Research Journal of Engineering Technology and Medical Sciences (ISSN: 2582-6212), Volume 09, Issue 02, June-2026
Available at www.rjetm.in/

A Lightweight CNN–Transformer Hybrid Framework for Intelligent IoT Botnet Detection Using Deep Learning

[1]Priyanka Giri, [2]Aashish Kumar Tiwari
[1]Mtech Scholar, Department of School of Computer Science and Technology, Sam Global University, Bhopal, India
[2]Assistant professor, Department of School of Computer Science and Technology, Sam Global University, Bhopal, India
[1]priyanka20011013@gmail.com ,[2] aashish.tiwari7898@gmail.com

* Corresponding Author: Priyanka Giri

Abstract:

The exponential growth of the Internet of Things (IoT) has brought about a revolution in the field of communication through its capability to connect a large number of intelligent devices within the fields of healthcare, smart cities, industrial automation, and intelligent transportation. However, owing to the constrained nature of IoT devices and the growing complexity of botnets attacks, the IoT networks have been vulnerable to serious cybersecurity threats such as DDoS, malware spread, credential hijacking, and access exploitation. Traditional methods based on predefined signatures and rule detection have proven to be ineffective in detecting emerging attacks on IoT devices. This paper offers an elaborate review on machine learning and deep learning for IoT botnet detection and also introduces a lightweight CNN-Transformer hybrid model for intrusion detection. This approach uses Convolutional Neural Networks (CNN) to extract local features and Transformer network architecture to learn dependencies in network traffic. For increasing the robustness of the proposed framework, class imbalance is handled by generating synthetic data and class-weighted learning, while improving the interpretability of the model by using the attention mechanism in the Transformer. In addition to the above contributions, the research also offers a comprehensive literature review on IoT botnet detection approaches, datasets, feature extraction techniques, evaluation criteria, and detection-prevention approaches. The main goal of the proposed framework is to attain high detection accuracy, precision and recall, good generalizability to different attack types, and efficiency from a computational point of view that is ideal for IoT. The results will help in the creation of intelligent and adaptable intrusion detection systems that will be able to enhance the security of IoT cyber space from the botnets.

Keywords: Internet of Things (IoT), IoT Botnet Detection, Intrusion Detection System (IDS), Deep Learning, Convolutional Neural Network (CNN), Transformer, Machine Learning, Cyber security, Network Traffic Classification, Class Imbalance Handling, Explainable Artificial Intelligence (XAI), BoT-IoT Dataset.

I. INTRODUCTION

The rapid advancement of the Internet of Things (IoT) has transformed the modern digital ecosystem by enabling seamless communication among billions of interconnected devices. IoT technologies are extensively utilized across diverse domains, including healthcare, smart cities, industrial automation, transportation, agriculture, and environmental monitoring. Through the integration of sensors, wireless communication protocols, and cloud-based analytics, IoT devices facilitate real-time data collection and intelligent decision-making. However, the exponential growth of IoT deployments has simultaneously expanded the cyber-attack surface, making IoT networks increasingly vulnerable to sophisticated security threats. Unlike traditional computing systems, IoT devices are often constrained by limited computational resources, inadequate storage capacity [1], weak authentication mechanisms, and infrequent software updates, rendering them attractive targets for cybercriminals.

Traditional security solutions, including signature-based Intrusion Detection Systems (IDS), firewalls, and antivirus software, have proven insufficient for protecting heterogeneous IoT environments. These approaches rely heavily on predefined attack signatures and manually crafted rules, limiting their effectiveness against zero-day threats and evolving malware variants [2]. Furthermore, the dynamic nature of IoT traffic, characterized by high volume, diverse communication protocols, and continuously changing behavioral patterns, necessitates the development of intelligent and adaptive security mechanisms. Consequently, Machine Learning (ML) and Deep Learning (DL) techniques have gained significant attention as promising solutions for enhancing IoT security through automated threat detection and classification [3].

Machine learning approaches provide the capability to identify hidden patterns and anomalies within network traffic without relying exclusively on prior knowledge of attacks. Algorithms such as Support Vector Machines (SVM), Random Forest (RF), Decision Trees (DT), and XGBoost have demonstrated substantial improvements in intrusion detection accuracy [4]. More recently, deep learning architectures, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Transformer models, have shown remarkable potential

in learning complex relationships from high-dimensional network data. CNNs are particularly effective in extracting local spatial features, while Transformer architectures excel at capturing long-range dependencies through self-attention mechanisms.

To address these limitations, this research proposes a lightweight CNN–Transformer-based intrusion detection framework for IoT botnet detection. The proposed approach leverages the feature extraction capabilities of CNNs and the contextual learning strength of Transformer networks to enhance classification performance. Furthermore, techniques such as synthetic data generation and class-weighted learning are incorporated to mitigate class imbalance and improve model robustness [5]. The attention mechanism within the Transformer architecture also contributes to improved interpretability, enabling better understanding of the decision-making process.

