SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X VOLUME 4, ISSUE 5, 2026

A BINARY AND FAMILY CLASSIFICATION INTRUSION DETECTION FRAMEWORK FOR IOT USING TRANSFORMER CNN HYBRID DEEP LEARNING

Hasaan Haider[*1], **Husnain Butt**[2]

[*1,2]*School of systems & Technology, University of Management & Technology Lahore, Lahore Pakistan*

[*1]hasaanhaider3@gmail.com, [2]husnainbutt399@gmail.com

DOI: https://doi.org/10.5281/zenodo.20717026

Keywords
IOT devices, Transformer-CNN, Deep learning, Family Classification, Cybersecurity

Article History
Received: 03 April 2026
Accepted: 15 May 2026
Published: 30 May 2026

Corresponding Author: *
Hasaan Haider

Abstract
The proliferation of Internet of Things (IoT) devices has expanded the attack surface for cyber threats, necessitating robust and intelligent Intrusion Detection Systems (IDS). Traditional machine learning models often struggle to capture complex, non-linear spatial and temporal dependencies in high volume network traffic. This research proposes a novel hybrid Deep Learning framework integrating 1D Convolutional Neural Networks (1D-CNN) and Transformer architectures. The 1D-CNN component is utilized to extract local feature correlations from tabular network flows, while the Transformer mechanism captures global context and long-range dependencies. The model will be trained and evaluated on the CICIoT2023 dataset, addressing class imbalance through SMOTE (Synthetic Minority Over-sampling Technique). The proposed framework aims to achieve state-of-the-art accuracy in both Binary Classification (Benign vs. Malicious) and Family Classification (DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, Mirai), providing a granular and actionable security solution for modern IoT environments.

I. INTRODUCTION

One of the most significant technological changes of the 21st century is the process of the Internet of Things (IoT) implementation in both critical infrastructures and industrial processes and everyday life. Nevertheless, such ubiquity has spawned a security paradox: the systems that have become the foundation of the operational efficiency and data-driven decision-making are becoming more the weakest links in the global cybersecurity chain[1]. By 2025, the number of connected devices has grown exponentially to enable a hyper-connected ecosystem that is inherently vulnerable, heterogeneous due to a limited number of device resources, and vulnerable by default to a pervasive security by design shortfall. In this unstable environment, this study suggests a new model that can be used to solve the shortcomings of the existing Intrusion Detection Systems (IDS). The proposed hybrid Deep Learning (DL) architecture, which combines the 1D Convolutional Neural Networks (1D-CNN) with the mechanisms of Transformer, is expected to combine the efficiency of local feature extraction with CNN's and the global context-awareness of Transformers[2]. The proposed model addresses two different classification tasks with the help of the most up-to-date CICIoT2023 dataset: Binary Classification (benign vs. malicious) and Family Classification (differentiating attacks belonging to the following families: DDoS, DoS, Reconnaissance, Web-based, Brute Force,

Spoofing, and Mirai). The proposed model will change the IDS into a generator of actionable intelligence by shifting away the binary detection to Family Classification, thus turning the IDS into a passive alarm. Granular classification allows Security Orchestration, Automation, and Response (SOAR) tools to initiate playbooks such as isolating an infected device infected with Mirai versus cleaning traffic of a volumetric DDoS. As an average cost of an industrial breach is estimated to be 5.56 million in the year 2025 1, there is a financial rationale of having an effective intrusion detection. The framework suggested offers a significant point of safety to the infrastructure that supports the contemporary society[3]. The combination of Transformers and CNN's in Tabular Network Traffic is a new area, even though they have already revolutionized the field of NLP. This paper substantiates the effectiveness of applying CNN's as tokenizers over Transformers in non-image tasks, acting as a reference architecture in time series anomaly detection.

II. BACKGROUND

It has been estimated that over 55 billion connected devices have been produced. This connectivity massiveness is unmeasured by security measures. Everyday, the IoT ecosystem in the year 2025 will withstand an average of 820,000 hacking attempts, which is 46 per cent higher than the past year. The development of the current threat environment is the shift of hostility toward IT to Operational Technology (OT). The trend in 2024, in which more than 50 percent of reported cyber incidents to the SEC were OT attacks, represents a harmful development since cyber-physical system disruption has become the goal of the attackers[4]. This feature of the ecosystem of the Internet of Things is the root cause of this crisis. It is estimated that 98 percent of IoT over-the-air traffic is unencrypted, which eases Man-in-the-Middle (MITM) and Spoofing attacks and 7.36 percent of identified attacks are brute force attacks targeting the ongoing default credential problem. Botnets are no longer viewed as simple volumetric engines as apps such as Mirai, but advanced platforms such as the so-called Mantis, which can discriminate between servers with precision HTTPS requests, as opposed to just blowing volume.1 This development requires an IDS that is able to identify not only volumetric anomalies (via CNN's) but also subtle changes in behaviours (via Transformers).

III.RESEACH QUESTIONS

This study is guided by four core inquiries designed to rigorously test the model's performance and operational viability:

- What is the effectiveness of a hybrid Transformer-CNN deep learning model in detecting intrusion attempts in IoT networks for both binary and multi-class attack classification?
- Which improvements in detection accuracy, precision, recall, and F1-score are achieved by combining Transformer and CNN architectures compared to traditional models?
- What specific impact does the hybrid model have on identifying distinct IoT attack families, such as distinguishing DoS from DDoS, in a multi-class setting?
- Which factors determine the capacity of the proposed Transformer-CNN model to maintain consistent performance levels when generalizing across heterogeneous IoT datasets and unseen network environments?

IV.LITERATURE REVIEW

Fast development of the Internet of Things (IoT) has radically altered the digital ecosystem of the present day by integrating networked intelligence into all common objects, industrial systems, medical structures, and smart cities. On one hand, this change has brought about unmatched efficiency and automation but on the other, it has increased the size of the cyber-attack surface at a concerning pace. It is projected that by 2025, there will be more than 55 billion connected IoT devices, producing a hyper-connected environment, led by heterogeneity, scale and poor in-built security[5]. The IoT devices, in contrast to traditional computing systems, sometimes have very tight restrictions in terms of memory, processing power, and energy usage, requiring more complex security controls like a strong encryption, round-the-clock monitoring, or regular patching to be deployed. This rigid and non-homogenous character of IoT settings has predisposed them to attacks by adversaries.

