Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047387 Published Online: 02 February 2024

ARTICLE

Unknown DDoS Attack Detection with Fuzzy C-Means Clustering and Spatial Location Constraint Prototype Loss

Thanh-Lam Nguyen[1], Hao Kao[1], Thanh-Tuan Nguyen[2], Mong-Fong Horng[1,*] and Chin-Shiuh Shieh[1,*]

[1]Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, 807618, Taiwan

[2]Department of Electronic and Automation Engineering, Nha Trang University, Nha Trang, 650000, Vietnam

*Corresponding Authors: Mong-Fong Horng. Email: mfhorng@nkust.edu.tw; Chin-Shiuh Shieh. Email: csshieh@nkust.edu.tw

Received: 04 November 2023 Accepted: 25 December 2023

ABSTRACT

Since its inception, the Internet has been rapidly evolving. With the advancement of science and technology and the explosive growth of the population, the demand for the Internet has been on the rise. Many applications in education, healthcare, entertainment, science, and more are being increasingly deployed based on the internet. Concurrently, malicious threats on the internet are on the rise as well. Distributed Denial of Service (DDoS) attacks are among the most common and dangerous threats on the internet today. The scale and complexity of DDoS attacks are constantly growing. Intrusion Detection Systems (IDS) have been deployed and have demonstrated their effectiveness in defense against those threats. In addition, the research of Machine Learning (ML) and Deep Learning (DL) in IDS has gained effective results and significant attention. However, one of the challenges when applying ML and DL techniques in intrusion detection is the identification of unknown attacks. These attacks, which are not encountered during the system's training, can lead to misclassification with significant errors. In this research, we focused on addressing the issue of Unknown Attack Detection, combining two methods: Spatial Location Constraint Prototype Loss (SLCPL) and Fuzzy C-Means (FCM). With the proposed method, we achieved promising results compared to traditional methods. The proposed method demonstrates a very high accuracy of up to 99.8% with a low false positive rate for known attacks on the Intrusion Detection Evaluation Dataset (CICIDS2017) dataset. Particularly, the accuracy is also very high, reaching 99.7%, and the precision goes up to 99.9% for unknown DDoS attacks on the DDoS Evaluation Dataset (CICDDoS2019) dataset. The success of the proposed method is due to the combination of SLCPL, an advanced Open-Set Recognition (OSR) technique, and FCM, a traditional yet highly applicable clustering technique. This has yielded a novel method in the field of unknown attack detection. This further expands the trend of applying DL and ML techniques in the development of intrusion detection systems and cybersecurity. Finally, implementing the proposed method in real-world systems can enhance the security capabilities against increasingly complex threats on computer networks.

KEYWORDS

Cybersecurity; DDoS; unknown attack detection; machine learning; deep learning; incremental learning; convolutional neural networks (CNN); open-set recognition (OSR); spatial location constraint prototype loss; fuzzy c-means; CICIDS2017; CICDDoS2019

1 Introduction

After the outbreak of the new Coronavirus pneumonia in 2020, people have become more reliant on the internet. Entertainment, shopping, education, and other remote activities on the Internet have become increasingly diverse and rapidly growing. Naturally, the number of DDoS attacks has been significantly increasing. CloudFlare, a content delivery network (CDN) and attack mitigation service provider, published a quarterly investigation on DDoS attacks [1] showing thousands of attacks occurring every month. While most attack traffic remains below 500 Mbps, this volume is sufficient to cause short disruptions for some enterprise services. However, the stability of networks and services is of utmost importance for a business service provider. The service disruption caused by an attack can lead to business losses, and more importantly damage to their image and reputation.

Defending enterprise network systems against DDoS attacks is an essential demand. Nevertheless, DDoS attack methods are continually evolving and becoming more diverse. In contemporary times, the IDS system plays a pivotal role in securing computer networks by identifying and responding to malicious activities in general, and DDoS attacks in particular. Researching and integrating cutting-edge technologies, such as ML and DL technologies into IDS systems to enhance their capabilities is an inevitable trend. Many related experiments have demonstrated that ML and DL methods achieve very high accuracy, up to 98%, on conventional data [2–4]. However, existing ML and DL methods primarily focus on modeling and normalizing known attack patterns. Consequently, these methods often struggle to effectively identify unknown attacks with new characteristics, leading to a reduction in the defensive efficacy of IDS systems. Therefore, the identification of unknown DDoS attacks continues to pose a significant challenge for IDS systems.