The primary objective of this study is to develop an intelligent, scalable, and efficient intrusion detection framework capable of accurately distinguishing between benign and malicious IoT traffic. By integrating advanced deep learning techniques with robust preprocessing and evaluation strategies, the proposed framework aims to strengthen the security posture of IoT ecosystems and contribute toward the development of adaptive cybersecurity solutions for future interconnected environments.

II. RELATED WORK

The rapid proliferation of Internet of Things (IoT) devices has significantly transformed modern digital ecosystems while simultaneously introducing numerous security and privacy challenges. Ataullah and Chauhan [1] presented a comprehensive review of IoT security enhancement technologies, emphasizing the importance of privacy preservation, authentication mechanisms, and intelligent threat mitigation strategies. Similarly, Qudus [2] analyzed emerging cybersecurity threats in evolving digital and IoT environments and highlighted the necessity of adaptive security frameworks to address sophisticated attacks. Amoo et al. [3] further investigated contemporary cybersecurity threats affecting IoT systems and reviewed protective measures, concluding that traditional security mechanisms are insufficient against increasingly complex cyberattacks. Patel et al. [4] examined cybersecurity risks associated with IoT devices and discussed various countermeasures, including intrusion detection systems and access control techniques, to mitigate vulnerabilities in heterogeneous IoT environments. Additionally, Sotnik [5] explored the integration of IoT into security systems, emphasizing both its opportunities and inherent risks in large-scale deployments.

Botnet attacks remain among the most severe threats to IoT ecosystems. Asadi et al. [6,14] conducted an extensive survey on evolving botnet threats and corresponding defense mechanisms, identifying challenges such as adaptive malware, decentralized botnet architectures, and zero-day exploits. Sutheekshan et al. [7] investigated the evolution of malware targeting IoT devices and demonstrated how compromised devices are recruited into botnets for malicious activities, including Distributed Denial-of-Service (DDoS) attacks and credential theft. Almazarqi et al. [8] proposed BotPro, a data-driven framework for tracking and profiling IoT botnets in real-world environments, while Almazarqi [9] provided an in-depth doctoral study on profiling IoT botnet activity and its behavioral characteristics. These studies collectively indicate that IoT botnets continue to evolve in complexity, necessitating intelligent and scalable detection methodologies.

Authentication failures and insecure communication mechanisms have been identified as major contributors to IoT vulnerabilities. Guo et al. [10] examined authentication schemes in IoT environments and revealed fundamental reasons behind their inability to achieve desired security objectives. Furthermore, Almutairi and Sheldon [11] investigated security challenges associated with IoT-cloud integration and highlighted issues related to data confidentiality, access control, and secure communication. Szymoniak et al. [12] reviewed existing defense and security mechanisms in IoT, whereas Hossain et al. [13] presented a holistic analysis of IoT security principles, practices, and emerging perspectives. Their findings emphasize the need for integrated and adaptive cybersecurity solutions capable of addressing evolving threats across interconnected infrastructures.

Several researchers have focused specifically on botnet detection and anomaly identification techniques. Gelgi et al. [15] systematically reviewed IoT botnet DDoS attacks and evaluated existing detection methodologies, concluding that machine learning-based approaches outperform traditional signature-based systems. Wahab et al. [16] discussed the role of Artificial Intelligence (AI) in IoT security and highlighted future prospects of intelligent cyber defense mechanisms. Panigrahi and De Albuquerque [17] emphasized the significance of big data analytics and edge intelligence for strengthening cybersecurity frameworks. Affinito et al. [18] conducted a six-year longitudinal study of Mirai botnet scans and demonstrated the persistent evolution of Mirai variants across multiple network ports. Similarly, Mansour et al. [19] presented a comprehensive survey on recent advancements in botnet detection and mitigation strategies, identifying machine learning, deep learning, and hybrid approaches as promising solutions for future IoT environments.

Foundational studies have also contributed significantly to understanding IoT security challenges. Mahmoud et al. [20] provided one of the earliest comprehensive analyses of IoT security issues, highlighting challenges related to scalability, privacy, and device heterogeneity. Hassan et al. [21] surveyed IoT security attacks, vulnerabilities, and countermeasures, while Tariq et al. [22] critically analyzed existing cybersecurity techniques and outlined future research directions for secure IoT ecosystems. Silva et al. [23] presented a seminal survey on botnets, establishing a foundation for subsequent botnet research. More recently, Morshedi et al. [24] reviewed deep learning-based anomaly detection techniques for IoT networks and identified challenges associated with interpretability and computational overhead.