Numerous gadgets set up the default passwords, old software, or weak encryption standards, thus enabling mass usage. According to recent intelligence reports, the attempts at attacks on IoT ecosystems occur through hundreds of thousands of attacks per day, and the number of attacks and their complexity is growing steadily each year[6]. One of the most important changes that have been witnessed over the last few years is a transition of attacks on traditional Information Technology (IT) systems to Operational Technology (OT) and cyber physical systems. This shift is an indicator of shifting the goals of the attackers, the theft of data is transferred to the physical processes, the system of power distribution, manufacturing and transportation. DDoS attacks are still among the most common in the IoT environment primarily because devices with low security are easy to enlist in botnets[7]. Mirai was one of the first botnets to use default credentials to make traffic floods. Modern botnets have however adopted more intelligent forms than brute-force volumetric attacks, and currently use more intelligent, application-layer techniques, which create legitimate appearing traffic characteristics. Such attacks are much more difficult to notice, since they have the appearance of harmless behaviour but slowly drain system resources. Simultaneously, reconnaissance attacks, brute force authentication, spoofing, and web-based exploits have remained the most frequent attack types on the IoT gateways or cloud interfaces[8]. The unbalanced nature of real-world datasets also poses a significant problem in the field of IoT security. Popular publicly available datasets, such as CICIoT2023, are often overrepresented with samples of high-volume attack categories, such as DDoS and DoS. There is gross underrepresentation of the minority classes, including web-based attacks, or brute-force intrusions. This skewed learning causes bias to intrusion detection models, causing high overall accuracy at low detection performance of less frequent but equally important attack types. There is, therefore, an increasing agreement that intrusion detection systems (IDS) should go beyond the coarse-grained detection and fine-grained family-level classification to allow the use of response strategies that are precise and automated[9].

A. Limitations of Traditional Approaches

Classical intrusion detection systems can be generally classified as signature-based and anomaly-based systems. Signature-based IDS are based on the existing patterns or rules, which are based on known attack behaviours[10]. Although such systems can be used to limit attacks previously noticed, they will always fail to notice zero-day attacks or new forms of attacks having the same nature. In addition, it is not feasible to keep signature databases current in a large-scale IoT deployment because of device heterogeneity and constant evolution of attacks. Anomaly-based IDS are trying to address these shortcomings by attempting to model normal system behaviour and indicate abnormal behaviour as possible intrusion[11]. The systems used in the early anomaly-based anomaly detection used classical machine learning models, including Support Vector Machines (SVM), k Nearest Neighbours (k-NN), Decision Trees, and Random Forests. These systems although proved better than the signature-based systems have several disadvantages. Most prominently, to be effective, they need a lot of manual feature engineering, domain knowledge and tuning. The feature selection in high dimensional IoT traffic data is getting increasingly sophisticated, irrelevant or redundant features may cause a serious performance degradation[12]. The appearance of deep learning methods as an alternative to the previously mentioned one can be attributed to the fact that they are able to automatically learn hierarchical feature representations out of the raw or minimally processed data. A popular use of CNN's, and specifically one-dimensional CNN's, in network traffic analysis is due to their ability to capture local spatial correlations between features, e.g. packet-level statistics or flag distributions[13]. The CNN's are, however, necessarily constrained to local receptive fields and are unable to capture long-range interactions and interactions among features across a global scale. The introduction of Recurrent Neural Networks (RNN's) and Long Short-Term Memory (LSTM) networks was to deal with temporal dependencies of sequential

data. These models are computationally costly, hard to parallelize, and may develop vanishing or exploding gradients, although they are effective in theory[14]. They cannot be practically implemented in resource constrained IoT or edge environments. Moreover, the use of single-architecture models, either CNN or RNN, does not capture the duality of network traffic, having both local and global contextual dependence.