The main objective of our research is to propose multiple IDS methods capable of concurrently detecting both known and unknown DDoS attacks and evaluating their detection performance. To address this challenge, we emphasize the necessity of the Open-Set Recognition (OSR) technique. The OSR technique deals with the challenge of identifying and classifying objects or instances not encountered during the training phase. Recently, there have been several outstanding achievements in OSR techniques [5]. Notably, the Spatial Location Constraint Prototype Loss (SLCPL) [6] method is a novel OSR technique designed for deep neural networks. It has demonstrated superior effectiveness compared to many previous OSR techniques when testing on many different datasets, with a majority achieving accuracy above 88% [6]. However, when applied alone in the context of detecting unknown DDoS attacks, the effectiveness of SLCPL is not excellent enough. Therefore, we have considered a supporting method, the Fuzzy C-Means (FCM) [7] clustering technique, with a prominent soft clustering feature. The combination of SLCPL and FCM enhances the ability to recognize changes in data patterns, increasing the accuracy of identifying unknown attacks.

Through the utilization of the FCM and the SLCPL, our proposed method achieves an impressive accuracy of up to 99.7% and a precision of up to 99.9% for unknown DDoS attack detection on the open CICDDoS2019 dataset. Simultaneously, it maintains a high accuracy of 99.8% for known attack detection on the well-known CICIDS2017 dataset. With this achievement, we aim to enhance tech organizations' detection capabilities, safeguarding network infrastructure and ensuring service continuity amid evolving network threats.

The key contributions of this research are focused on the following aspects:

- We have selected AlexNet [8] as the neural network architecture for our training process, and we have enhanced the AlexNet architecture for more effective classification of conventional data.

• Through the SLCPL and FCM methods, we have adjusted the positions of unknown attack samples in the feature space, bringing them closer to specific categories and thus enabling the recognition of unknown DDoS attacks.

The structure of this article is as follows: Section 2 presents a concise summary of pertinent literature. Section 3 encompasses the system's architecture, the methodologies, and the algorithms utilized. Section 4 provides a detailed account of the experimental procedure and presents the findings obtained. The research is concluded in Section 5, which also explores potential directions for future research.

2 Related Work

Detecting and mitigating DDoS attacks is a top concern in modern cybersecurity. Several methods have been proposed to handle this problem, varying from traditional signature-based methods to more advanced anomaly detection techniques.

2.1 DDoS Attack Detection Technique

Traditional signature-based methods have undeniable advantages such as effectiveness against known DDoS attacks, low false positive rate, and ability to respond quickly to attacks. However, the signature-based method clearly shows its disadvantages against unknown DDoS attacks, zero-day attacks as well and high dependence on databases. Researchers have recognized the limitations of signature-based systems and have explored other approaches. In recent years, ML and DL technologies have been a research trend in developing IDS systems [9].

Recent research by Maseer et al. [2] synthesized and compared current popular ML algorithms on the CICIDS2017 dataset. In their research, multiple algorithms have demonstrated highly favorable outcomes, including Support Vector Machine (SVM), Random Forest (RF), Naive Bayes (NB), Artificial Neural Networks (ANN), and Convolutional Neural Network (CNN).

Ho et al. [3] introduced a novel CNN approach that surpasses conventional single-class classification methods, delivering exceptional performance in the realm of multi-class classification, particularly in the identification of both known and unknown attacks. Furthermore, many studies have applied CNN-based models, producing highly effective results [10,11].

Kim et al. [4] introduced a DL model that combines CNN and Recurrent Neural Networks (RNN) to detect Denial of Service (DoS) attacks. They optimized the CNN design through numerous experiments and achieved impressive results, particularly in terms of accuracy on two datasets KDD and CSE-CIC-IDS2018.

Kiranyaz et al. [12] surveyed 1D Convolutional Neural Networks (1D-CNN) and their main applications. The 1D-CNN model [12,13] has demonstrated its advantages in a scarce training data environment as well as in some specific fields such as anomaly detection, personalized biomedical data classification, early diagnosis, etc.

Beitollahi et al. [14] proposed an ML approach for detecting DDoS traffic. Their approach employs a Radial Basis Function (RBF) network in conjunction with the cuckoo search algorithm (CSA) to identify Application-layer DDoS attacks. This approach stands out for its effective performance in identifying DDoS traffic compared to several other methods, with notably low error rates and high precision.

