ResNet-Based Detection of SYN Flood DDoS Attacks

Hiba S. Bazzi, Ali H. Nassar, Imane M. Haidar, Ali M. Haidar and Ziad Doughan
Department of Electrical and Computer Engineering
Beirut Arab University
Dibbieh, Lebanon
(h.bazzi, a.nassar, i.haidar, ari, z.doughan)@bau.edu.lb

***Abstract*—This paper presents a novel approach to detect SYN flood Distributed Denial of Service (DDoS) attacks using the ResNet 50 architecture. DDoS attacks, known for their ability to disrupt normal network traffic through overwhelming floods, have evolved in complexity, rendering traditional detection methods inadequate. Our methodology is threefold: data acquisition from both simulated and real-world environments, data processing where network traffic data is converted into 2D images, and attack detection using a Convolutional Neural Network model. The model's performance was rigorously evaluated, demonstrating exceptional accuracy of 97.5%, which indicates the model's effectiveness in controlled environments. The ResNet-50 based model shows promising results in accurately classifying network traffic and identifying DDoS attacks. This not only validates the effectiveness of deep learning in cybersecurity but also opens avenues for more robust and adaptable network defense mechanisms.**

***Index Terms*—Convolution neural network, Machine learning, cybersecurity,network security,Artificial intellegence**

I. Introduction

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources, such as IoT devices. The influx of incoming messages, connection requests, and malformed packets can cause the victimized system to slow down or even crash and shut down, thereby denying service to legitimate users. Attacks are increasingly complex and sophisticated, often making them challenging to prevent with traditional security infrastructure. As the scale and impact of these attacks have grown over the years, they have become a significant concern for cybersecurity experts and organizations worldwide [1].

SYN Flood, a type of DDoS attack, exploits the TCP handshake mechanism, severely impacting TCP connections [2]. It involves bombarding a server with numerous SYN requests using spoofed IP addresses, causing resource depletion and denying service to legitimate users. These attacks are notably challenging to trace and have become more prevalent with the increase in Internet-connected devices. The evolution of DDoS attacks has led to more frequent and complex strategies, combining volumetric, protocol, and application layer tactics [3]. This escalation is reflected in the growing variety and scale of attacks, some reaching unprecedented traffic levels, making detection and mitigation increasingly difficult. Historical trends show a significant rise in both the frequency and complexity of these attacks, with predictions indicating a doubling of global DDoS attacks from 7.9 million in 2018 to 15.4 million by 2023, as shown in Fig. 1 [4].

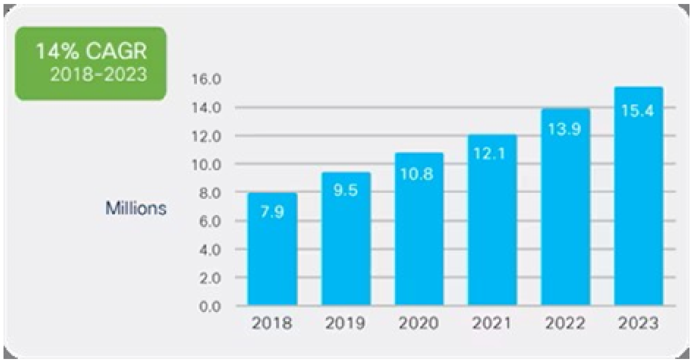

Fig. 1. Global Trends of DDos Attacks 2018-2023 [4]

As the complexity of network-based attacks continues to evolve, traditional methods of detection and mitigation are often found lacking. This has led to a growing interest in leveraging advanced machine learning techniques [5], particularly Convolutional Neural Network (CNN), in the domain of network security. CNN are renowned for their proficiency in handling image data, making them an excellent tool for pattern recognition and anomaly detection tasks [6].

Among the various architectures in deep learning, Residual Networks (ResNet) have emerged as a powerful tool. Introduced by He *et al.* [7], ResNet models have revolutionized the field with their unique 'skip connections,' allowing the training of much deeper networks by addressing the vanishing gradient problem common in traditional deep learning models. This capability makes ResNet particularly suitable for complex classification tasks, such as differentiating between normal and malicious network traffic.

