AI-Driven Multi-Attack Detection in Network Traffic Using Tabular and Image-Converted Data

Abstract—**The exponential growth of cyber threats, including Distributed Denial of Service (DDoS), BotNets, intrusion, and Zero-day attacks, demands advanced intrusion detection systems (IDS) capable of real-time and accurate threat classification. To attain this objective, this research proposes an AI-based framework. Firstly, raw tabular data from the NSL-KDD dataset have been encoded, mapped and normalized. Secondly, both raw tabular data and image-converted network traffic have been integrated into representations for multi-attack detection. And finally, multiple machine learning and deep learning architectures, including Random Forest, XGBoost, 1D CNN, Vision Transformer (ViT), Convolutional Autoencoder (CAE), EfficientNetV2, and Palo Alto Standard Threat Detection, are evaluated to predict DDoS, BotNet, Zero-day attacks and Normal Network traffic. Experimental results demonstrate that ensemble tree-based methods achieve superior performance on raw tabular data, with XGBoost achieving an F1-score above 99.9% for most classes. Conversely, CNN-based models excel on image-converted data, with up to 97.72% F1-score for BotNet detection. Zero-day attack detection using Isolation Forest and CNN models yields balanced precision-recall performance, achieving up to 94.28% recall. Comparative analysis shows that image-converted representations consistently improve detection accuracy, particularly for complex attack classes such as BotNet. The results highlight the potential of hybrid data representation and AI-driven modeling for robust and scalable network security solutions.**

Index Terms—**Network intrusion detection, Distributed Denial of Service (DDoS), Botnet detection, Zero-day attack, Machine learning, Deep learning, Convolutional Neural Network (CNN), Vision Transformer (ViT), NSL-KDD dataset, Image-based intrusion detection.**

I. Introduction

Cybersecurity focuses on protecting networks, devices, and data from evolving threats such as botnets, Distributed Denial of Service (DDoS) attacks, intrusions, and zero-day exploits. These threats compromise confidentiality, integrity, and availability, posing severe challenges to organizational security. The increasing complexity and frequency of attacks demand advanced approaches to intrusion detection.

Earlier research primarily addressed DoS/DDoS detection using artificial intelligence methods. For instance, Yungaicela-Naula [1] proposed a modular SDN-based architecture for attack detection. However, recent trends show that zero-day exploits and botnets are becoming equally significant, often bypassing traditional IDS solutions. Hence, there is a growing need for AI-driven frameworks capable of analyzing network traffic and accurately identifying diverse attack types.

Therefore, the objective of this research is to utilize an AI-based framework. It is capable of real-time and accurate threat classification and intrusion detection. To achieve this, at first, raw tabular data from the NSL-KDD dataset have been encoded, mapped and normalized. Secondly, both raw tabular data and image-converted network traffic have been integrated into representations for multi-attack detection. And finally, multiple machine learning and deep learning architectures are evaluated to predict DDoS, BotNet, Zero-day attacks and Normal Network traffic. The key contributions of this research are as follows:

- Proposition of a unified AI-driven intrusion detection framework that integrates both raw tabular and image-converted data representations. Unlike prior studies that rely exclusively on one representation, our approach demonstrates the complementary benefits of combining both formats.
- Conduction of a comprehensive benchmarking of classical machine learning, deep learning, and commercial systems. This provides a broad evaluation rarely seen in prior IDS research.
- Addressing the challenge of zero-day attack detection. The experiments demonstrate balanced precision-recall performance for unseen attacks, highlighting the adaptability of our framework to novel threats.
- A practical insight into how data representation influences detection accuracy. Specifically, CNN-based models benefit significantly from image-converted data, while ensemble tree models achieve superior performance on tabular data.

These findings contribute to design guidelines for future IDS solutions. Overall, this research bridges the gap between academic IDS models and real-world systems by providing both methodological contributions and actionable insights for robust, scalable, and adaptive network security.

II. Related Works

Numerous studies have investigated network intrusion detection using machine learning and deep learning methods. N. M. Yungaicela-Naula et al. [1] conducted a study focusing on building a modular SDN architecture using machines and deep learning models to detect DDoS attacks on transport and application layers. However, this proposed system has some limitations as it was performed on a simulated environment rather than a real environment, and no discussion of latency, real traffic controller load.