Laghrissi et al. [15] presented an IDS that utilizes Long Short-Term Memory (LSTM) networks, in combination with Principal Component Analysis (PCA) and Mutual Information (MI) techniques. This method achieves outstanding accuracy compared to other methods in both binary and multiclass classification.

2.2 Open Set Recognition Technique

The Open Set Recognition (OSR) technique aims to classify data into known classes and detect instances that do not belong to any known class, unknown class, or new instances [5].

Recent advancements in OSR techniques include the work of Bendale et al. [16], who introduced the OpenMax technique. This technique has become a crucial method in the field of open-set recognition, where systems need the capability to recognize objects that do not belong to any of the classes learned during training. The fundamental theory behind the OpenMax algorithm involves calculating the "openness" level of a data sample based on the distance between that sample and the nearest samples in the nearest known class. OpenMax allows for the determination of whether a data sample belongs to a known class, an open-set class (a class corresponding to openness), or is unknown (not belonging to any known class). This enhances recognition capabilities in real-world situations where objects that do not belong to any known class may appear.

Ge et al. [17] have published their research results as a development method of OpenMax. Unlike previous methods where unknown classes were inferred based on characteristics or distance decisions with known classes, the authors' novel approach offers a clear framework and decisive criterion for unknown classes. The proposed technique, known as Generative OpenMax, enhances OpenMax by incorporating Generative Adversarial Networks (GANs) to create images for new classes artificially. Additionally, Yoshihashi et al. [18] have proposed the Classification-Reconstruction learning for the OSR method (CROSR) to enhance the reliable detection of unknown classes without affecting the accuracy of known classes. Research results have shown the superiority of this method over traditional approaches.

Generally, Open-Set Recognition has been receiving the attention and research efforts of many scientists and scholars worldwide. The mentioned papers provided earlier represent only a fraction of the noteworthy contributions within this field.

2.3 Unknown DDoS Attack Detection Technique

The task of identifying unknown DDoS attacks is difficult, requiring inventive methods to improve the protection of network infrastructures. In recent years, researchers have made significant progress in the field of unknown DDoS attack detection, employing various techniques and methodologies to identify and mitigate these threats [19]. This section provides an overview of recent advances in unknown DDoS attack detection, highlighting key contributions in this domain.

Extreme Value Theory (EVT) has been utilized to enhance the identification of DDoS attacks [20]. This statistical methodology has proven effective in capturing the extreme behaviors of network traffic, aiding in the recognition of anomalous patterns associated with DDoS attacks.

Gaussian Mixture Models (GMMs) and related methods have been widely used for determining the distribution of network traffic data [21,22]. Chapaneri et al. have explored the use of several GMMs for modeling individual input features in the context of DDoS detection [21]. By modeling the underlying data distribution, this technique can help distinguish between benign and malicious traffic patterns, contributing to more accurate detection. Shieh et al. have adopted DL techniques, including Bidirectional Long Short-Term Memory (BI-LSTM) networks and GMMs, for the identification of unknown DDoS attacks [22]. Their research demonstrates the efficacy of combining deep learning and statistical modeling for robust attack identification.

Yang et al. have introduced the AutoEncoder-based DDoS attacks Detection Framework (AE-D3F), a novel technique for threat detection, which has shown promise in identifying anomalous network behavior [23]. By leveraging autoencoders, they contribute to the arsenal of tools for enhancing DDoS attack detection.

Generative Adversarial Networks (GANs) have demonstrated efficacy in DDoS attack detection [24,25]. GANs are proficient in generating synthetic data that can be used to compare and contrast with real network traffic, aiding in the identification of malicious activity. Lin et al. have presented the IDSGAN framework, which incorporates GAN networks as part of a defense system to protect against DDoS attacks [24]. This approach focuses on the proactive use of GANs to safeguard network resources. Chauhan et al. have harnessed Wasserstein GAN (WGAN) to address training issues in DDoS detection models [25]. By incorporating WGAN, they aim to improve the robustness and reliability of DDoS detection techniques.

2.4 Fuzzy C-Means Clustering and Comparison between Recent Algorithms

Fuzzy C-Means (FCM) clustering is a common unsupervised learning technique used for data clustering and classification. In the context of DDoS attack detection, FCM has been applied to group network traffic data into clusters, allowing the identification of abnormal traffic patterns related to attacks. The work by Wu et al. [26] used FCM clustering to partition network traffic data into distinct clusters and then employed anomaly detection techniques to identify DDoS attacks within these clusters. This approach has shown promising results in the identification of both known and unknown attacks.