In this study, we explore the innovative application of a ResNet model to detect SYN Flood DDoS attacks. We created our own DDoS attack traffic in a lab, then converted network traffic data into a 2D image format, utilizing ResNet's strengths in image recognition to address the challenges of DDoS attack detection. The subsequent sections detail our methodology, implementation, and the results achieved, showcasing the potential of deep learning in enhancing network security.

II. Related Works

In exploring the intersection of DDoS attacks and machine learning, many studies have contributed valuable insights. CNN models have achieved high significance due to their efficient performance in image processing and computer vision fields [8]. The CNN models have also been used in detecting network attacks. The authors in [9] use machine learning techniques to classify and detect DDoS attacks, such as Naive Bayes and Random Forest Tree. Lower accuracy has been shown in UDP classification [10], which is used to detect three types of DDoS attacks through a specific model.

CNN models have also been used for detecting network attacks. The authors in [11] proposed a CNN-based approach to detect malicious traffic from NetFlow data; they convert NetFlow data to images and then feed these images to a CNN model.

Deepak Kshirsagar and Sandeep Kumar [12] present an approach for recognizing application-level Denial of Service (DoS) threats based on ontology. The system uses an ontology model with semantic rule to identify HTTP flood attack. They use the GoldenEye DoS dataset with semantic rule, and the proposed system can identify a DoS attack with a 94.89

The authors of [13] used a deep learning model such as Long Short-Term Memory (LSTM) and CNN to detect and mitigate DDoS attacks. They directed flood attacks to a controller using TCP, ICMP, and UDP, achieving an accuracy of 89.63% with this model. In their research, Chen *et al.* [14] used CNN with CICIDS2017 [15] to evaluate the performance of their system, examining the proposed system using the featured data as input and the raw data as another input from the CICIDS2017 [15] dataset.

Liu *et al.* [16] use CNN to detect network intrusions. They proposed a methodology to convert network traffic into three-dimensional (3D) images by using the NSL-KDD dataset [17] and applying Fast Fourier Transformation (FFT), then passing these images to a CNN model for detection. The authors of [18] also used CNN to classify real network traffic as malicious, capturing live network packets with Wireshark, taking screenshots, and feeding these images to the CNN model for classification.

In their research, Boonchai *et al.* [19] proposed research in DDoS classification using machine learning. They used the dataset provided by CICDDoS2019 [20] to feed two proposed models, DNN and convolutional autoencoder. They concluded that their proposed CNN provides the best efficiency in multiclass classification.

The authors in [21] use a CNN model to detect HTTP flood attacks, employing the dataset provided by Kaggle [22] as network logs. After training their system with a CNN model, they achieved a 99% accuracy. Shaaban *et al.* [23] proposed an article to detect and classify DDoS attacks using CNN, comparing its accuracy with other machine learning techniques such as Decision Tree, SVM, and KNN. They found that CNN's accuracy is much higher than other techniques. On the other hand, Hussain *et al.* [24] proposed a study using ResNet in DoS and DDoS detection in the Internet of Things (IoT). They used ResNet 18 and the CICDDoS2019 dataset [20] to train and test their model, achieving an accuracy of 99%.

Building upon the insights from previous studies, our proposed work aims to enhance the accuracy, precision, F1 score, and recall beyond the achievements of existing methodologies in the field. We intend to achieve this enhancement by implementing our novel methodology, which leverages advanced machine learning techniques. This approach is designed not only to refine the detection of DDoS attacks but also to set a new benchmark in the effectiveness of network security solutions.

III. Proposed Methodology

Our proposed methodology is structured into three primary steps: data acquisition, data processing, and attack detection. Initially, network traffic data is acquired. The processing stage then involves two crucial sub-steps: data filtering and conversion of this data into two-dimensional (2D) images. The final stage focuses on attack detection, where the processed data is used to train and evaluate various Convolutional Neural Network (CNN) models, specifically for the detection of SYN flood DDoS attacks. Fig. 2 provides a detailed depiction of our methodology, with each step further elaborated in the subsequent subsections.

