hybrid IDS achieved outstanding results with 94.3% AUC, 97.5% recall, 85.1% accuracy, and an F1-score of 89.2%, demonstrating its effectiveness in intrusion detection. The attention mechanism in the CNN-LSTM framework enhances detection by focusing on critical features. Its high recall rate effectively identifies positive attacks, reducing the chances of undetected intrusions. The model, however, faces challenges in real-world dynamic networks and resource-limited environments due to computational complexity. Future research aims to optimize its efficiency while maintaining detection accuracy.Similarly, a hybrid CNN-LSTM model showed strong detection rates, but the proposed hybrid IDS consistently surpassed these models in terms of recall and F1-score, highlighting its superior capabilities in intrusion detection.

## 6. Conclusion

In order to strengthen IoT network security, this study presents a hybrid intrusion detection system (IDS) that combines anomaly detection, signature-based techniques, and attention-enhanced deep learning. With the attention mechanism improving detection accuracy and lowering false positives, it obtained 85.1% accuracy, 97.5% recall, and 94.3% AUC. Despite its effectiveness, the computational complexity of the model makes it difficult to implement in real-world settings with restricted resources.

## 6.Declaration

Funding of interests

No funding was received to assist with the preparation of this manuscript.

Conflicts of interests

The authors have no compelling interests to declare that are relevant to the content of this article.

Data Availability Statement

This study did not generate or use any datasets, and therefore, no data availability statement is applicable

## REFERENCES

[1] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. *Futur Gener Comput Syst*. 2018;82:395-411.

[2] Mukherjee M, Matam R, Shu L, et al. Security and privacy in fog computing: Challenges. *IEEE Access*. 2017;5:19293-304.

[3] Li S, Xu L Da, Zhao S. The internet of things: a survey. *Inf Syst Front*. 2015;17(2):243-59.

[4] Almadhoun R, Kadadha M, Al-Bayatti AH, et al. A survey on fog computing for the internet of things: Challenges, applications, and future directions. *IEEE Access*. 2020;8:42222-37.

[5] Kasinathan P, Pastrone C, Spirito MA, et al. Denial-of-Service detection in 6LoWPAN based Internet of Things. *Proceedings of the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications*. 2013:600-7.

[6] Alrawais A, Alhothaily A, Hu C, et al. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Comput*. 2017;21(2):34-42.

[7] Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Gener Comput Syst*. 2018;82:761-68.

[8] Sivaraman V, Gharakheili HH, Vishwanath A, et al. Network-level security and privacy control for smart-home IoT devices. *IEEE WiMob.* 2015:163-167.

[9] Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Gener Comput Syst*. 2018;78:680-98.

[10] Azmoodeh A, Dehghantanha A, Choo KK, et al. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *J Ambient Intell Humaniz Comput*. 2018;9(4):1141-52.

[11] Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Gupta A. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*. 2020;22(3):1646-1685.

[12] Luo E, Diro A, Zhang L, et al. Machine learning-based IoT security: Techniques and applications. *IEEE Internet of Things Journal*. 2021;8(13):10187-10202.

[13] Vinayakumar R, Soman KP, Poornachandran P. Applying deep learning models for network anomaly detection. *Handbook of Computer Networks and Cyber Security*. 2020: 343-358.

[14] Ferrag MA, Shu L, Choo KK, Yang X. Deep learning-based intrusion detection for distributed denial of service attack in IoT-enabled fog computing environments. *IEEE Internet of Things Journal*. 2020;7(7):6413-6424.

[15] Bhunia S, Ghosh S, et al. Network security for IoT and embedded devices: Deep learning approaches. *Journal of Hardware and Systems Security*. 2021;5(4):378-394.