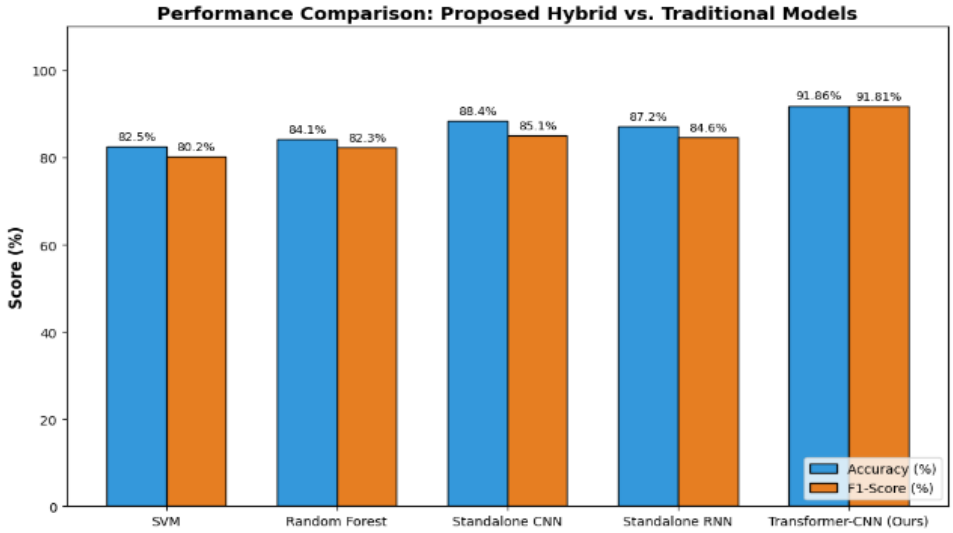

Fig. 1. Performance comparison of proposed system

B. **The Transformer and Hybrid Architectures**

Paradigm shift of the deep learning model observed with the introduction of the Transformer architecture is that recurrence is substituted by self-attention mechanisms. The importance of various input features of the model is computed by self-attention and is independent of their positional distance, thus Transformers are especially effective in capturing global dependencies. Transformers were initially created as a natural language processing model but have since been shown to perform well on tabular data (such as cybersecurity data) by capturing the complex interactions of features that cannot be captured by the traditional architecture. Transformers may not be the best to capture the fine-grained local patterns in network traffic features despite their strengths[15]. Consequently, hybrid architectures started to be given more attention in the literature on intrusion detection. The goal of these architectures is to combine the complementary capability of various deep learning models. Under a Transformer-CNN hybrid architecture, the CNN layers serve as local feature extractors, which learn the local correlations and provide feature one-level and higher-level embeddings. These embeddings are then inputted to Transformer encoders which conduct global reasoning by using multi-head self-attention. Experimental research has indicated that hybrid frameworks perform better than single architecture in the accuracy of detection, resilience to imbalance in classes, and reduction of false positives[16]. Trying to model local and global features of the IoT traffic together, the hybrid techniques are more appropriate to identify both the large-scale and the low-frequency attacks. This renders them especially appealing to actual IoT applications, where attack patterns have been diversified, evolved, and completely unequal.

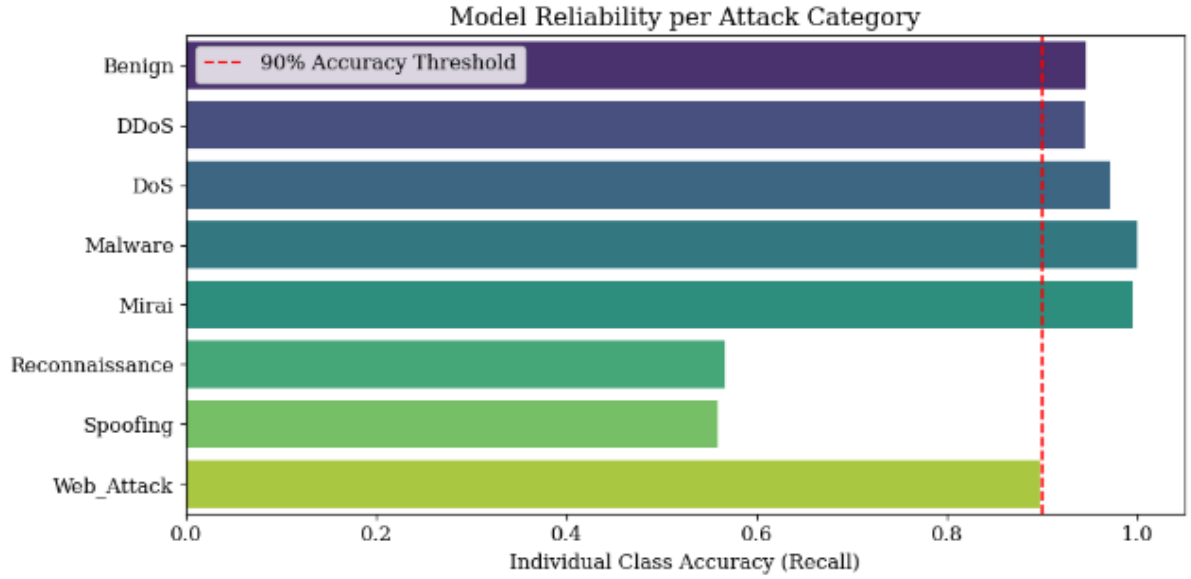

Fig. 2. Shows reliability against each attack

V. METHODOLOGY

This Study uses a quantitative, experimental research design to design and test a hybrid deep learning-based intrusion detector system to be used in IoT setups. The main aim is to examine the possibility of facilitating the performance of intrusion detection using one-dimensional Convolutional Neural Networks (1D-CNNs) together with Transformer encoders at binary and family classification levels[17]. Binary classification is used to differentiate between benign and malicious traffic, whereas family classification attempts to classify the malicious traffic into a particular set of attack families, such as DDoS, DoS, Reconnaissance, Web-based attacks, Brute Force, Spoofing, and Mirai. The suggested framework is tested during a set of controlled experiments based on a benchmark IoT dataset. The standard evaluation metrics that are used to make performance comparisons put into consideration the class imbalance and multi-class classification challenges. The design of the experiment focuses on reproducibility, robustness, and applicability to actual IoT security situations[18]. The CICIoT2023 dataset is used to perform an experimental evaluation because this dataset is a state-of-the-art benchmark that is specifically created to model the real-world traffic of an IoT network. The data were produced in a controlled testbed system comprising of 105 heterogeneous IoT devices, such as smart cameras, sensors, home automation hubs and consumer-grade IoT appliances. Traffic data was gathered in realistic conditions of normal operation and in various attack conditions to make it realistic and diverse. CICIoT2023 includes 33 different types of attacks, and it has seven major attack families except benign. All the network flows are modelled in terms of 47 extracted features including statistical, temporal, and protocol-level features. They have features such as, but not limited to, packet header lengths, flow rates, inter-arrival times (IAT), flag counters, and protocol-specific indicators[19]. These characteristics are exceptionally fitting in machine learning-based analysis and deep learning-based analysis since they can assume short-term traffic behaviour and aggregated flow-level patterns at the same time . One of the benefits of CICIoT2023 is that it reflects modern-day IoT attack techniques, such as volumetric and low-rate stealth attacks. Nonetheless, like most practical cybersecurity datasets, it is highly imbalanced, with volumetric attacks including DDoS prevailing in the dataset. The given characteristic requires cautious preprocessing and evaluation strategies, which are integrated into the suggested methodology.

A. Data Preprocessing

A stringent preprocessing pipeline is used before developing the model so that the data quality and model training are stable. First, any records

with missing (NaN) or infinite values due to anomalies in the computation of the flows are eliminated. This measure helps avoid the situation of numerical instability in training and provides the consistency of feature distributions[20]. The labels of the data sets are converted by label encoding (where benign traffic is labelled 0, and the seven attack families are labelled with integer values between 1 and 7). Such encoding scheme enables both binary and multi-class classification tasks to be performed using the same modelling scheme. All numerical features are Z-score normalized to give the features a mean of zero and a standard deviation of one. Deep learning models need normalization to achieve faster convergence, gradient updates, and features with large numeric ranges should not have an unfairly high impact on the process of learning. Since the likelihood of the occurrence of attack classes is tremendously disproportionate, the Synthetic Minority Over-sampling Technique (SMOTE) is only used on the training data. SMOTE creates pseudo instances of minority groups by interpolating between the closest samples in features space, to enhance the representation of the classes without creating redundant instances. Application of SMOTE to the training set only makes the validation and testing set free and unbiased of the real-world traffic distributions. The data will be divided into 70 percent training, 10 percent validation and 20 percent testing sets[21]. This division permits hyperparameter effective searching, model and training, without bias.