Moreover, studies by authors S. Dong and M. Sarem [2] have enhanced the KNN-based algorithm to identify DDoS attacks in SDN systems to detect DDoS severity level in SDN. In this study, they used K-NN in the ACM Digital Library, IEEE Xplore, MDPI, and SAGE Journals datasets.

However, this study needs to improve performance in the real SDN environment. Recently, research has been conducted focusing on botnet attack detection in the network. A. Guerra-Manzanares et al. [3] propose a study to demonstrate the detection of botnets in network traffic using XGboost and Random Forest. To detect botnets and malicious activities, they are used multiple models like RF, XGBoost, CNN, and RNN classifiers in UNSW-NB15 and Bot-IoT datasets. Like other studies, they also have some limitations, where they need to use more classifiers and datasets for validation tests. Despite the demonstration, they didn't focus on peer review results and evaluation details. Likewise, Mustafa et al. [4] published a paper that also focuses on botnet attack detection using a deep autoencoder in IOT networks to identify anomalies. They use the N-BaloT dataset using an autoencoder to detect anomalies in IoT traffic, but their project has some limitations where they get considerably lower detection rates in IoT devices. In this paper, an autoencoder processed vectorized input image is used for a better representation of features.

Moreover, studies focusing on botnets were M. Ali et al. [5] combined KNN and Decision trees to a hybrid model to detect botnet attacks in IOT environments. They use the UNSW-NB15 dataset to build a stacking model ACLR for botnet attack identification. However, this research has some drawbacks as it doesn't validate for real environment and increases computational complexity with higher training time. Amarudin et al. [6] et al. proposed a study by improving the accuracy of machine learning classifiers on IDS using different models, but the results show inconsistency to measure accuracy in overcoming challenges. In this study, they used 49 public datasets and 13 private datasets with multiple models like (k-NN, RF, NB, DT, NN, and SVM) for botnet detection. Despite using many models there are some inconsistency exits for measuring accuracy for overcoming challenges.

For the detection of Intrusion detection in networks, several studies have been conducted, as mentioned below. Mohab et al. [7] proposed a comparative study of classical machine learning and deep learning approaches to detect anomaly-based intrusion detection. In this study, they focus on the strengths of ML and DL in anomaly detection by comparison with the KDD-99 dataset. However, in less common attack types, they achieve a low accuracy score. Consequently, other studies have been conducted focusing on the integration of CNN and BiLSTM with hybrid feature selection to design an IDS system on SDN proposed by authors R. Ben Said et al. [8]. They use two datasets, NSL-KDD and CIC IDS2017, where tabular data is converted likely shape as an image for CNN model processing, focusing on enhancing IDS using binary and multiclass classification. However, these studies are only performed on simulated environments, not in real environments, and they need to explore the potential of transfer learning techniques for better results. Sumaiya et al. [9] provide a paper based on the intrusion detection system using machine learning models like Naive Bayes, Decision Trees, SVM, etc. Since the paper shows the different Machine learning model classifiers in the KDD 99 / NSL KDD datasets for comparing their performances. In this study, there are no deep learning models used.

To detect Zero-day attacks in systems, there are several studies have been conducted, which are mentioned below. Authors I. Mbona et al. [10] proposed a study focused on Semi-Supervised Learning for Zero-Day Intrusion Detection. In this study, they used CICDDoS2019, IOTIntrusion2020, and CIRA-CIC-DoHBrw-2020 datasets for Zero-day attack detection. But they need to combine multiple feature selection methods and ML classifiers. However, the limitations on this study are a lack of details on model architecture and generalizability. Similarly, author Sumaiya et al. [11] proposed research that is based on zero-day attack detection by identifying malicious behavior on encrypted traffic flows. In this study they used SimCSE models using vectorized embedding of the traffic that can be visualized in an image for classification. AI-Based Review on Zero-Day Attack Detection research written by authors Mbona et. al. [12], where they review current AI-based methods used for zero-day threat detection and summarize their limitations and gaps. They use different datasets like ACM Digital Library, IEEE Xplore, MDPI, SAGE Journals, Semantic Scholar, Science Direct, Scopus, using an SLR focused on exploring zero-day attacks. However, in this research no experimental validation or datasets are used, and significant limitations remain in mitigating zero-day attacks.