A. Data Acquisition

Data acquisition is the first step in our proposed methodology. Initially, we need to acquire both attack and normal traffic. To achieve this, we have constructed our own lab, as shown in Fig. 3. Our lab comprises a web server running on an Ubuntu operating system, connected to a network switch. This setup includes an attacker machine with a Kali operating system to generate DDoS attacks against our web server, and a third computer, a Windows 10 machine equipped with Wireshark, used for sniffing the data entering and leaving the web server. All these devices are configured on the same network.

Utilizing this setup, we launched a SYN DDoS attack from the attacker machine to the web server and captured these packets using Wireshark, saving them into a pcap file. Subsequently, we generated normal traffic using our web server and captured these packets through the capture machine with Wireshark, storing them in another pcap file.

In addition to our own data, we employed the CICDDoS2019 dataset [20] to test the results of our trained system, comparing its performance against the data we generated.

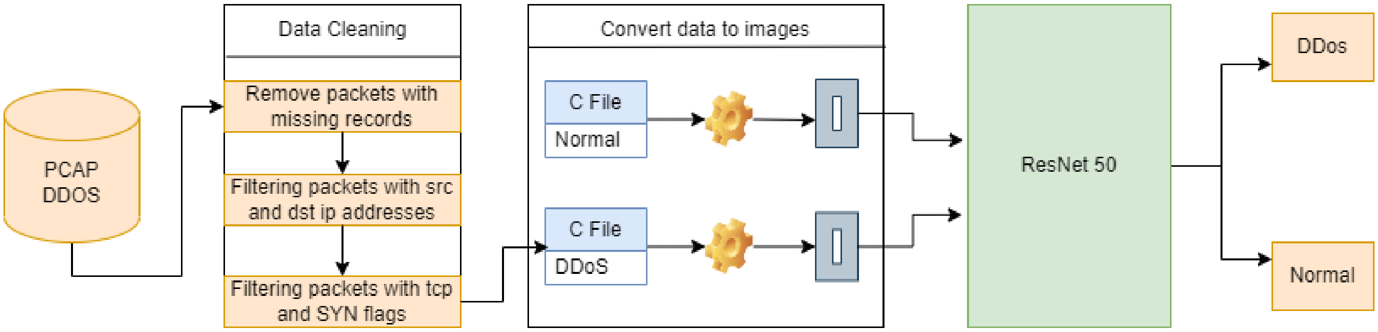
PCAP
DDOS
Data Cleaning
Remove packets with missing records
Filtering packets with src and dst ip addresses
Filtering packets with tcp and SYN flags
Convert data to images
C File
Normal
C File
DDoS
ResNet 50
DDos
Normal

Fig. 2. Proposed methodology to detect DDos attacks using ResNet50

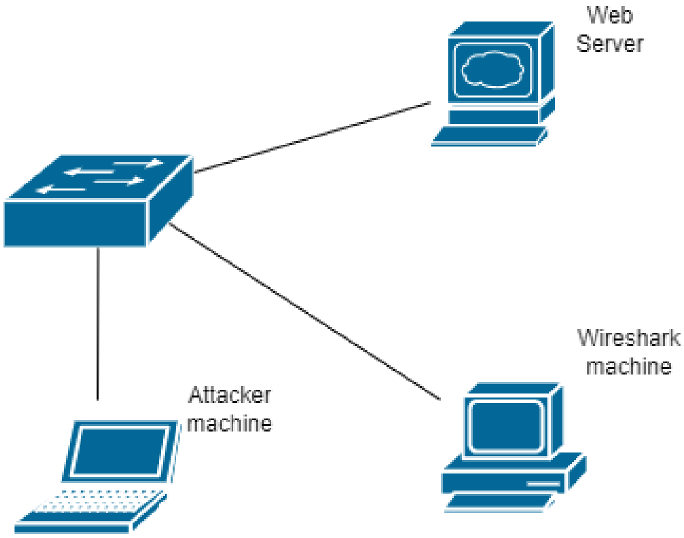

Fig. 3. Lab overview to generate network traffic

B. Processing Data

After acquiring the data, our next step is to process it into a well-formed dataset. This involves three key stages: data cleaning, data conversion, and finally, splitting the data for training, validation, and testing.

a) Data Cleaning: The acquired data, consisting of both attack and normal traffic, is initially stored in pcap files. To refine this data, we remove several unwanted packets by filtering the network data. This filtering process is based on specific criteria such as port information, the presence of SYN in packet details, and the source IP address of the attacker compared to the destination IP address of the web server. Consequently, we have a dataset that fully captures the DDoS attack traffic from the attacker to the web server.