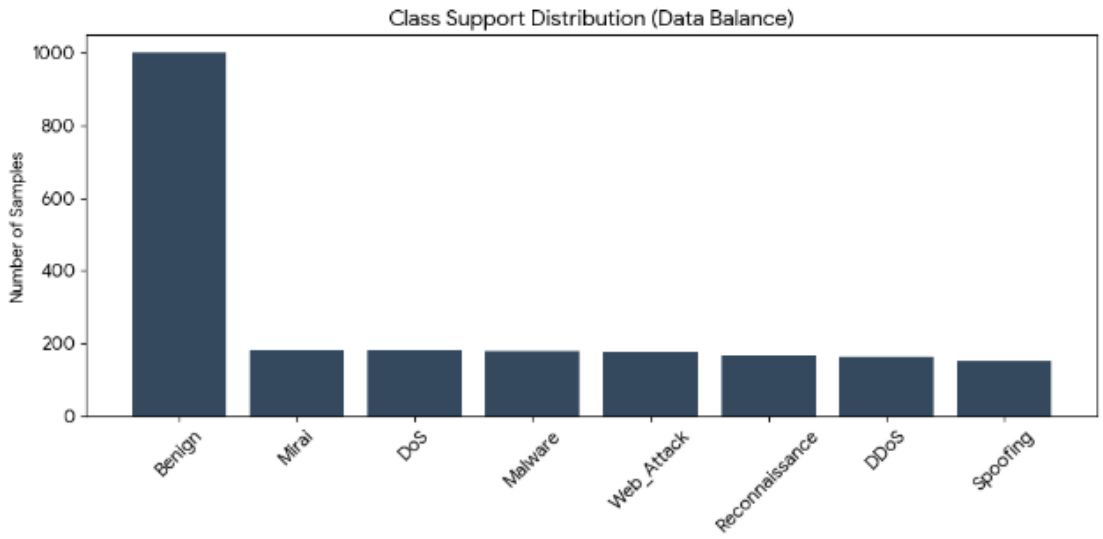

Fig. 3. Number of samples per attack

B. Proposed Hybrid Architecture

Suggested intrusion detection framework is designed as a three-stage hybrid deep learning model with the combination of convolutional and attention-based learning processes. The model input is a reformed feature image of size (Batch Size, 46, 1) with each feature image describing an individual network flow. Such a representation allows the use of one-dimensional convolution operations on the sequences of features[22]. The initial step in the model utilizes two 1D convolutional layers with activation functions of the Rectified Linear Unit (ReLU). The layers provide local feature extractors, which find short-range correlations between neighbouring traffic features, e.g., packet statistics and flag distributions. The convolutional layers are followed by a MaxPooling 1D layer to minimize the features dimension, intricate noise, and better generalization. The product of the CNN module is inputted into a Transformer encoder which employs the use of multi-head self attention to model long range dependencies and intricate feature interactions. In contrast to convolutional operations, which pay attention to local features, self-attention facilitates the model to evaluate the relative importance of

each feature considering all other features, irrespective of their positional distance[23]. This feature is especially useful in the case of the IoT traffic analysis, where world relationships between features tend to reflect highly complex attack patterns. After Transformer encoder, Global Average Pooling (GAP) layer is used to pool feature representations and make the computation more complex. The fully connected dense layers take the pooled output as input and dropout regularization (rate = 0.5) The last output layer application is the A Sigmoid activation function, used when classifying binary. Multi-class family classification with a SoftMax activation function[24].

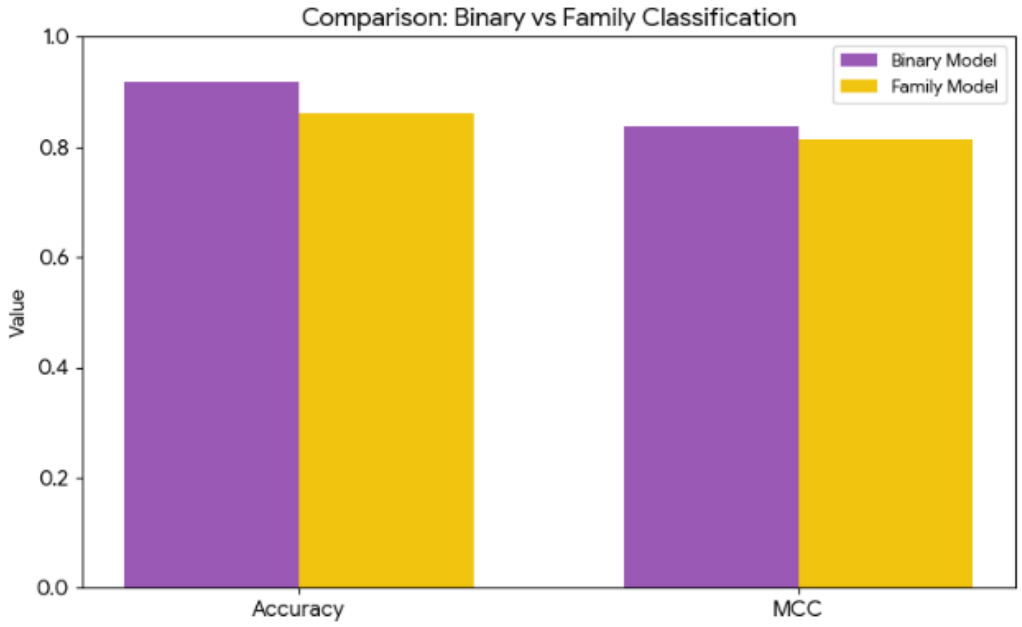

Fig. 4. Performance com parison of binary and family classification

C. Performance Metrics

As a result of the asymmetry of the IoT intrusion data, accuracy is not enough to assess the performance of the model. Consequently, in this paper, a set of measures, such as Precision, Recall, and Macro-averaged F1-score is used to make sure that the assessment of each of the classes is balanced[25]. The pattern of misclassification about various attack families is analysed using a Confusion Matrix, and this gives an insight into the weaknesses of the model and performance at the class level. Also, Receiver Operating Characteristic (ROC) curve and Area Under the Curve (AUC) are also used to evaluate the model discriminatory capacity in both binary and multi-class models. Lastly, there is inference latency which is calculated to assess the practicability of implementing the suggested framework in real-time or edge-based IoT setups. This makes the model much more than accurate but operational in the practical intrusion detection situations[26].