There are several research courses conducted on converting raw tabular datasets into image data and applying different machine learning and deep learning methods. Likewise, as described in the papers [4], [8], and [11] the same procedure has been applied in paper kim et al. [13] use image-based data. They convert PCA, t-SNE, UMAP, and kernel PCA (kPCA) to image data using the NSL-KDD dataset to be using deep CNN model for classification in an intrusion detection system. This project focused on converting tabular data into images to improve detection accuracy in an intrusion detection system. However, this paper has some drawbacks to handling high-capacity network traffic. In another study, Siddiqi et al. [14] proposed a new intrusion detection system for higher classification precision in a CNN model using image processing techniques. They convert the raw tabular data into grayscale images in the CICIDS2017, NSL-KDD, and ISCX2012 datasets. Additionally, they apply Gabor filtering for enhancing texture and features before CNN classification.

Finally, Choi et al. [15] implemented a malicious network traffic detection framework based on a Convolutional Neural Network with feature engineering techniques in the NSL-KDD dataset. In this paper, they have shortcomings, where the framework has not been validated on real life traffic, with image conversion steps incur additional computational overhead.

Overall, it can be said that several studies have attempted to detect single-attack using machine learning and deep learning models. Most existing research targets single-attack detection, relies on simulated datasets, or lacks generalization across multiple attack types. Our work addresses this gap by proposing a unified AI-driven framework using both raw and image-converted NSL-KDD data for multi-attack detection."

III. Methodology

A. Dataset Description

The NSL-KDD [16] dataset is a refined and improved version of the classic KDD Cup 1999 intrusion detection dataset. It's structured to address the shortcomings of the original dataset and serve as a more reliable benchmark for network intrusion detection research.

Specifically, NSL-KDD removes redundant records from the training set, helping to avoid classifier bias toward frequently occurring samples and eliminates duplicate entries from the test set to ensure fairer evaluation of detection methods. The data set carefully balances the representation of the difficulty levels of the samples. The number of records per difficulty group is chosen inversely to their frequency in KDD-99. This design enables a broader range of classification results and a more robust comparison of machine learning models.

The dataset is sized in such a way that it can be used for experiments even on limited hardware, promoting consistent and comparable research outcomes. It typically includes multiple variants such as KDDTrain+, KDDTest+, and subsets like KDDTrain+_20Percent or KDDTest-21, which exclude the most challenging records (with difficulty score = 21), facilitating flexible experimentation and staged evaluation.

Each connection record in NSL-KDD includes 41 core features along with additional label attributes like attack type and difficulty score, for a total of 43 fields per record. Attack categories include Denial of Service (DoS), Probe (network surveillance), User-to-Root (U2R) and Remote-to-Local (R2L). They together mirror the taxonomy of KDD-99.

B. Data Preprocessing

The KDDTrain+ and KDDTest+ subsets were used, with missing headers. Headers mapped from the ARFF attribute list. Then the two datasets were merged into a single consolidated dataset. Categorical features (protocol type, service, flag) were encoded numerically, and all features were normalized using Min-Max scaling. Attack labels were grouped into four categories: DoS, Probe, R2L, and U2R. These were further consolidated into three primary classes: Normal (0), DDoS (1), and BotNet (2).

An additional column, attack_class, was introduced to represent grouped attack classes, where DoS attacks were labeled as DDoS-attack and encoded as '1', while Normal traffic was denoted by '0'. Botnet operations typically unfold in multiple stages: scanning, infection, control, and attack. For instance, the Mirai [17] malware exemplifies this lifecycle by first scanning networks to identify vulnerable IoT devices with open Telnet ports. During the infection phase, Mirai exploits weak default credentials to compromise these devices. In the control phase, the infected devices (bots) connect to a Command and Control (C&C) server to receive instructions [18]. Finally, in the attack phase, these bots carry out coordinated attacks such as Distributed Denial of Service (DDoS). In this context, attack types related to reconnaissance (Probe), unauthorized access attempts (R2L), and privilege escalation (U2R) can be viewed as integral phases or components of botnet activities [19]. Therefore, in the proposed classification, these three attack categories are collectively labeled as BotNet and encoded as '2' in the attack_class column.