Following this, we focus specifically on SYN flood packets, utilizing Wireshark tools to further filter out unnecessary features. This includes removing attributes like Bwd PSH Flags, Bwd URG, Fwd URG, FIN Flag count, PSH Flag count, and others. Through this meticulous data cleaning process, we ensure that our dataset for attack traffic retains only the essential features, optimizing it for effective training outcomes.

b) Data Conversion: Our methodology's data conversion process serves as a crucial link between raw network traffic data and the application of advanced machine learning techniques. Initially, pcap files with network traffic data are converted into C language arrays, each representing a network packet. These arrays are then transformed into two-dimensional (2D) grayscale images, with the elements of the arrays determining the pixel intensities, thus representing packet features. This crucial step enables the use of Convolutional Neural Network (CNN) to analyze network traffic and identify SYN flood attack patterns.

Subsequently, these grayscale images are resized to 224x224 pixels, a dimension chosen for compatibility with our CNN models, specifically the modified ResNet model employed in our study. Python scripts, using libraries like OpenCV or PIL (Python Imaging Library), are utilized for this resizing process. This step is carefully executed to adjust the images' scale and aspect ratio without compromising their key features, ensuring the integrity of the represented traffic data. Fig. 4 illustrates two such images: one representing DDoS and the other normal traffic.

Ensuring uniform image size, as achieved in our methodology, is critical for several reasons. It enables efficient batch processing in Convolutional Neural Network (CNN) and is in line with standard deep learning practices for image recognition. This consistency not only facilitates the use of pre-trained

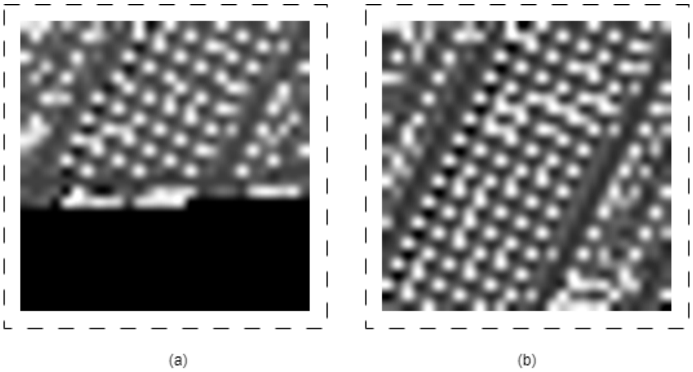

Fig. 4. (a) is for DDos packet image and (b)is for a normal packet image

models and established architectures with minimal changes but also plays a vital role in our data preparation process. It integrates network traffic data smoothly into advanced machine learning models, significantly enhancing the detection of DDoS attacks, particularly the challenging SYN flood attacks, by combining traditional network analysis with innovative AI techniques.

c) Train, Validation, Testing Splitting: Our process continues with organizing the converted 224x224 pixel images into specific sets for training, validation, and testing. We create three main directories for this purpose. The 'train' directory is bifurcated into 'ddos' and 'normal' subdirectories, containing images representative of DDoS and normal traffic, respectively.

A second directory, 'validation', mirrors this structure and contains a different set of images, ensuring the model's validation on unfamiliar data. This is crucial for evaluating the model's generalization capabilities.

For testing, we select around 2300 images each from both DDoS and normal traffic, storing them in a 'test' directory. This separate dataset is crucial for the final assessment of our model post-training, providing an unbiased evaluation of its performance in realistic scenarios.