The security of Industrial Internet of Things (IIoT) and Operational Technology (OT) systems has gained considerable attention in recent years. Stouffer et al. [25] developed the NIST guidelines for OT security, providing standardized recommendations for securing industrial infrastructures. Kwon et al. [26] and Feng et al. [27] comprehensively analyzed cybersecurity threats and defense strategies for IIoT environments, emphasizing the importance of intelligent intrusion detection mechanisms. Finally, Alieyan et al. [28] surveyed botnet detection techniques and highlighted key research challenges, including scalability, adaptability, and the need for lightweight detection frameworks. Collectively, the reviewed literature demonstrates substantial progress in IoT security; however, challenges such as evolving botnet behavior, resource constraints, and real-time detection capabilities remain open research problems, motivating the development of advanced deep learning-based intrusion detection systems.

III. RESEARCH METHODOLOGY

a. Data Acquisition and Preprocessing

The BoT-IoT dataset was utilized for experimental analysis, followed by data cleaning, normalization, and preprocessing to ensure data consistency. Class imbalance was addressed using GAN-based synthetic data generation, selective down-sampling, and class-weighted learning. Subsequently, the processed dataset was partitioned into training and testing subsets to facilitate robust model development and unbiased performance evaluation.

b. Feature Engineering and Data Balancing

Feature engineering involved the application of Particle Swarm Optimization (PSO) and Gorilla Troops Optimization (GTO) to identify ten discriminative features for the baseline model. GAN-based synthetic data generation and selective down-sampling addressed class imbalance, while weighted loss optimization and learned feature representations enhanced the performance of the deep learning architectures.

c. Development of Deep Learning Architectures

This study developed two deep learning architectures for effective IoT botnet detection under highly imbalanced traffic conditions. The first architecture integrated Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) networks to exploit both spatial and temporal characteristics of network traffic. The second and proposed architecture combined CNN with Transformer networks to leverage self-attention mechanisms for capturing long-range dependencies among traffic features. CNN layers were utilized for automatic feature extraction and dimensionality reduction, while the Transformer enhanced contextual understanding and model interpretability. Comparative analysis demonstrated that the CNN–Transformer architecture provides superior attack detection performance, improved generalization capability, and lower computational complexity. Figure 1 illustrates the complete workflow of IoT botnet detection, encompassing BoT-IoT data acquisition, preprocessing, class imbalance mitigation, and preparation of balanced datasets for subsequent deep learning model training and evaluation.

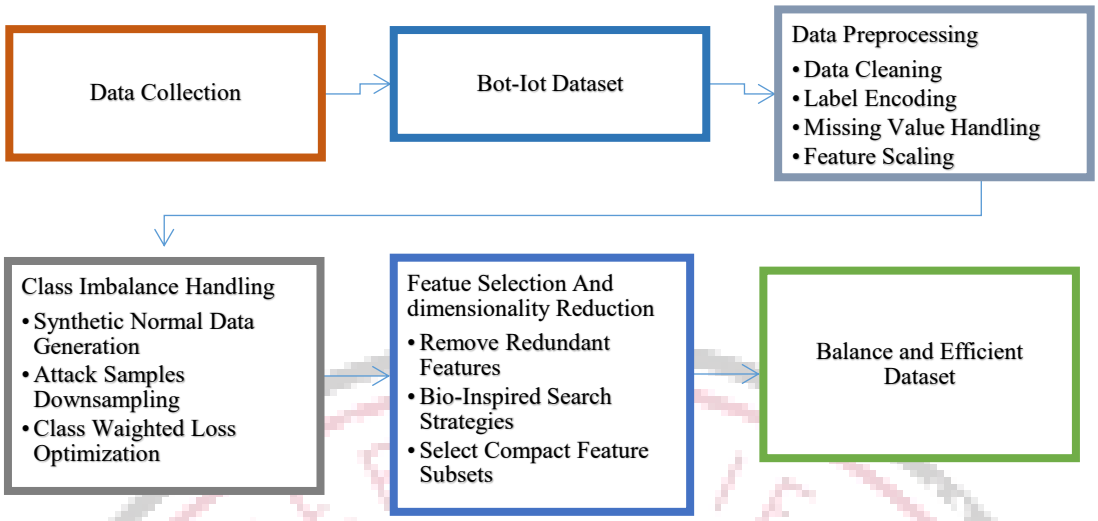

Figure 1: Flowchart of Data Collection, Pre-processing, and Class Imbalance Handling for IoT Botnet Detection

d. Model Training and Validation Strategy

This study employed a structured model training and validation strategy to ensure reliable performance assessment of the developed architectures. Hyperparameters were configured empirically to optimize learning efficiency and convergence. The models were trained on the preprocessed BoT-IoT dataset and evaluated using unseen test samples. Performance monitoring was conducted throughout the training process using standard evaluation metrics, while computational complexity was analyzed by comparing the processing overhead and architectural efficiency of the CNN–LSTM and CNN–Transformer models, highlighting the lightweight nature and scalability of the proposed framework.

e. Performance Evaluation Framework

Accuracy

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Where, TP = True Positives (correctly classified diseased leaves), TN = True Negatives (correctly classified healthy leaves),FP = False Positives (healthy leaves misclassified as diseased), FN = False Negatives (diseased leaves misclassified as healthy)

Precision

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

Recall

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

F1-Score

$$\text{F1-Score} = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

Confusion Matrix

The confusion matrix gives a detailed view of the results of classification by showing how many true positives, false positives, true negatives, and false negatives there are. It enables you to visualize the errors made during classification and helps in calculating other measures of performance.