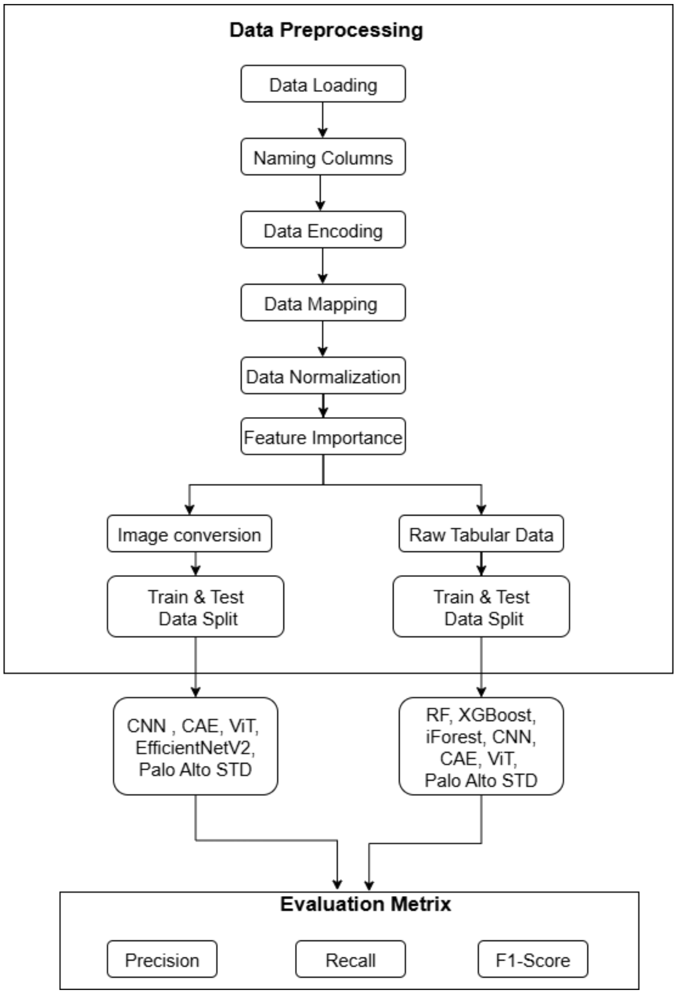

Fig. 1. Data preprocessing with model training-testing and feature importance.

Finally, the tabular records were also transformed into 6×7 images to enable CNN-based processing, later resized to 48×48 for EfficientNetV2 compatibility. Fig. 1 shows the data preprocessing steps.

C. Feature Selection

All 42 available features from the dataset were retained for model training. Given the feature dimension, each record was reshaped into a 6×7 image representation. However, the EfficientNetV2 architecture does not natively support 6×7 input images. Therefore, each 6×7 image was resized to 48×48 using the preprocess_for_effnet() function. EfficientNetV2 is designed for RGB images with three channels. This preprocessing step also ensures compatibility by converting grayscale inputs into a three-channel format. Fig. 2 shows converted image data for CNN, CAE, ViT and Palo Alto STD. Fig. 3 converted image data of EfficientNetV2.

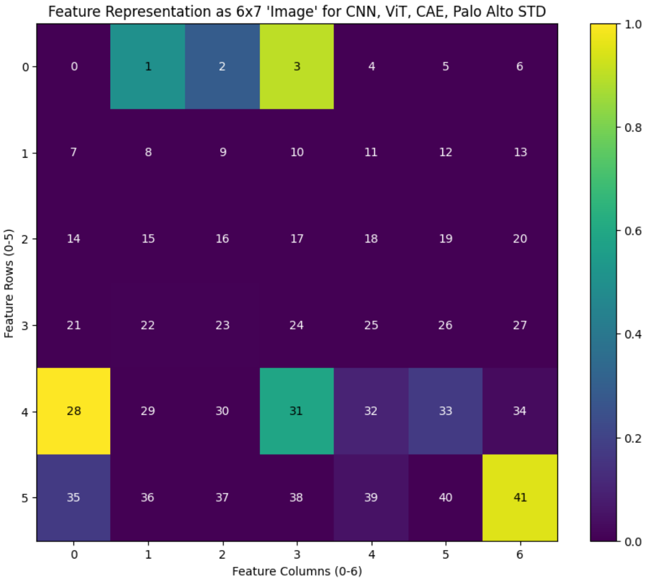

Fig. 2. A sample of converted image data for CNN, CAE, ViT and Palo Alto STD.