C. Attack Detection

a) Utilizing CNN and ResNet50 Architecture:: For the task of detecting SYN flood DDoS attacks, we employed a Convolutional Neural Network (CNN) approach, specifically utilizing the ResNet50 architecture. ResNet50, known for its deep architecture of 50 layers, is highly effective in image classification tasks. This depth allows the network to learn a rich hierarchy of features, crucial for accurately distinguishing between complex patterns in DDoS and normal network traffic. The model was adapted for our binary classification task, discerning between DDoS attack images and normal traffic images.

b) Model Training and Data Augmentation:: Our training process involved feeding 224x224 pixel images into the ResNet50 model in batches of 32. We applied data augmentation techniques, such as rotation, width and height shift, and horizontal flipping, to the training dataset. These techniques help prevent overfitting and enhance the model's ability to generalize to new data. Training was facilitated by TensorFlow's MirroredStrategy for efficient computation across multiple GPUs or TPUs.

c) Model Validation and Custom Metrics:: In tandem with training, we validated the model using a distinct dataset to monitor and adjust its performance. A custom Keras callback was implemented to calculate the F1 score and precision at the end of each epoch. These metrics, critical in network security applications, provide a more nuanced view of the model's performance beyond standard accuracy.

d) Training Procedure and Epoch Management:: The model underwent a total of 10 epochs of training, with each epoch refining the model's weights for improved performance in subsequent iterations. This step-by-step approach ensured the model's continuous adaptation and optimization.

e) Post-Training Testing and Evaluation:: After completing the training phase, we proceeded to evaluate the model using two distinct test datasets. The first set comprises 2300 images each of DDoS and normal traffic, specifically generated in our lab environment. The second dataset, sourced from CICDDoS2019 [20], also consists of 2300 images representative of DDoS traffic. This dual-dataset approach is instrumental in determining the model's effectiveness in classifying unseen data under varied conditions.

IV. Results and Discussion

In this evaluation phase, we loaded the final trained model to conduct tests on both datasets. This step was essential to verify the model's real-world applicability and assess its accuracy in identifying DDoS attacks. For each dataset, we focused on calculating key performance metrics such as F1 score, precision, and recall. These metrics provide a comprehensive understanding of the model's capabilities, allowing us to compare its performance on our custom dataset against the external dataset. Such comparative analysis is crucial in demonstrating the robustness and adaptability of our system in different network security scenarios. The results of this testing, presented in a comparative table format, offer valuable insights into the strengths and potential areas for improvement in our DDoS detection methodology.

After completing the training phase of our system, as previously mentioned, we proceeded to test our model using two distinct datasets. The first dataset, which we created ourselves, and the second dataset, CICDDoS2019 [20], were both utilized for this evaluation. To assess the effectiveness of our system, we employed four key performance metrics: accuracy, precision, recall, and F1 score. The results of this evaluation, detailing the precision, recall, and F1 score for each dataset, are systematically presented in Table 1. Additionally, Fig. 5 displays the confusion matrix, which was generated from the application of our model to our own dataset, and Fig. 6 displays the confusion matrix for the CICDDoS2019 [20] dataset.

TABLE I
EVALUATION METRICS FOR OWN DATASET AND CICDDOS2019 [20] DATASET

Dataset	Accuracy	Precision	Recall	F1 Score
Own Dataset	0.999	0.999	0.999	0.999
CICDDoS2019 [20] Dataset	0.965	0.967	0.965	0.965
Both provided Datasets	0.977	0.983	0.982	0.982

The overall results obtained from our proposed methodology, which employs the ResNet 50 architecture, are highly encouraging. Utilizing our custom dataset, the system achieved an exceptional accuracy of 99.99%, demonstrating its efficacy in accurately identifying and classifying network traffic. This near-perfect accuracy underscores the model's capability to effectively discern between normal and DDoS attack patterns within the data we generated. In contrast, when applied to