VI.RESULT

In this section, the performance and diagnostic effectiveness of the proposed Transformer-CNN hybrid framework to identify IoT network intrusions are assessed. The experimental analysis was performed with the state-of-the-art dataset CICIoT2023 that embraces a wide spectrum of benign operation and attack family variations that are produced due to the 105 heterogeneous IoT devices. To preprocess the data in the deep learning pipeline, network flows are modelled as reshaped feature tensors of size (Batch Size, 46, 1), which enables the model to process 46 statistical and protocol-level features using one-dimensional convolution and self-attention layers. To have a sound evaluation, the set was divided based on a standardized validation plan: 70% of the data was used to train, 10% to validate, and 20% to test. Since the volumetric attacks (e.g., DDoS) and the stealthy intrusions (e.g., Web-based attacks) have an inherent difference in their classes, the

Synthetic Minority Over-sampling Technique (SMOTE) was only applied to the training subset to obtain a balance between the classes in the models and avoid bias of the model. The performance of the framework was measured with a full set of performance measures, which are Accuracy, Precision, Recall, F1-score, Matthews Correlation Coefficient (MCC) and the Area Under the ROC Curve (ROC-AUC).

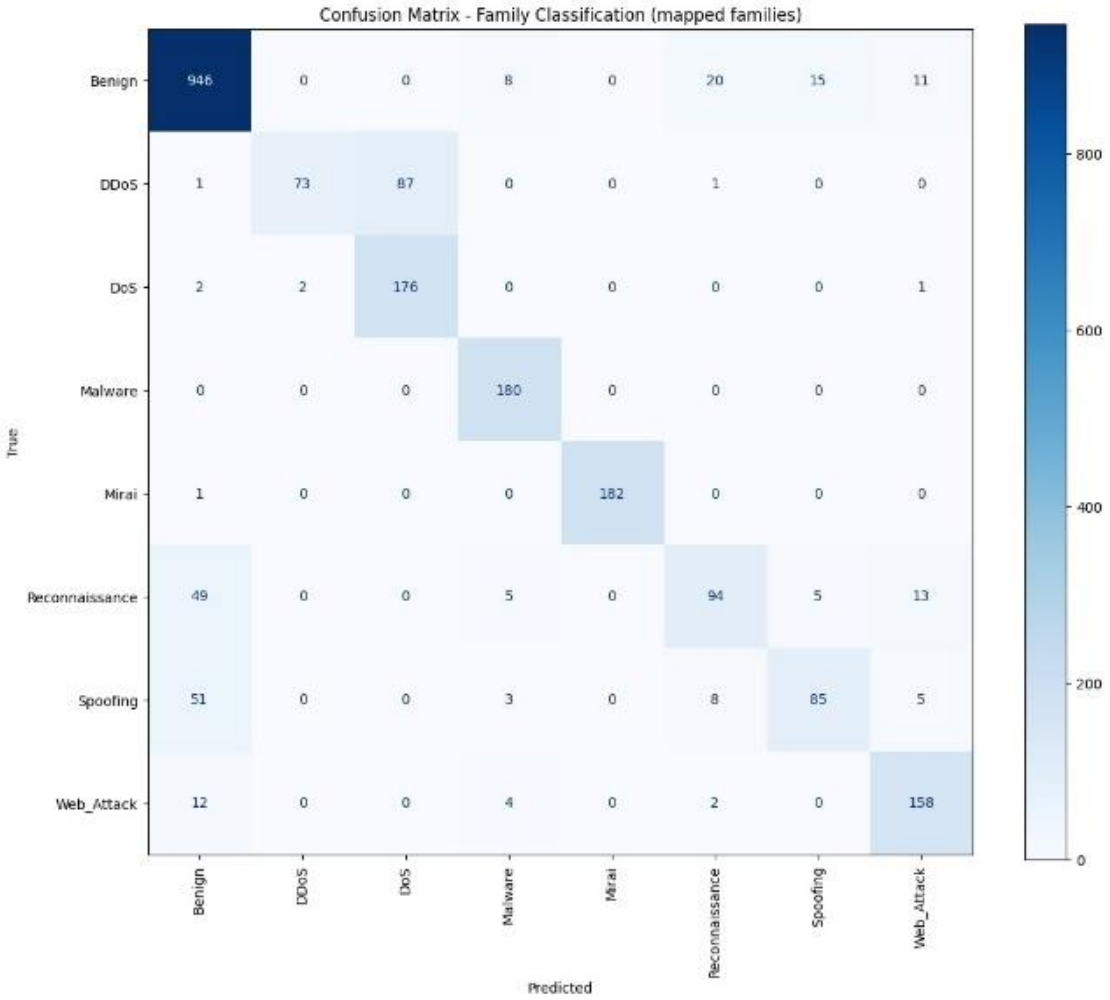

Fig. 5. Confusion matrix of family classification

A. Binary Classification Performance

As described in the methodology, the main goal of the binary detection unit is to place a secure perimeter by filtering the malicious traffic within the benign operational telemetry correctly[27]. A gatekeeper of high-fidelity is played by the hybrid model in this step. Originally, the classification report presents the statistics of the test partition which was composed of 2,200 observations that were divided into 1,000 benign flow and 1,200 malicious. Based on the findings of the experiment, it is possible to conclude that the proposed hybrid architecture can obtain a high alarm accuracy with a binary accuracy of 91.86. This is understandable since so long as the Transformer-CNN architecture is trained in a way that the acquired feature interactions win over the natural noise of networks and modelling errors of heterogeneous IoT devices the false alarms could be prevented. However, our approach has been effective in the sense that the Binary Matthews Correlation Coefficient (MCC) was found to be 0.8365, indicating that there was strong correlation between the predicted state of the intrusion and the actual state of the network. The measures of the binary test are given below to demonstrate the way the given framework detects anomalies. In the Class 0 (Benign), the model had a precision of 0.9005

and recall of 0.9230. Class 1 (Malicious) precision was obtained to be 0.9345 and F1-score was 0.9246. This means that the structural dependencies of an attack are accurately determined by the global awareness of the Transformer even with individual packet flags that may seem harmless to other conventional detectors.