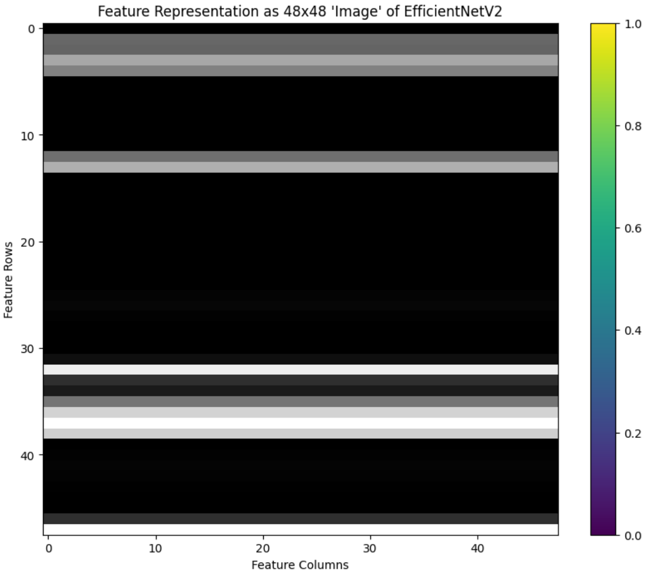

Fig. 3. A sample of converted image data for EfficientNetV2

D. Model Training and Evaluation

AI-driven models such as combinations of Random Forest and Isolation Forest, XGboost and Isolation Forest, CNN/1D CNN and CAE, ViT and CAE are trained on the NSL-KDD dataset in order to predict Normal, DDoS, Zero-Day attack and BotNets. In addition, single-model approaches such as EfficientNetV2 and Palo Alto Standard Threat Detection (STD) were also evaluated. For detecting Zero-Day attacks, normal network traffic has been trained on CAE and Isolation Forest. Then, it is tested on the dataset to classify normal network traffic and Zero-day attacks. Fig. 4 shows the ROC curve of Zero-day attack detection for the Isolation forest.

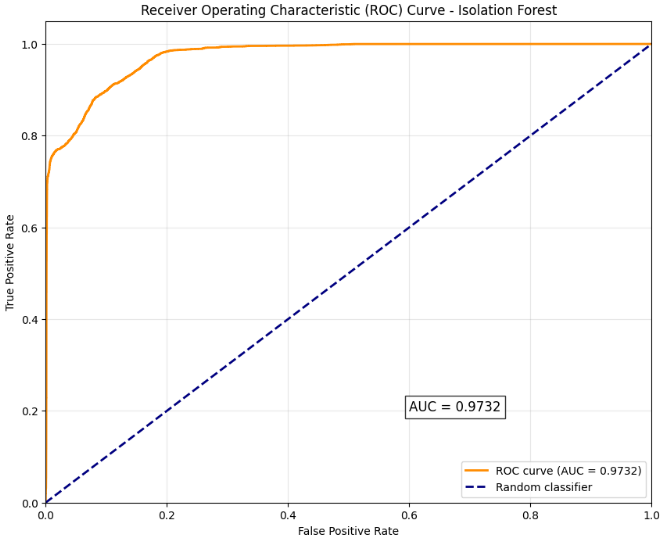

Fig. 4. ROC curve of Zero-day attack detection for the Isolation forest

Precision, Recall and F1-Score were used to evaluate the performance of the models.

Precision: Precision measures whether the positive predictions are correct. It is calculated as the ratio of true positives (TP) to all predicted positives (TP + FP).

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

Recall: Recall quantifies the ability to detect all actual positives. It is the ratio of TP to all actual positives (TP + FN).

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

F1-Score: The F1-Score harmonizes precision and recall via their harmonic mean, penalizing extreme imbalances.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{3}$$

80% data from the dataset was used for training purposes and the rest 20% was used for conducting test.

IV. Results and Discussion

A. Model Evaluation

The performance of the proposed and baseline models was evaluated using *Precision*, *Recall*, and *F1-score* for multi-class classification tasks involving Normal, DDoS, and BotNet traffic. Tables I–III summarize the results for tabular data, image-converted data, and zero-day attack detection, respectively. A comparative evaluation between tabular and image-converted data reveals consistent gains for deep learning models when using image representations.