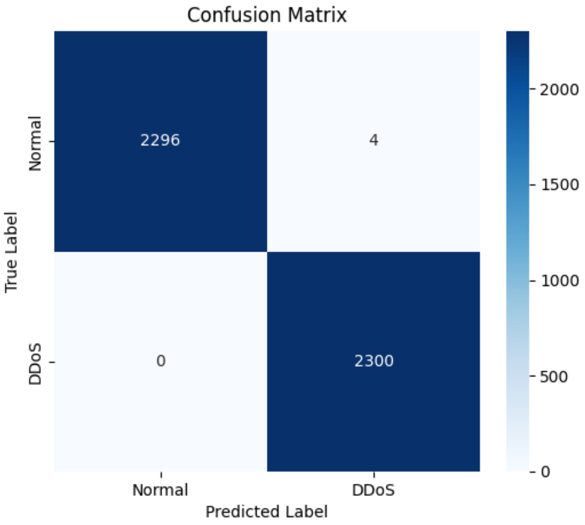

Fig. 5. Confusion matrix for our dataset

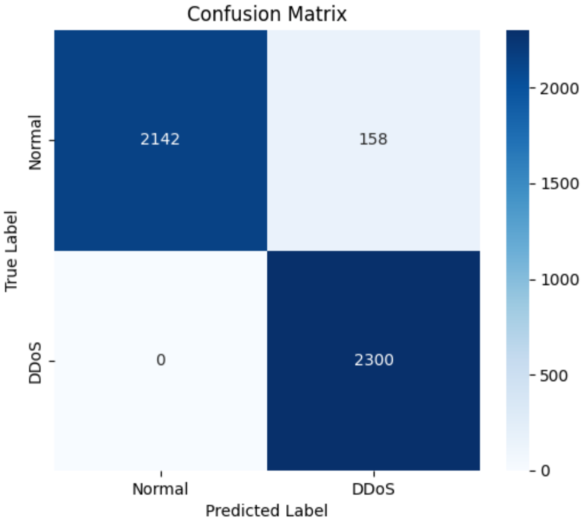

Fig. 6. Confusion matric for CICDDoS2019 [20] dataset

CICDDoS2019 [20] dataset, the accuracy slightly decreased to 96.56%. This reduction, although marginal, is insightful. It highlights the challenges posed by external data sources, which likely contain more varied and complex patterns, thus testing the model's adaptability and generalization capabilities.

V. Conclusion

These findings yield two primary insights: First, the remarkable accuracy achieved with our own dataset indicates that our ResNet 50-based model is well-calibrated and adept at discerning the nuances of network traffic in the environment for which it was specifically trained. This high level of precision points to the model's effectiveness in a controlled, known environment.

Second, while the performance for CICDDoS2019 [20] dataset remains commendable, it also unveils areas for potential enhancement. The observed decrease in accuracy, albeit slight, underlines the importance of generalizability across diverse network conditions. To address this, future work could focus on broadening the training dataset with more varied examples or employing advanced fine-tuning methods. Such improvements aim to bolster the model's ability to adapt to a wider range of network behaviors that were not part of the initial training data.

A significant direction for our future research is the expansion of our model's capabilities to classify various classes of DDoS attacks beyond just SYN flood attacks. Our goal is to develop a comprehensive system capable of accurately identifying and differentiating between multiple types of DDoS attacks, thereby providing a more robust solution to network security challenges.

In summary, this study demonstrates the capability of the ResNet 50 architecture in effectively classifying network traffic and discerning between regular operations and DDoS attack patterns. While the results highlight the model's current strengths, they also reveal the need for continuous improvements to adapt to the diverse and often unpredictable conditions of real-world network environments. Advancing this model to recognize a wider array of DDoS attack types is essential for its successful implementation in various cybersecurity contexts, thus establishing it as a crucial asset in advancing network security. Looking ahead, our focus will be on refining the model to achieve better generalization across different network scenarios. Future efforts will be directed towards broadening the model's ability to classify a wider spectrum of DDoS attacks, contributing to a more robust and comprehensive network security solution.

References

[1] what is dos attack? https://www.datto.com/blog/what-is-a-ddos-attack. Accessed: 2023-11-24.

[2] what is a syn flood attack? https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/. Accessed: 2023-11-24.

[3] Mustafa El Bizri, Ahmad M. EL-Hajj, and Ali M. Haidar. Towards safer wi-fi networks: Leveraging neural networks for intrusion detection. *4th IEEE International Multidisciplinary Conference on Engineering Technology (IMCET 23)*, 2023.

[4] Cisco annual internet report (2018–2023) white paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed: 2023-11-24.