Macro Average

Macro averaging includes calculating the evaluation metric for each class individually followed by taking an average of all these values. The macro averaging technique treats all classes equally, regardless of the number of samples in each class.

$$\text{Macro Average} = \frac{1}{N}\sum_{i=1}^{N} Metrics_i \quad (5)$$

Where N denotes the number of classes.

Weighted Average

$$\text{Weighted Average} = \frac{\sum_{i=1}^{N}(Metrics_i \times Support_i)}{\sum_{i=1}^{N} Support_i} \quad (6)$$

ROC Curve and Area under the Curve (AUC)

The ROC curve explains the relationship between the True Positive rate and the False Positive rate at various classification thresholds. The area under the curve is an indicator of the discriminatory power of the model. The closer the AUC is to 1, the better the classification ability of the model; the closer it is to 0.5, the worse.

IV. RESULT AND DISCUSSION

a. Results of CNN-Transformer-Based Model

From the results obtained from the balanced dataset, the proposed CNN-Transformer model performed very well in classifying IoT network traffic. During the training and evaluation of the model, it was evident that it was able to handle both normal and malicious traffic without any error.

- **Model Performance**

In addition to that, the model CNN-Transformer had 98.67% accuracy in training and 98.70% in the testing stage, which shows that the model is highly generalized. The model went through 15 epochs, and in the learning process, there were improvements in training accuracy and validation accuracy as well. During the training period, the learning process was fast in the first few epochs.

- **Class-wise Performance**

The model got 58.91% precision, 100% recall, and 74.14% F1-score for normal traffic. Even though the precision rate was low, but it means that all normal traffic data were predicted by the model correctly, which is very important for avoiding any misclassification. For attack traffic, the model got 100% precision, 98.67% recall, and 99.33% F1-score, which proves the model's high accuracy in predicting the vast majority of attack traffic. In addition, from the macro average values of precision, recall, and F1-score, we can say that the model performed well on both classes, with a little bit higher performance in attack prediction, which was expected due to the high-class imbalance. Additionally, the weighted average measures support the effectiveness of the model in detecting the majority attack class.

- **Classification Performance**

Table 1: Performance Metrics of CNN-Transformer-Based Model on Balanced Validation Set

Class	Precision	Recall	F1-Score	Support
Normal (0)	0.5891	1.0000	0.7414	119
Attack (1)	1.0000	0.9867	0.9933	6251
Macro Avg	0.7946	0.9934	0.8674	6370
Weighted Avg	0.9923	0.9870	0.9886	6370

The accuracy of normal traffic (Class 0) is 58.91%, implying that among all cases predicted as normal traffic by the classifier, 58.91% cases are indeed accurately categorized. The comparatively poor accuracy rate could be attributed to the nature of the data and the difficulties associated with differentiating normal traffic from attack traffic. However, the recall of normal traffic is 100%, meaning that the model correctly detects all normal traffic cases and does not misclassify any normal traffic cases as attack cases. The F1 score of normal traffic is 74.14%. While the accuracy is low, the excellent recall rate guarantees that no normal traffic case will go undetected. For the attack traffic (Class 1), the accuracy is 100% in that all attacks predicted are actual attacks. This shows that the model is effective at reducing false positive rate since there is no instance where normal traffic has been misclassified as attack traffic. For attack traffic, the recall is 98.67% which means that the model successfully detected 98.67% of the attacks present in the dataset. However, 1.33% of attack traffic instances have been wrongly classified by the model. The F1-score of attack traffic is 99.33%. The accuracy of the whole model is 98.70%, which indicates that the model classified 98.70% of the total number of traffic as correct. This level of accuracy of the model can be attributed to the excellent classification rate for attack traffic and the perfect recall rate of normal traffic, ensuring that no normal traffic is labelled as attack traffic. However, the macro average measures that are computed by taking an average of the performance measures regardless of class imbalance are 79.46% precision, 99.34% recall, and 86.74% F1-score. This indicates that the classifier is performing well on both classes, although with a bit of bias towards attack traffic, which has more samples in the dataset than the normal traffic.