In this section, we have discussed various approaches related to DDoS attack detection, OSR techniques, and Fuzzy C-Means clustering. For convenience, we have established a comparison table among recent research studies in machine learning and deep learning. Table 1 summarizes the techniques used, the scope of the problems, and some limitations of the studies.

Table 1: Comparison between recent machine learning techniques

Author	Dataset	Problem scope	Technical	Limitation
Ho et al. (2021) [3]	CICIDS2017	CSR, OSR	An IDS based on CNN and its comparison against nine well-known classifiers.	The model may struggle with classes having insufficient samples in the CICIDS2017 dataset, indicating potential issues in detecting open set data.

(Continued)

Table 1 (continued)

Author	Dataset	Problem scope	Technical	Limitation
Laghrissi et al. (2021) [15]	KDD99	CSR	An LSTM network, combined with PCA and ML techniques for intrusion detection.	The primary limitation is the reliance on the KDD99 dataset, which, despite its widespread use, is outdated and not fully representative of current network traffic and attack patterns.
Chapaneri et al. (2021) [21]	CICIDS2017	CSR, OSR	A robust GMM with multiple levels has been proven effective in multi-class classification.	The model's effectiveness is tied to the quality and comprehensiveness of the CICIDS2017 dataset.
Beitollahi et al. (2022) [14]	NSL-KDD	CSR	An RBF network model with CSA technique.	The study primarily relies on the NSL-KDD dataset could limit the model's broader applicability, especially in open-set attacks.
Najafimehr et al. (2022) [27]	CICIDS2017, CICDDoS2019	CSR, OSR	The Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm is utilized for traffic labeling, while statistical measures are employed to define the ML framework for DDoS detection.	The computational complexity and resources required for the proposed method might be challenging for real-world deployment.
Zhao et al. (2023) [28]	CICDDoS2019, CICIDS2017, CICIDS2018, KDD_CUP99, NSL-KDD, UNSW	CSR	An automatic method for generating Deep Neural Network (DNN) networks by using a genetic algorithm.	This study primarily focuses on model generation for close-set recognition (CSR).
Sharif et al. (2023) [29]	CICIDS2017	CSR	The study explores the use of Multi-layer Perceptron (MLP) to detect DDoS attacks produced by different tools.	The study primarily relies on the CICIDS2017 dataset could limit the model's broader applicability, especially in open-set attacks.

(Continued)

Table 1 (continued)

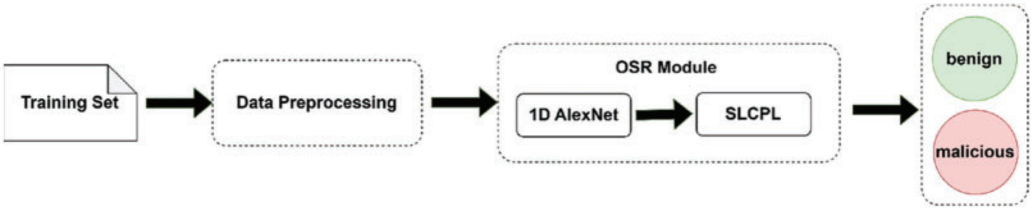
Author	Dataset	Problem scope	Technical	Limitation
Shieh et al. (2023) [30]	CICIDS2017, CICDDoS2019	CSR, OSR	DDoS defense model employs Reconstruct Error and One-Class SVN (OC-SVM) featuring Stochastic Gradient Descent (SGD).	The complexity of the proposed method might also pose challenges in terms of computational resources and real-time applicability.
Our	CICIDS2017, CICDDoS2019	CSR, OSR	CNN-based model, combined with OSR and FCM techniques for unknown attack detection.	N/A

Recent notable studies have primarily focused on addressing the challenge of Closed Set Recognition (CSR). Some performance evaluations are conducted on outdated datasets (KDD99) or specific datasets such as NSL-KDD or CICIDS2017. Regarding methods for tackling the OSR problem, some approaches exhibit drawbacks, such as complexity and difficulty in real-world deployment. Our proposed method successfully addresses both CSR and OSR problems, with performance validated on both the CICIDS2017 and CICDDoS2019 datasets. This approach achieves exceptionally high performance and flexibility for real-world deployment. Of course, our method still has some limitations, which will be discussed in the section “Discussion” of this article.