TABLE I
Performance comparison of models for Raw Tabular Data (Normal, DDoS and BotNet detection)

Model	Class	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	Normal	99.92	99.94	99.93
	DDoS	99.95	99.94	99.95
	BotNet	99.75	99.69	99.72
XGBoost	Normal	99.94	99.91	99.93
	DDoS	99.95	99.97	99.96
	BotNet	99.69	99.78	99.73
1D CNN	Normal	98.79	99.27	99.03
	DDoS	99.79	99.81	99.80
	BotNet	97.19	95.09	96.13
Vision Transformer	Normal	96.74	98.09	97.41
	DDoS	99.63	97.83	98.72
	BotNet	90.52	89.94	90.23
Palo Alto STD	Normal	74.70	97.22	84.49
	DDoS	96.47	84.73	90.22
	BotNet	83.61	41.62	55.57

TABLE II
Performance comparison of models for Converted Image Data (Normal, DDoS and BotNet detection)

Model	Class	Precision (%)	Recall (%)	F1-Score (%)
EfficientNetV2	Normal	98.31	88.46	93.12
	DDoS	82.44	78.58	80.46
	BotNet	59.30	92.81	72.37
CNN	Normal	99.91	99.17	99.54
	DDoS	99.87	99.61	99.74
	BotNet	95.88	99.64	97.72
Vision Transformer	Normal	99.49	97.64	98.56
	DDoS	99.81	99.77	99.79
	BotNet	90.93	98.31	94.48
Palo Alto STD	Normal	68.60	97.05	80.38
	DDoS	96.21	82.62	88.90
	BotNet	82.74	36.93	51.07

TABLE III
Performance comparison of models for Zero-Day Attack

Model	Class	Precision (%)	Recall (%)	F1-Score (%)
iForest (Tabular Data)	Normal Zero-Day	90.64 89.05	89.80 89.95	90.22 89.50
CAE (Tabular Data)	Normal Zero-Day	94.12 85.36	85.00 94.27	89.33 89.59
CAE (Image Converted Data)	Normal Zero-Day	94.12 85.36	85.00 94.28	89.33 89.59

1) Tabular Data Evaluation: As shown in Table I, tree-based ensemble methods achieved the highest performance. XGBoost achieved the best overall results. Its Precision, Recall, and F1-scores exceed 99.90% for both Normal and DDoS classes, and 99.73% for BotNet. Random Forest demonstrated comparable results, slightly outperforming XGBoost for the BotNet class in terms of Recall (99.69% vs. 99.78%). Deep learning models such as 1D CNN performed competitively for Normal and DDoS detection, but showed reduced performance for the BotNet class (F1-score of 96.13%). The Vision Transformer achieved lower scores for BotNet (F1-score of 90.23%) compared to ensemble models. The commercial Palo Alto STD system exhibited significantly lower performance, particularly for BotNet (F1-score of 55.57%).

2) Image-Converted Data Evaluation: Table II shows results for models trained on image-converted data. The CNN achieved the highest accuracy across all three classes. Its F1-scores are 99.54%, 99.74%, and 97.72% for the Normal, DDoS, and BotNet classes. The Vision Transformer performed well for Normal and DDoS detection (F1-scores above 98%) but lagged behind for BotNet (94.48%). EfficientNetV2 struggled with BotNet detection. Its Precision is only 59.30%, despite maintaining a high Recall (92.81%). The Palo Alto STD again showed limited effectiveness, particularly for BotNet traffic (F1-score of 51.07%).

3) Tabular vs. Image-Converted Data Evaluation: Both Table I and Table II have common ViT, CNN and Palo Alto STD models. It can be seen that for all 3 models, Image-Converted Data does better performance than Raw Tabular Data.

For the CNN model, image-converted data improved the BotNet class F1-score from 96.13% to 97.72%, while maintaining similarly high performance for Normal and DDoS classes. The ViT model also showed notable gains, with the BotNet F1-score increasing from 90.23% to 94.48%, and improvements for Normal and DDoS classes by approximately 1–2%. The Palo Alto STD system, despite overall lower performance compared to machine learning and deep learning models, it shows opposite development compared to others. In its case, all of its results for image converted data decreased compared to raw tabular data. For BotNet, F1-score decreases from 55.57% to 51.07%, for DDoS, F1-score decreases from 90.22% to 88.90% and Normal traffic detection from 84.49% to 80.38% in F1-score. Normal traffic detection F1-score decrease for Palo Alto STD indicates a possible trade-off in class-specific optimization.