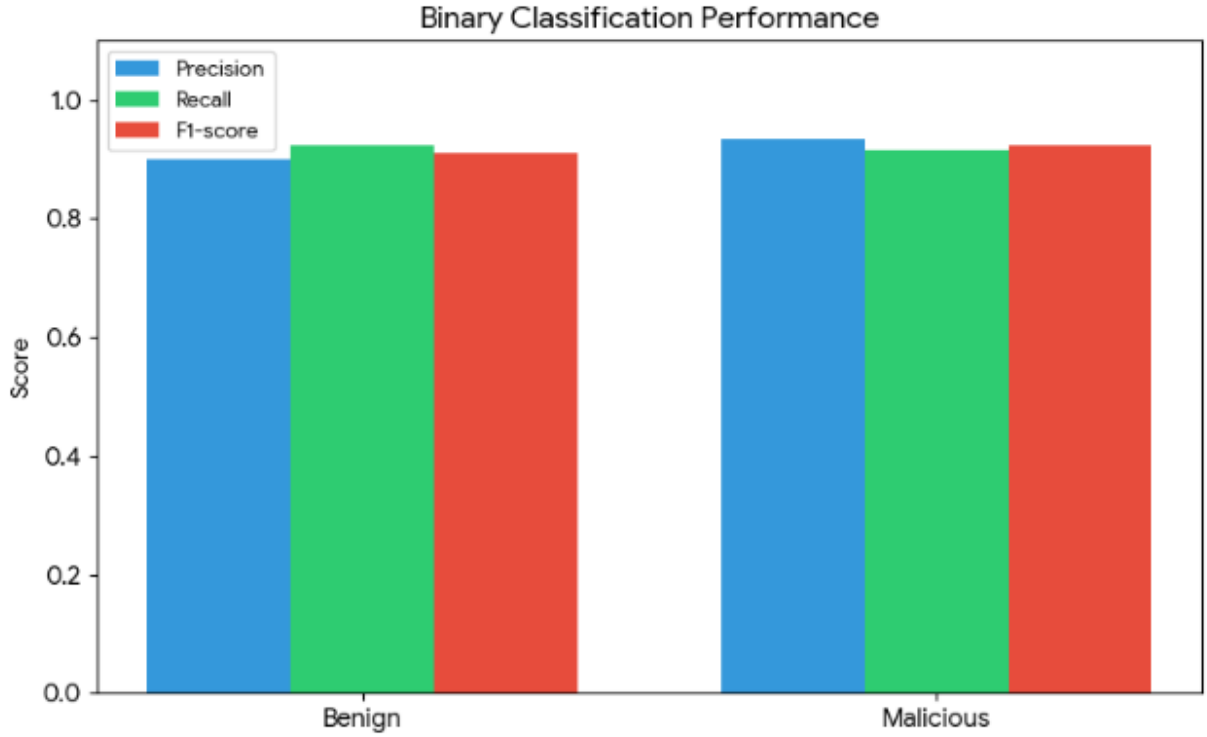

Fig. 6. Performance evaluation of binary classification

B. Family Classification Performance

In the contemporary IoT settings, the targeted mitigation strategies, including isolating a device infected with Mirai, are activated with the help of identification of the threat family, whilst simply filtering the volumetric DoS traffic. The attack family can be retrieved by comparing the statistics of the online traffic flow with the embedded deep features obtained while training. Given the principle of operation, granular classification is susceptible to the problem of class imbalance, where large families such as DDoS take up the learning mechanism. Here, the multi-class task in the paper was created to classify the threats into seven major families, with SMOTE being selected as a way of enhancing the representation of the minor classes. The report below shows the statistics of the multi-class test, according to which it is possible to determine that both the high volume and the stealthy attack families can be identified with a considerable accuracy. The total accuracy was 86.09 and Family MCC was 0.8146, which shows that the quality of multi-class separation is good. This can be readily explained as the abrupt changes in the volumetric data detected by CNN and subtle behavioural changes detected by Transformers were identified by the hybrid model.