In the following sections, we will explain our method in detail, a solution involving a deep neural network combined with the SLCPL and FCM techniques to detect unknown DDoS attacks. This combination is relatively new and remains unexplored.

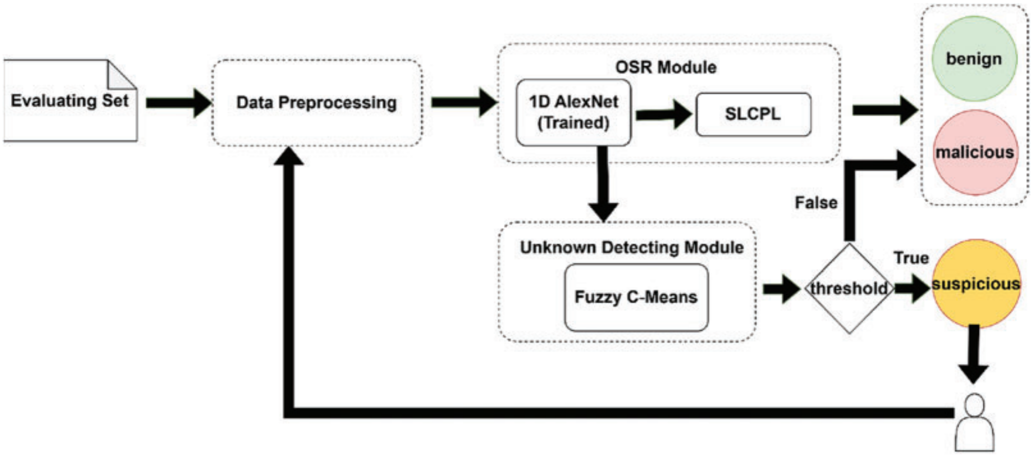
3 Proposed IDS

Figs. 1a and 1b show the architecture of our proposed IDS developed in this research. The architecture consists of three main modules: Data Preprocessing Module, OSR Module, and Unknown Detecting Module. The primary machine learning technologies include AlexNet, SLCPL, and FCM. AlexNet is a deep CNN architecture that takes on an essential role in the development and popularization of deep learning. The SLCPL is a novel OSR technique with outstanding advantages. Additionally, we utilized the FCM clustering technique to distinguish between known and unknown attacks. By including the clustering method, the classification performance is enhanced compared to using SPCLP alone.



(a)

Figure 1a: Training phase



(b)

Figure 1b: Evaluating phase

3.1 AlexNet

AlexNet, a Convolutional Neural Network, was developed by Krizhevsky and his team in 2012. It garnered significant acclaim for its exceptional performance in the ImageNet Large Scale Visual Recognition Challenge (ILSVRC) competition [8]. This network architecture marked an important milestone at the time, having a major influence on the advancement of deep learning and the development of the task of image classification.

The main characteristics of AlexNet lie in its combination of depth, convolution, and pooling layers, along with a large number of trainable parameters. Its architecture is as follows:

- Convolutional and Pooling Layers: AlexNet utilizes convolutional and pooling layers to extract features. The layers efficiently capture specific characteristics within images and employ pooling layers to decrease the complexity of feature maps while preserving important features.
- Activation Function: The (Rectified Linear Unit) ReLU activation function is applied by AlexNet after each convolutional layer to mitigate the issue of vanishing gradients and accelerate the training process.
- Dropout: The dropout technique is introduced in the fully connected layers of AlexNet, mitigating overfitting and enhancing the model's generalization capability.
- Multi-GPU Training: AlexNet pioneered the use of multiple GPUs for training in deep learning models, significantly accelerating the training process.

The success of AlexNet underscores the formidable capabilities of deep learning in tasks like image classification. While more profound neural network architectures emerged in the subsequent years, AlexNet's role as a starting point in deep learning has cast a lasting influence on the design and development of subsequent models. Fig. 2 describes the architecture of the AlexNet network.