Overall, the results confirm that image-based transformation enhances discriminative ability, particularly for complex attacks such as BotNet. But for the Palo Alto STD model, tabular data performs better than image-converted data.

4) Zero-Day Attack Evaluation: The zero-day attack detection results are reported in Table III. The iForest anomaly detection model achieved balanced Precision and Recall values, with F1-scores of 90.22% and 89.50% for Normal and Zero-Day classes, respectively. CNN-based models, both for tabular and image-converted data, demonstrated similar performance, with an F1-score of 89.59% for Zero-Day detection. While CNNs exhibited slightly higher Recall for Zero-Day traffic (94.27% and 94.28%) compared to iForest, they showed lower Precision for the Normal class.

Overall, the evaluation results indicate that tree-based ensembles dominate in tabular data classification, CNNs excel in image-based representations, and both iForest and CNNs provide comparable performance in zero-day attack detection scenarios. The commercial Palo Alto STD solution consistently underperformed compared to the machine learning and deep learning models.

B. Feature Importance

Random Forest Feature Importance Analysis is performed to identify features that have the most influence on classification. Higher importance means that the feature is more useful in predicting the target variable. 'difficulty_level' achieved the highest importance score during model training. 'num_root', 'root_shell', 'num_file_creations', 'num_access_files',

’num_shells’, ’land’, ’urgent’, ’su_attempted’, ’is_host_login’, ’num_outbound_cmds’ these column have the lowest importance score. Fig. 5 shows the top 10 important features among 42 features for threat detection.

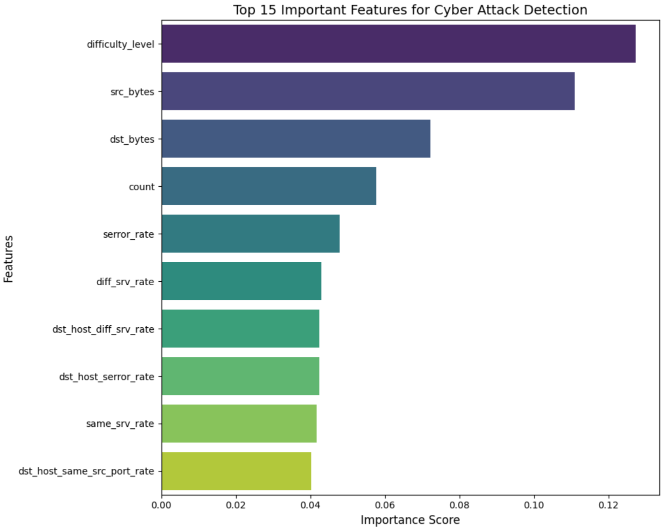

Fig. 5. Random Forest top 10 Important features for threat detection

V. Conclusion

This study presented an AI-based multi-attack detection framework capable of identifying DDoS, botnet, intrusion, and zero-day attacks by leveraging both raw tabular and image-converted network traffic data. Using the NSL-KDD dataset, the evaluation revealed that ensemble learning models such as XGBoost and Random Forest perform exceptionally well on tabular data, achieving over 99.9% accuracy for Normal and DDoS traffic. CNN-based models demonstrated superior performance on image-converted data, especially for BotNet detection, achieving an F1-score of 97.72%. Moreover, transforming tabular network traffic features into image representations significantly enhanced detection performance across multiple models, even benefiting commercial threat detection systems. For zero-day detection, Isolation Forest and CNN models provided competitive and balanced results. These findings underscore the effectiveness of combining different data representations and model architectures for comprehensive network intrusion detection.

Future research will focus on expanding this approach to larger and more diverse real-world datasets, including encrypted traffic and IoT-specific attack patterns. Transfer learning and federated learning techniques will be explored to improve generalization across different network environments while preserving data privacy. The integration of temporal traffic patterns, real-time streaming analytics, and multi-modal feature fusion could further enhance detection performance. Additionally, optimizing computational efficiency for deployment in high-throughput and resource-constrained environments remains an essential direction. The incorporation of explainable AI (XAI) methods will be pursued to improve interpretability and trust in IDS decision-making for cybersecurity professionals.