- **Confusion Matrix Analysis**

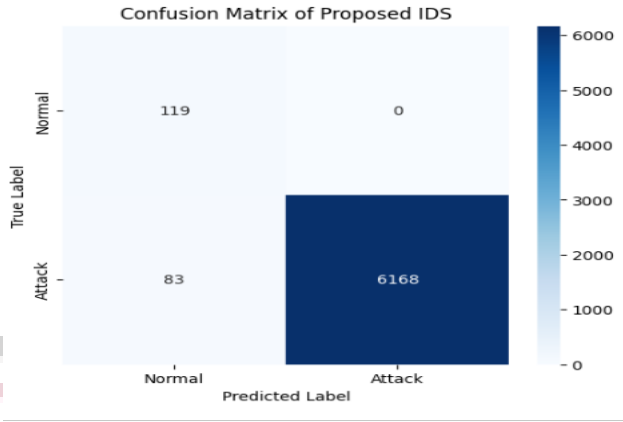

Figure 2: Performance Metrics of Proposed Model CNN–Transformer Model

Figure 2 explains the performance of the proposed CNN–Transformer model in detecting IoT botnet attacks, highlighting its superior accuracy, precision, recall, F1-score, and zero false-positive rate. Figure 3 explains the distribution of training and testing samples used in the study, illustrating the partitioning of the BoT-IoT dataset for effective model training, validation, and unbiased performance evaluation.

- **Training and Testing Set Distribution**

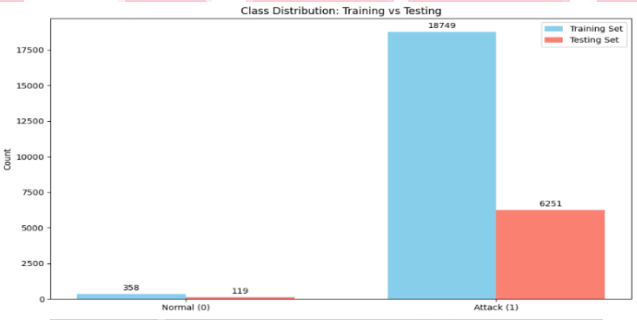

Figure 3: Training and Testing Set Distribution

In the training set, attack traffic (Class 1) dominates with 18,749 samples, while normal traffic (Class 0) consists of only 358 samples. This highlights the significant class imbalance in the training data, where the attack traffic heavily outnumbers normal traffic. This imbalance presents a challenge for the model, as it may tend to predict the majority class (attack traffic) more frequently, potentially leading to a biased model that struggles to recognize normal traffic behaviour. The testing set also exhibits a class imbalance, with 6,251 attack traffic samples and 119 normal traffic samples. However, the proportions of normal and attack traffic are similar to those seen in the training set. This balanced distribution of classes in the testing set is essential to evaluate the model's performance fairly, ensuring that the model is assessed on its ability to classify both classes correctly. The test set contains enough normal traffic samples to validate the model's generalization capability.

- **Training vs. Validation Loss and Training vs. Validation Accuracy:**

Figure 4 explains the training and validation accuracy of the proposed model across multiple epochs, demonstrating its learning capability, convergence behavior, and generalization performance during the training process. Figure 5 explains the training versus validation accuracy and loss trends of the proposed model, illustrating stable convergence, effective learning, and the absence of significant overfitting throughout the training process.

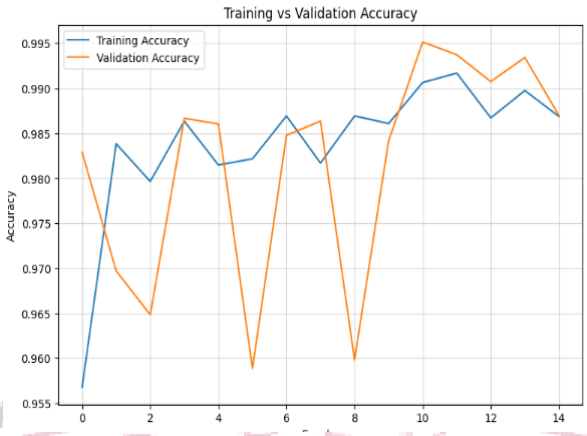

Figure 4: Training vs. Validation Accuracy

The trend in the first graph of training loss (blue line) is downward, meaning that the model is learning and developing. Nonetheless, there seems to be fluctuations, especially at the beginning of the training when the loss goes up before going down. This might mean that the model was having challenges with over fitting in the initial stages. The validation loss (orange curve) is more varied than the training loss. It can be observed that even though the performance of the model on the training set keeps on improving, the performance of the model on the validation set does not remain constant. The spikes in the validation loss might denote the points at which the model starts to over fit. It is observed that there is an increment, which denotes that the model starts to memorize the data instead of learning from it.