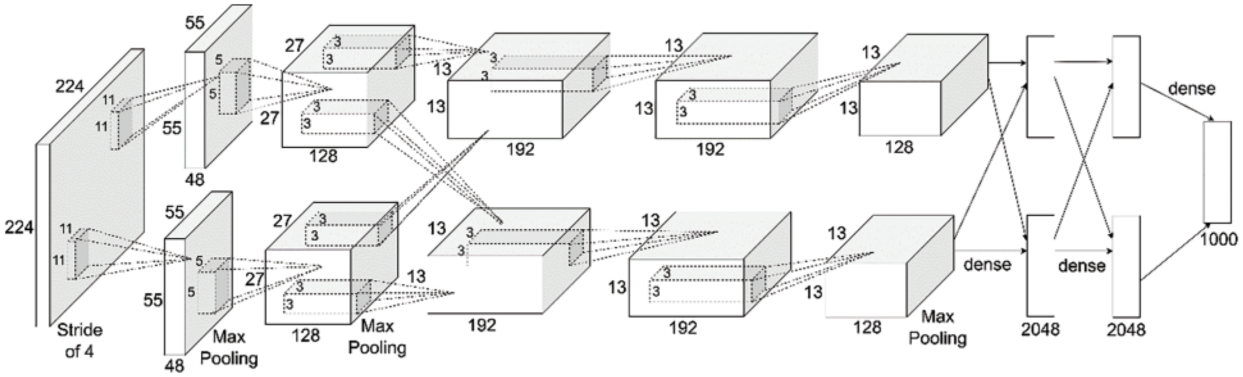


Figure 2: AlexNet architecture

3.1.1 1D AlexNet

In our model, we adapted the architecture of AlexNet using one-dimensional convolution. The structure of 1D AlexNet is similar to 2D AlexNet, and the main difference is that 1D AlexNet processes one-dimensional input data. In this research, we have modified the model of 1D AlexNet as shown in Fig. 3.

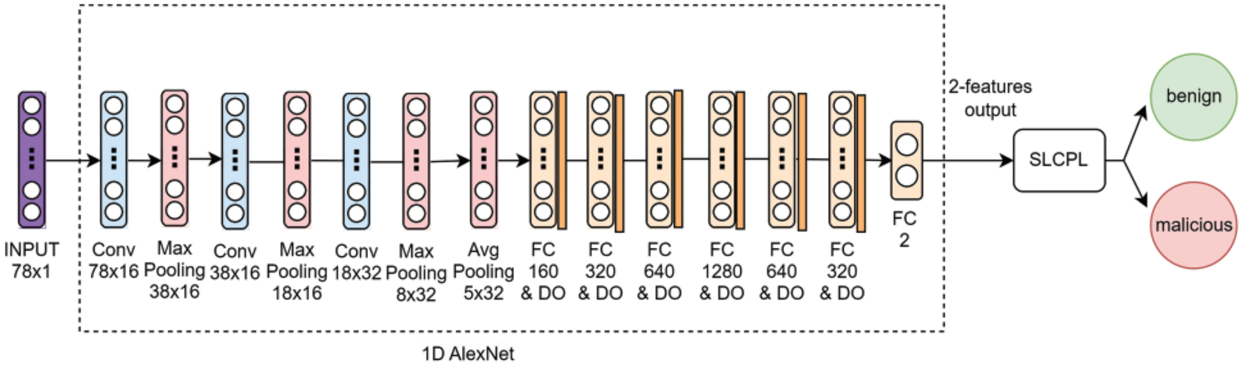


Figure 3: The architecture of improved 1D AlexNet

The model includes some important components as follows. First, convolutional layers use convolution to capture features from one-dimensional data. Next, activation function classes introduce nonlinearity, using the ReLU function. Subsequently, pooling layers are incorporated to diminish the dimensions of the feature map and the computational load, while preserving crucial features. Here, we utilized two kinds of pooling layers, Max Pooling and Average Pooling.

Additionally, 1D AlexNet includes fully connected layers to map features to the end goal of the classification. Normally, the output layer utilizes the SoftMax function to produce the final classification result. However, in this research, we used the SLCPL technique for classification during the training process as well as the evaluation process. Preceding a fully connected layer, a dropout layer is employed to alleviate overfitting. Finally, the proposed modified model is the best result of our multiple testing iterations.

3.2 Spatial Location Constraint Prototype Loss

Spatial Location Constraint Prototype Loss (SLCPL) [6] is an OSR technique, a loss function designed for the Convolutional Neural Network model. The SLCPL extends from the Generalized Convolutional Prototype Learning (GCPL) [31] by introducing spatial location constraints to solve a common issue faced by most current training methods, such as SoftMax and GCPL. The problem lies in the concentration of known features towards the center of the feature space, resulting in the overlapping of known and unknown feature distributions. To prevent this phenomenon, a spatial location restriction is incorporated into the loss function while undergoing the prototype learning procedure. This allows SLCPL to manipulate the spatial positioning of the prototypes. Consequently, the known features tend to be located in the periphery of the feature space, while the center of the feature space is typically reserved for unknown features.