References

[1] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, “Sdn-based architecture for transport and application layer ddos attack detection by using machine and deep learning,” *IEEE Access*, vol. 9, pp. 108 495–108 512, 2021.

[2] S. Dong and M. Sarem, “Ddos attack detection method based on improved knn with the degree of ddos attack in software-defined networks,” *IEEE Access*, vol. 8, pp. 5039–5048, 2020.

[3] A. Guerra-Manzanares, H. Bahsi, and S. Nõmm, “Hybrid feature selection models for machine learning based botnet detection in iot networks,” in *2019 International Conference on Cyberworlds (CW)*, 2019, pp. 324–327.

[4] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, “Botnet attack detection using machine learning,” in *2020 14th International Conference on Innovations in Information Technology (IIT)*, 2020, pp. 203–208.

[5] M. M. F. A. U. A. D. G. V. M. M. K. H. A. I. Ali, Mudasir, “Botnet detection in internet of things using stacked ensemble learning model,” *Scientific Reports*, vol. 15, no. 1, pp. 2045–2322, 2025.

[6] Amarudin, R. Ferdiana, and Widyawan, “New approach of ensemble method to improve performance of ids using s-sdn classifier,” in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, 2022, pp. 463–468.

[7] M. S. Abdel-Wahab, A. M. Neil, and A. Atia, “A comparative study of machine learning and deep learning in network anomaly-based intrusion detection systems,” in *2020 15th International Conference on Computer Engineering and Systems (ICCES)*, 2020, pp. 1–6.

[8] R. Ben Said, Z. Sabir, and I. Askerzade, “Cnn-bilstm: A hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection,” *IEEE Access*, vol. 11, pp. 138 732–138 747, 2023.

[9] I. Sumaiya Thaseen, B. Poorva, and P. S. Ushasree, “Network intrusion detection using machine learning techniques,” in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, 2020, pp. 1–7.

[10] I. Mbona and J. H. P. Eloff, “Detecting zero-day intrusion attacks using semi-supervised machine learning approaches,” *IEEE Access*, vol. 10, pp. 69 822–69 838, 2022.

[11] R. Bar and C. Hajaj, “Simcse for encrypted traffic detection and zero-day attack detection,” *IEEE Access*, vol. 10, pp. 56 952–56 960, 2022.

[12] L. Yee Por, Z. Dai, S. Juan Leem, Y. Chen, J. Yang, F. Binbeshr, K. Yuen Phan, and C. Soon Ku, “A systematic literature review on ai-based methods and challenges in detecting zero-day attacks,” *IEEE Access*, vol. 12, pp. 144 150–144 163, 2024.

[13] T. Kim and W. Pak, “Deep learning-based network intrusion detection using multiple image transformers,” *Applied Sciences*, vol. 13, no. 5, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/5/2754

[14] W. P. Murtaza Ahmed Siddiqi, “An optimized and hybrid framework for image processing based network intrusion detection system,” *Computers, Materials & Continua*, vol. 73, no. 2, pp. 3921–3949, 2022. [Online]. Available: http://www.techscience.com/cmc/v73n2/48399

[15] D.-S. Choi, T. Kim, B. Kang, and E. G. Im, “Image-based malicious network traffic detection framework: Data-centric approach,” *Applied Sciences*, vol. 15, no. 12, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/12/6546

[16] M. H. Zaib. Nsl-kdd. [Accessed: Aug. 28, 2025]. [Online]. Available: https://www.kaggle.com/datasets/hassan06/nslkdd

[17] C. D. McDermott, F. Majdani, and A. V. Petrovski, “Botnet detection in the internet of things using deep learning approaches,” in *2018 International Joint Conference on Neural Networks (IJCNN)*, 2018, pp. 1–8.

[18] A. A. Korba, A. Diaf, and Y. Ghamri-Doudane, “Ai-driven fast and early detection of iot botnet threats: A comprehensive network traffic analysis approach,” in *2024 International Wireless Communications and Mobile Computing (IWCMC)*, 2024, pp. 1779–1784.

[19] B. Liu and Q. Zhang, “Gamma factors and converse theorems for classical groups over finite fields,” *Journal of Number Theory*, vol. 234, pp. 285–332, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022314X21002250