- **Training vs Validation Accuracy:**

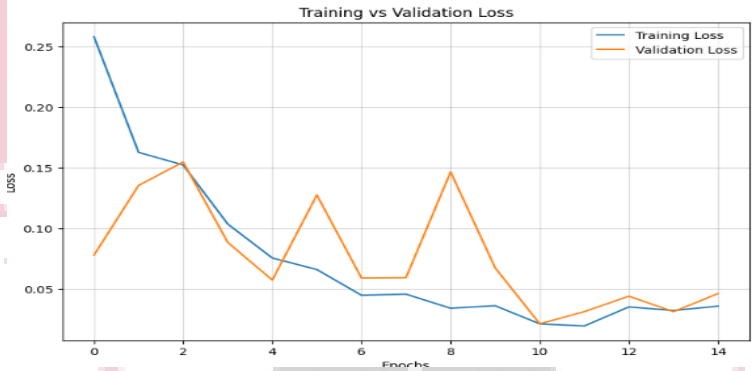

Figure 5: Training vs. Validation Accuracy and Training vs. Validation Loss

The second plot depicts the performance statistics of training and validation. Training accuracy (represented by the blue line) keeps on increasing as the training process progresses and reaches up to 99% at the end. This indicates that the model has learned well from the training set. Unlike the training accuracy, the validation accuracy (represented by the orange line) varies more widely across the different epochs. Although it exhibits an increasing trend just like the training accuracy, the increase in validation accuracy is less consistent than the increase in training accuracy. The fact that validation accuracy varies indicates that the model's generalization capacity may not be optimal at some points, perhaps as a result of over fitting at some other points. However, peaks in validation accuracy show instances when the model's generalization capability is optimal.

b. Proposed CNN-Transformer Model and the Base Paper Model (CNN-LSTM)

Table 2: Comparison table for the Proposed CNN-Transformer Model and the Existing Model (CNN-LSTM)

Metric	Base Paper Model (CNN-LSTM)	Proposed CNN-Transformer Model
Training Accuracy	97.66%	98.67%

Testing Accuracy	97.73%	98.70%
Precision (Normal Traffic)	95.66%	58.91%
Precision (Attack Traffic)	100%	100%
Recall (Normal Traffic)	100%	100%
Recall (Attack Traffic)	95.47%	98.67%
F1-Score (Normal Traffic)	97.78%	74.14%
F1-Score (Attack Traffic)	97.68%	99.33%
False Positive Rate (FPR)	0%	0%
Macro Average F1-Score	97.83%	86.74%
Weighted Average F1-Score	97.83%	98.86%

Table 2 explains the comparative performance analysis between the proposed CNN–Transformer model and the existing CNN–LSTM model, highlighting improvements in accuracy, recall, precision, computational efficiency, and overall IoT botnet detection capability. Training and Testing Accuracy for the two models is high, with the Proposed CNN-Transformer Model performing slightly better than the Existing Model. The Proposed Model attains 98.67% for training accuracy and 98.70% for testing accuracy, whereas the Base Model attains 97.66% and 97.73%, respectively. Both models attain 100% accuracy on attack traffic; however, the Proposed Model has low precision of 58.91% on normal traffic because of class imbalance, while the Base Paper Model has a higher precision of 95.66%. Nonetheless, the Proposed Model offsets this with 100% recall of normal traffic, making sure no normal traffic is overlooked. In terms of recall, both models have a perfect recall of normal traffic. In terms of attack traffic, the CNN-Transformer Model has a much higher recall of 98.67% compared to that of the Base Model of 95.47%. The Existing Model yields a higher F1-score of 97.78% in case of normal traffic, but the Proposed Model outperforms in attack traffic by providing an F1-score of 99.33% as against 97.68% of the Existing Model. This means that there is greater balance between precision and recall in attack traffic for the Proposed Model. Both models yield 0% False Positive Rate (FPR) which is very important to avoid false alarms. In terms of average F1-scores, the Base Paper Model shows a higher macro F1-score of 97.83%, whereas the Proposed Model performs better in terms of weighted average F1-score of 98.86%. the CNN-Transformer Model is a superior choice as it outperforms in attack traffic and class imbalance.