We will describe the SLCPL function as follows:

Given a training set S $= \{(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots\}$ with N known classes, and the label x_i is $y_i \in \{1, 2, 3, \ldots, N\}$. A CNN is a classifier with the parameters θ and the embedding function F. The prototypes O $= \{O^i, i = 1, 2, 3, \ldots, N\}$ are initialized randomly or with a distribution.

With a training sample (x, y), the SLCPL loss function can be represented by:

$$L_s = L_G\left(x, y; \theta, O\right) + slc(O) \tag{1}$$

Here $L_G\left(x, y; \theta, O\right)$ is a GCPL loss function and $slc\left(O\right)$ is a spatial location constraint introduced by SLCPL.

$L_G\left(x, y; \theta, O\right)$ can be represented as follows:

$$L_G\left(x, y; \theta, O\right) = l\left(x, y; \theta, O\right) + \lambda.pl\left(x; \theta, O\right) \tag{2}$$

The function $l\left(x, y; \theta, O\right)$ will be optimized to cluster different known classes. And $l\left(x, y; \theta, O\right)$ can be represented as follows:

$$l\left(x, y; \theta, O\right) = -\log p\left(y = k|\, x, F, O\right) = -\log \frac{e^{-d(F(x), O^k)}}{\sum_{i=1}^{N} e^{-d(F(x), O^k)}}, \text{with K = 1,....N} \tag{3}$$

where $d\left(F\left(x\right), O^k\right)$ is the Euclidean distance between $F\left(x\right)$ and O^k.

The param λ and the constraint $pl\left(x; \theta, O\right)$is used to enhance the compactness of the cluster.

$$pl\left(x; \theta, O\right) = ||F\left(x^k\right) - O^k||^2, \text{with} \quad \text{K} = 1, 2, \text{....N} \tag{4}$$

where x^k is the training sample of class k.

The spatial location constraint $slc(O)$ can be represented as follows:

$$slc\left(O\right) = \frac{1}{N-1} \sum_{i=1}^{N} \left(r_i - \frac{1}{N} \sum_{j=1}^{N} r_j\right)^2 \tag{5}$$

where $r_i = d(O^k, O_c)$ and $O_c = \frac{1}{N} \sum_{i=1}^{N} O^i$.

To clarify, $slc(O)$ represents the variability of the distances r_i between the prototype of the cluster and the center O_c.

As presented, the time complexity to compute the SLCPL loss function for each data sample is O(N.D), where N is the number of known classes and D is the dimensionality of the feature space.

Finally, SLCPL is a new OSR technique with the ability to enhance the accuracy for classifying known and unknown classes. And SLCPL and 1D AlexNet are a promising combination for our OSR module.

3.3 Fuzzy C-Means

Fuzzy C-Means (FCM) [7] is a clustering analysis method to partition samples into multiple fuzzy categories. The algorithm considers the degree of membership of each sample to every category rather than just employing traditional hard clustering methods. In this research, we integrated FCM with OSR modules including SLCPL and 1D AlexNet. The 2-feature output from the OSR module will be clustered by FCM for Unknown DDoS attack detection.

We will describe the FCM algorithm as follows:

Given N samples and C cluster centers, each sample is denoted as x_i, and each cluster center as v_j. Define the fuzzy membership matrix U, where U_{ij} is the degree of membership of the sample x_i to cluster center v_j. The objective function of FCM is to minimize the following cost function:

$$J(U, V) = \sum\nolimits_{i=1}^{N} \sum\nolimits_{j=1}^{C} U_{ij}^{m} ||x_i - v_j||^2 \tag{6}$$

Here, m is the fuzziness param that controls the degree of fuzziness in clustering. This objective function combines the weighted total of Euclidean distances between the samples and the cluster centres. The algorithm operates in the following manner:

i. Initialize the fuzzy assignment matrix U and cluster centers V.
ii. Perform iterative updates until a stopping condition is met (the maximum number of iterations or convergence of the objective function):
  a. Update U: Compute the degree of membership of each sample to each cluster center using the membership update formula:

$$U_{ij} = \left(\sum\nolimits_{k=1}^{C} \left(\frac{||x_i - v_j||}{||x_i - v_k||} \right)^{\frac{2}{m-1}} \right)^{-1} \tag{7}$$

  b. Update V:

$$v_j = \frac{\sum\nolimits_{i=1}^{N} U_{ij}^{m} . x_i}{\sum\nolimits_{i=1}^{N} U_{ij}^{m}} \tag{8}$$

iii. Returns the final fuzzy assignment matrix U and the cluster centers V.