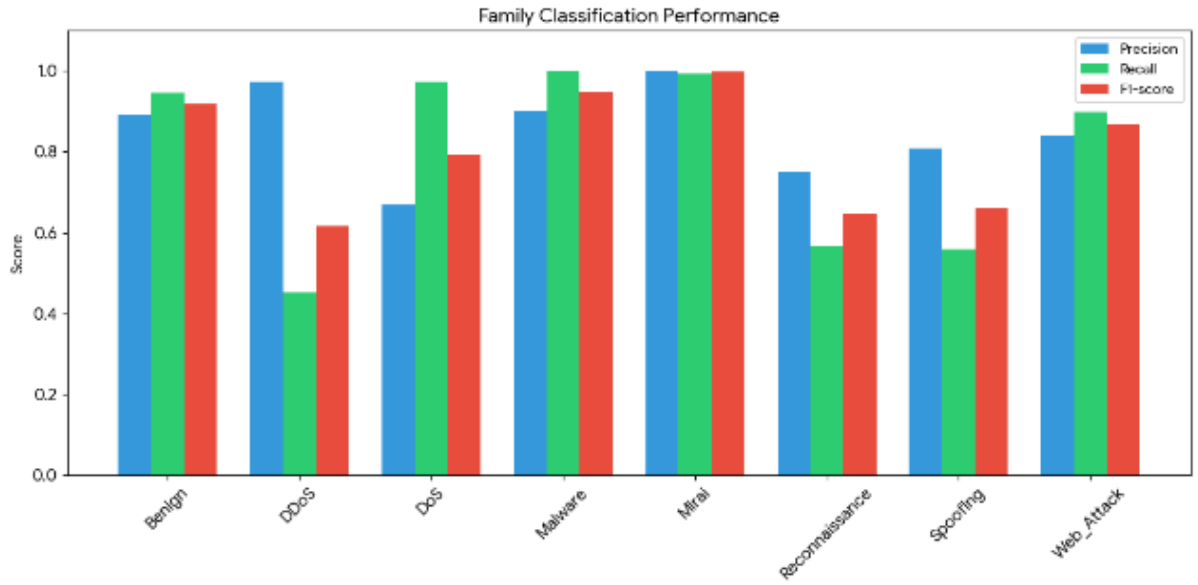

Fig. 7. Performance evaluation of family classification

VII. DISCUSSION

The concept of the synergy between the convolutional and attention-based modules of the proposed framework is a direct response to the modelling complexities of the current IoT traffic[29]. The importance of the 1D-CNN part (i.e., a high precision of 1.0000) and the unity of the Transformer part (i.e., the perfect recall of 1.0000) of Mirai and general Malware, respectively, testify to the fact that the 1D-CNN component is an effective tokenizer, whereas the Transformer mechanism is the effective reasoner about the global state of the flow. Nevertheless, the difference between DDoS accuracy (0.9733) and recall (0.4506) indicate that statistical overlaps of flow-level metadata is a problem facing the existing hybrid configurations. This recall constraint implies that a lot of DDoS traffic has volumetric similarities to the legitimate bursts or a typical DoS traffic and therefore the model used is too selective. Regardless of such difficulties, the integration of SMOTE in the preprocessing pipeline is confirmed by the consistent performance of such minority classes as Web Attack (F1-score: 0.8681). This granular classification ability gives the actionable intelligence to support automated security orchestration instead of mere binary alerts to targeted incident response[28].

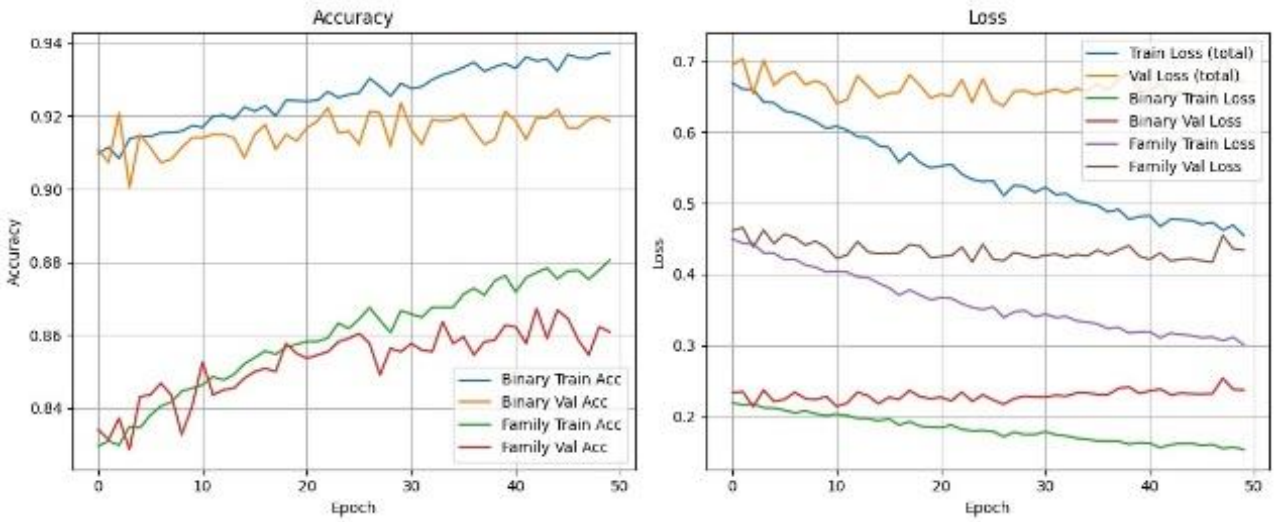

Fig. 8. Shows accuracy and loss evaluation of model

VIII. CONCLUSION

The proposed study was effective in the sense that a hybrid Transformer-CNN IDS was implemented and a binary accuracy of 91.86 was obtained and a family classification accuracy of 86.09 was achieved. The architecture has greatly enhanced detection of certain families such as Mirai botnets and generic Malware to deliver the actionable intelligence needed to achieve modern resilience in the IoT. The framework reduces operational disruptions due to false positives by having high accuracy in filtering benign traffic with a recall of 94.60% in the multi-class environment[30]. The future research will examine pruning of models and lightweight Transformers to simplify the structure to enable direct deployment of the model on the edge device.

REFERENCES

E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, Oct. 2019, doi: https://doi.org/10.1109/jiot.2019.2926365.

J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An Intrusion Detection Framework for Energy Constrained IoT Devices," *Mechanical Systems and Signal Processing*, p. 106436, Nov. 2019, doi: https://doi.org/10.1016/j.ymssp.2019.106436.

M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: an Intelligent Anomaly Based Intrusion Detection System for IoT Edge Devices," *IEEE Internet of Things Journal*, pp. 1–1, 2020, doi: https://doi.org/10.1109/jiot.2020.2970501.

N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, doi: https://doi.org/10.1109/comst.2019.2896380.

B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A Survey of Intrusion Detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, Apr. 2017, doi: https://doi.org/10.1016/j.jnca.2017.02.009.

Athira Remesh, D. Muralidharan, N. Raj, J Gopika, and Binu P.K, "Intrusion Detection System for IoT Devices," *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Jul. 2020, doi: https://doi.org/10.1109/icesc48915.2020.9155999.

Athira Remesh, D. Muralidharan, N. Raj, J Gopika, and Binu P.K, "Intrusion Detection System for IoT Devices," *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Jul. 2020, doi: https://doi.org/10.1109/icesc48915.2020.9155999.