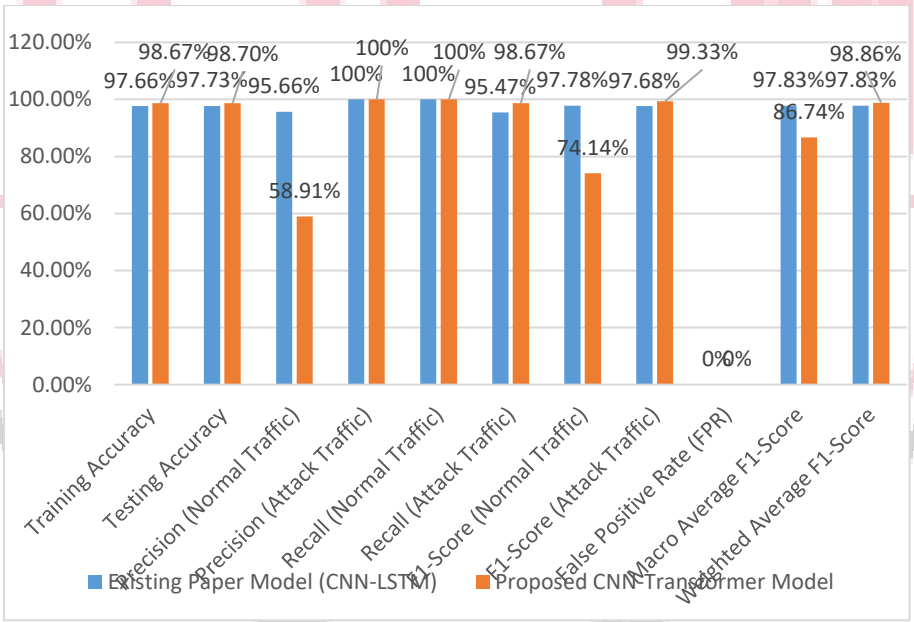

Figure 6: Comparison between the Baseline Model (CNN+LSTM) and the Proposed CNN-Transformer Model

Figure 6 explains the comparative performance of the baseline CNN–LSTM model and the proposed CNN–Transformer model, demonstrating the superiority of the proposed approach in terms of accuracy, attack detection capability, and overall classification performance. Comparisons of the Baseline Model (CNN+LSTM) and the Proposed CNN-Transformer Model reveal some major differences in terms of their performance based on such metrics as accuracy, recall, precision, F1-score, and False Positive Rate (FPR). As regards recall, the baseline model gets 83.7% recall while the proposed model scores a considerably higher recall score of 98.67%. The performance difference clearly reflects the greater ability of the proposed model to detect attack traffic and thus avoids any miss-detected cases. High recall rate is especially significant in intrusion detection systems since missing attacks can have a devastating impact on system security. Both models show excellent

precision in classifying the attack traffic, but the proposed model gives 100% precision, surpassing the baseline model with a score of 96%. This shows that the proposed architecture makes less mistakes while predicting attacks, hence making it easier to distinguish between legitimate and illegitimate traffic and increasing the accuracy of prediction results. The F1-score serves to highlight the efficiency of the proposed method. The proposed CNN-Transformer model achieves an F1 score of 99.33% in case of attacks traffic, which is a lot better than the F1 score of 87.1% achieved by the baseline model. Such a measure shows the right balance between the two parameters of precision and recall and shows the stability and consistency of the proposed method from both perspective.

V. CONCLUSION AND FUTURE WORK

In this work, two deep learning-based intrusion detection frameworks were developed to address IoT botnet attacks under highly imbalanced network traffic conditions. The first framework integrated bio-inspired feature selection techniques, Generative Adversarial Network (GAN)-based data augmentation, and a hybrid CNN-LSTM architecture, achieving 98.38% classification accuracy with 100% recall for normal traffic and zero false positives. The second and proposed framework employed a lightweight CNN–Transformer architecture that leveraged convolutional feature extraction and Transformer-based self-attention mechanisms to capture both local and global traffic dependencies. Experimental evaluation on the BoT-IoT dataset demonstrated that the proposed model outperformed the baseline approach, achieving 98.70% accuracy, 98.67% attack recall, and 100% attack precision while maintaining zero false positives. Comparative analysis revealed that the CNN–Transformer model offers superior generalization capability and computational efficiency, making it highly suitable for real-time IoT environments. These findings confirm the effectiveness of hybrid deep learning approaches in enhancing IoT botnet detection and strengthening cybersecurity resilience in next-generation interconnected systems.

References

[1] Ataullah, M., & Chauhan, N. (2024). Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. *Security and Privacy*, *7*(6), e448. https://doi.org/10.1002/spy2.448

[2] Qudus, L. (2025). Advancing cybersecurity: strategies for mitigating threats in evolving digital and IoT ecosystems. *Int Res J Mod Eng Technol Sci*, *7*(1), 3185. https://www.doi.org/10.56726/IRJMETS66504

[3] Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive*, *11*(1), 1304-1310. https://doi.org/10.30574/ijsra.2024.11.1.0217

[4] Patel, K. N., Ashok, P., Chirputkar, A., & Pillai, S. (2024, November). Cybersecurity risks and countermeasures in the threat landscape of IoT devices. In *2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS)* (pp. 875-883). IEEE. https://doi.org/10.1109/ICTACS62700.2024.10841210

[5] Sotnik, S. V. (2024). Integration of IoT into security systems: opportunities and risks. *International Journal of Academic Engineering Research (IJAER)*.