[5] Hadi Al Mubasher, Ziad Doughan, Layth Sliman, and Ali Haidar. A novel neural network-based recommender system for drug recommendation. In *International Conference on Engineering Applications of Neural Networks*, pages 573–584. Springer, 2023.

[6] Rikiya Yamashita, Mizuho Nishio, Richard Kinh Gian Do, and Kaori Togashi. Convolutional neural networks: an overview and application in radiology. *Insights into imaging*, 9:611–629, 2018.

[7] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.

[8] Zhipeng Li, Zheng Qin, Kai Huang, Xiao Yang, and Shuxiong Ye. Intrusion detection using convolutional neural networks for representation learning. In *International conference on neural information processing*, pages 858–866. Springer, 2017.

[9] Anton Yudhana, Imam Riadi, and Faizin Ridho. Ddos classification using neural network and naïve bayes methods for network forensics. *International Journal of Advanced Computer Science and Applications*, 9(11), 2018.

[10] Dragan Peraković, Marko Periša, Ivan Cvitić, and Siniša Husnjak. Model for detection and classification of ddos traffic based on artificial neural network. *Telfor Journal*, 9(1):26–31, 2017.

[11] Xiang Liu, Ziyang Tang, and Baijian Yang. Predicting network attacks with cnn by constructing images from netflow data. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 61–66. IEEE, 2019.

[12] Deepak Kshirsagar and Sandeep Kumar. An ontology approach for proactive detection of http flood dos attack. *International Journal of System Assurance Engineering and Management*, pages 1–8, 2021.

[13] James Dzisi Gadze, Akua Acheampomaa Bamfo-Asante, Justice Owusu Agyemang, Henry Nunoo-Mensah, and Kwasi Adu-Boahen Opare. An investigation into the application of deep learning in the detection and mitigation of ddos attack on sdn controllers. *Technologies*, 9(1):14, 2021.

[14] Lin Chen, Xiaoyun Kuang, Aidong Xu, Siliang Suo, and Yiwei Yang. A novel network intrusion detection system based on cnn. In *2020 eighth international conference on advanced cloud and big data (CBD)*, pages 243–247. IEEE, 2020.

[15] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A Ghorbani. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, 1:108–116, 2018.

[16] Weiyou Liu, Xu Liu, Xiaoqiang Di, and Hui Qi. A novel network intrusion detection algorithm based on fast fourier transformation. In *2019 1st international conference on Industrial Artificial Intelligence (IAI)*, pages 1–6. IEEE, 2019.

[17] Nsl-kdd dataset. https://www.unb.ca/cic/datasets/nsl.html. Accessed: 2023-12-03.

[18] Gilbert George and Chandrashekhar Uppin. A proactive approach to network forensics intrusion (denial of service flood attack) using dynamic features, selection and convolution neural network. *Open Journal of Physical Science (ISSN: 2734-2123)*, 2(2):01–09, 2021.

[19] Jirasin Boonchai, Kotcharat Kitchat, and Sarayut Nonsiri. The classification of ddos attacks using deep learning techniques. In *2022 7th International Conference on Business and Industrial Research (ICBIR)*, pages 544–550. IEEE, 2022.

[20] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A Ghorbani. Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)*, pages 1–8. IEEE, 2019.

[21] P Shorubiga and R Shyam. Cnn-based model for the http flood attack detection. In *2023 International Conference for Advancement in Technology (ICONAT)*, pages 1–6. IEEE, 2023.

[22] Ddos attack network logs. https://www.kaggle.com/datasets/jacobvs/ddos-attack-network-logs. Accessed: 2023-12-03.

[23] Ahmed Ramzy Shaaban, Essam Abd-Elwanis, and Mohamed Hussein. Ddos attack detection and classification via convolutional neural network (cnn). In *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, pages 233–238. IEEE, 2019.

[24] Faisal Hussain, Syed Ghazanfar Abbas, Muhammad Husnain, Ubaid U Fayyaz, Farrukh Shahzad, and Ghalib A Shah. Iot dos and ddos attack detection using resnet. In *2020 IEEE 23rd International Multitopic Conference (INMIC)*, pages 1–6. IEEE, 2020.