Ogobuchi Daniel Okey, D. Carrillo, M. Saadi, Renata Lopes Rosa, João Henrique Kleinschmidt, and Demostenes Zegarra Rodriguez, "Transfer Learning Approach to IDS on Cloud IoT Devices Using Optimized CNN," *IEEE Access*, vol. 11, pp. 1023–1038, Jan. 2023, doi: https://doi.org/10.1109/access.2022.3233775.

A. Zohourian, S. Dadkhah, H. Molyneaux, E. C. P. Neto, and A. A. Ghorbani, "IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks," *Computers & Security*, vol. 146, p. 104034, Aug. 2024, doi: https://doi.org/10.1016/j.cose.2024.104034.

Z. Cao, Z. Zhao, W. Shang, S. Ai, and S. Shen, "Using the ToN-IoT dataset to develop a new intrusion detection system for industrial IoT devices," *Multimedia Tools and Applications*, Jun. 2024, doi: https://doi.org/10.1007/s11042-024-19695-7.

A. Mudgerikar, P. Sharma, and E. Bertino, "Edge-Based Intrusion Detection for IoT Devices," ACM *Transactions on Management Information Systems*, vol. 11, no. 4, pp. 1–21, Dec. 2020, doi: https://doi.org/10.1145/3382159.

A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," *Sensors*, vol. 22, no. 21, p. 8417, Nov. 2022, doi: https://doi.org/10.3390/s22218417.

A. Kaushik and H. S. Al-Raweshidy, "A Novel Intrusion Detection System for Internet of Things Devices and Data," *Wireless Networks*, Aug. 2023, doi: https://doi.org/10.1007/s11276-023-03435-0.

Arnaud Rosay, E. Cheval, Mustapha Ghanmi, F. Carlier, and P. Leroux, "Study of Network IDS in IoT devices," vol. 4, no. 4, May 2023, doi: https://doi.org/10.1007/s42979-023-01849-3.

M. Bhavsar, K. Roy, J. Kelly, and Odeyomi Olusola, "Anomaly-based intrusion detection system for IoT application," *Discover Internet of Things*, vol. 3, no. 1, May 2023, doi: https://doi.org/10.1007/s43926-023-00034-5.

A. Alhowaide, I. Alsmadi, and J. Tang, "Ensemble Detection Model for IoT IDS," *Internet of Things*, p. 100435, Jul. 2021, doi: https://doi.org/10.1016/j.iot.2021.100435.

Esra Altulaihan, Mohammed Amin Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors*, vol. 24, no. 2, pp. 713–713, Jan. 2024, doi: https://doi.org/10.3390/s24020713.

V. Kumar, A. K. Das, and D. Sinha, "UIDS: a Unified Intrusion Detection System for IoT Environment," *Evolutionary Intelligence*, Sep. 2019, doi: https://doi.org/10.1007/s12065-019-00291-w.

Y. Otoum and A. Nayak, "AS-IDS: Anomaly and Signature Based IDS for the Internet of Things," *Journal of Network and Systems Management*, vol. 29, no. 3, Mar. 2021, doi: https://doi.org/10.1007/s10922-021-09589-6.

N. Islam *et al.*, "Towards Machine Learning Based Intrusion Detection in IoT Networks," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1801–1821, 2021, doi: https://doi.org/10.32604/cmc.2021.018466.

M. Luqman *et al.*, "Intelligent parameter-based in-network IDS for IoT Using UNSW-NB15 and BoT-IoT Datasets," *Journal of the Franklin Institute*, vol. 362, no. 1, p. 107440, Dec. 2024, doi: https://doi.org/10.1016/j.jfranklin.2024.107440.

K.-H. Le, M.-H. Nguyen, T.-D. Tran, and N.-D. Tran, "IMIDS: an Intelligent Intrusion Detection System against Cyber Threats in IoT," *Electronics*, vol. 11, no. 4, p. 524, Feb. 2022, doi: https://doi.org/10.3390/electronics11040524.

Rehab Alsulami, Batoul Alqarni, Rawan Alshomrani, F. Mashat, and Tahani Gazdar, "IoT Protocol-Enabled IDS Based on Machine Learning," *Engineering Technology & Applied Science Research*, vol. 13, no. 6, pp. 12373–12380, Dec. 2023, doi: https://doi.org/10.48084/etasr.6421.

A. Awajan, "A Novel Deep Learning-Based Intrusion Detection System for IoT Networks," *Computers*, vol. 12, no. 2, p. 34, Feb. 2023, doi: https://doi.org/10.3390/computers12020034.

F. Alsakran, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study," *Communications in Computer and Information Science*, pp. 87–98, 2020, doi: https://doi.org/10.1007/978-981-15-4825-3_7.

M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion Detection Systems for IoT-based Smart environments: a Survey," *Journal of Cloud Computing*, vol. 7, no. 1, Dec. 2018, doi: https://doi.org/10.1186/s13677-018-0123-6.

T. Li, Z. Hong, and L. Yu, "Machine Learning-based Intrusion Detection for IoT Devices in Smart Home," *2020 IEEE 16th International Conference on Control & Automation (ICCA)*, Oct. 2020, doi: https://doi.org/10.1109/icca51439.2020.9264406.

R. Alasmari and Areej Abdullah Alhogail, "Protecting Smart-Home IoT Devices from MQTT Attacks: an Empirical Study of ML-Based IDS," *IEEE Access*, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3367113.

Sunday Adeola Ajagbe, Joseph Bamidele Awotunde, and Héctor Flórez, "Ensuring Intrusion Detection for IoT Services through an Improved CNN," *SN Computer Science*, vol. 5, no. 1, Dec. 2023, doi: https://doi.org/10.1007/s42979-023-02448-y.

Stefanos Papafotikas and Athanasios Kakarountas, "A Machine-Learning Clustering Approach for Intrusion Detection to IoT Devices," *University of Thessaly Institutional Repository (University of Thessaly)*, pp. 1–6, Sep. 2019, doi: https://doi.org/10.1109/seeda-cecnsm.2019.8908520.