[6] Asadi, M., Jamali, M. A. J., Heidari, A., & Navimipour, N. J. (2024). Botnets unveiled: A comprehensive survey on evolving threats and defense strategies. *Transactions on Emerging Telecommunications Technologies*, *35*(11), e5056. https://doi.org/10.1002/ett.5056

[7] Sutheekshan, B., Basheer, S., Thangavel, G., & Sharma, O. P. (2024, February). Evolution of malware targeting IoT devices and botnet formation. In *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)* (Vol. 5, pp. 1415-1422). IEEE. https://doi.org/10.1109/IC2PCT60090.2024.10486705

[8] Almazarqi, H. A., Woodyard, M., & Marnerides, A. K. (2025). BotPro: Data-driven Tracking & Profiling of IoT Botnets in the Wild. *Computers & Security*, 104778.

[9] Almazarqi, H. (2024). *Profiling IoT botnet activity* (Doctoral dissertation, University of Glasgow).

[10] Guo, Y., Guo, Y., Xiong, P., Yang, F., & Zhang, C. (2024). Deeper insight into why authentication schemes in IoT environments fail to achieve the desired security. *IEEE Transactions on Information Forensics and Security*, *19*, 4615-4627.

[11] Almutairi, M., & Sheldon, F. T. (2025). IoT–cloud integration security: A survey of challenges, solutions, and directions. *Electronics*, *14*(7), 1394.

[12] Szymoniak, S., Piątkowski, J., & Kurkowski, M. (2025). Defense and security mechanisms in the internet of things: A review. *Applied Sciences*, *15*(2), 499.

[13] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. (2024). A holistic analysis of internet of things (IoT) security: principles, practices, and new perspectives. *Future Internet*, *16*(2), 40.

[14] Asadi, M., Jamali, M. A. J., Heidari, A., & Navimipour, N. J. (2024). Botnets unveiled: A comprehensive survey on evolving threats and defense strategies. Transactions on Emerging Telecommunications Technologies, 35(11), e5056.

[15] Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques. Sensors, 24(11), 3571.
[16] Wahab, F., Khan, M., Ullah, I., & Tao, Y. (2024). Artificial Intelligence in the Internet of Things, Recent Challenges and Future Prospects. Future Communication Systems Using Artificial Intelligence, Internet of Things and Data Science, 3-17.
[17] Panigrahi, R., & De Albuquerque, V. H. C. Big Data and Edge Intelligence for Enhanced Cyber Defense.
[18] Affinito, A., Zinno, S., Stanco, G., Botta, A., & Ventre, G. (2023). The evolution of Mirai botnet scans over a six-year period. Journal of Information Security and Applications, 79, 103629.
[19] Mansour, R. F., Escorcia-Gutierrez, J., Gandomi, A. H., Gupta, B. B., & Kumar, N. (2024). Recent Advances in Botnet Detection and Mitigation: A Comprehensive Survey. Journal of Network and Computer Applications, 233, 103938.
[20] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. A. (2015). Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 336–341. https://doi.org/10.1109/ICITST.2015.7412116.
[21] Hassan, M. M., Gumaei, A., Huda, S., & Fortino, G. (2024). A Comprehensive Survey on IoT Security Attacks, Vulnerabilities, and Countermeasures. Computer Networks, 248, 110487.
[22] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8), 4117.
[23] Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., & Salles, R. M. (2013). Botnets: A Survey. Computer Networks, 57(2), 378–403. https://doi.org/10.1016/j.comnet.2012.07.021.
[24] Morshedi, M., Ahmadi, M., & Ghorbani, A. A. (2025). Deep Learning-Based Anomaly Detection in IoT Networks: A Comprehensive Review. Journal of Network and Computer Applications, 240, 104089.
[25] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2023). Guide to Operational Technology (OT) Security (NIST Special Publication 800-82 Revision 3). National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-82r3.
[26] Kwon, Y., Kim, D., & Kim, H. (2024). Cybersecurity Threats and Defense Strategies for Industrial Internet of Things: A Comprehensive Survey. Journal of Industrial Information Integration, 39, 100602. https://doi.org/10.1016/j.jii.2024.100602.
[27] Feng, C., Yan, J., Liu, Y., Loukas, G., & Spyridopoulos, T. (2024). Cybersecurity for Industrial Internet of Things: Threats, Detection Techniques, and Future Research Directions. Computers & Security, 138, 103639. https://doi.org/10.1016/j.cose.2024.103639.
[28] Alieyan, K., Almomani, A., Anbar, M., Abdullah, R., & Alauthman, M. (2023).Botnet Detection Techniques: A Comprehensive Survey and Research Challenges. Journal of Information Security and Applications, 76, 103520.https://doi.org/10.1016/j.jisa.2023.103520.