As presented, the time complexity of FCM typically is O(I.N.C.D), where I represents the number of iterations, N represents the number of data samples, C represents the number of clusters, and D represents the dimension of each data sampling.

The core principle of this algorithm lies in iteratively updating the fuzzy assignment matrix and cluster centers, continuously adjusting the membership degrees of samples and the positions of cluster centers to minimize the objective function. Through the fuzzy assignment matrix, one can obtain the fuzzy membership degrees of each sample concerning each cluster center rather than solely obtaining rigid classification outcomes.

4 Experiments and Results

4.1 Dataset

In this research, we utilized the CICIDS2017 [32] and CICDDoS2019 [33] datasets to evaluate the proposed IDS. The CICIDS2017 and CICDDoS2019 are widely used datasets for IDS research and development. Developed by the Canadian Institute of Cyber Security (CIC), they aim to simulate various cyber attacks and common traffic in real-world networks. The simulation environment is set up with complete network topology, actual network traffic, and attack behaviors. They are used for various purposes, such as training, validating, and testing IDS performance. Both are valuable for many tasks like feature selection, model optimization, algorithm comparison, and other intrusion IDS-related research.

The CICIDS2017 dataset was collected from 9 AM on Monday, July 03, 2017, to 5 PM on Friday, July 07, 2017, spanning a duration of 5 days. The CICIDS2017 dataset encompasses a diverse range of attacks, such as Brute Force, DoS, Web Attack, Infiltration, Botnet, Heartbleed, and DDoS. In addition, the CICDDoS2019 dataset includes both benign traffic and the latest prevalent DDoS attacks such as DNS, LDAP, NETBIOS, and SNMP.

We utilized the CICIDS2017 Wednesday dataset to train the model in the context of known attack detection. In addition, we utilized CICIDS2017 Friday and CICDDoS2019 datasets in the context of unknown attack detection. Table 2 describes the structure of the datasets we used in this research.

Table 2: Statistics of experimental datasets

Dataset	Attack type	Quantity	Ratio	Total
CICIDS2017 Wednesday <<train dataset<<	BENIGN DoS Hulk DoS GoldenEye DoS Slowloris DoS Slowhttptest HeartBleed	319,186 159,049 7647 5707 5109 11	64.260% 32.021% 1.540% 1.149% 1.029% 0.002%	496,709
CICIDS2017 Friday	BENIGN DDoS	128027 97718	56.713% 43.287%	225745
CICDDoS2019 LDAP	BENIGN LDAP	1602 2,179,928	0.073% 2,179,928	2,181,530
CICDDoS2019 MSSQL	BENIGN MSSQL	1995 4,522,489	0.044% 99.956%	4,524,484
CICDDoS2019 DNS	BENIGN DNS	3380 5,071,002	0.067% 99.933%	5,074,382
CICDDoS2019 NetBIOS	BENIGN NetBIOS	1705 4,093,273	0.042% 99.958%	4,094,978
CICDDoS2019 NTP	BENIGN NTP	14,337 1,202,639	1.178% 98.822%	1,216,976

(Continued)

Table 2 (continued)

Dataset	Attack type	Quantity	Ratio	Total
CICDDoS2019 UDP	BENIGN UDP	2151 3,134,643	0.069% 99.931%	3,136,794
CICDDoS2019 SNMP	BENIGN SNMP	1502 5,159,863	0.029% 99.971%	5,161,365
CICDDoS2019 SSDP	BENIGN SSDP	762 2,610,610	0.029% 99.971%	2,611,372
CICDDoS2019 SYN	BENIGN Syn	389 1,380,015	0.028% 99.972%	1,380,404

4.2 Data Pre-Processing

Data pre-processing is a very important phase in conducting machine learning experiments. Preprocessing ensures the accuracy and reliability of the output. In this research, this phase includes Data cleaning and Feature transformation.

4.2.1 Data Cleaning

Data cleaning is a necessary process during preprocessing. Error data will be corrected to ensure the experiment produces the best and most reliable results. In this research, we clean the data by using the following methods:

- For data samples whose value of any feature is NAN, we proceed with elimination.
- For features whose value is INF, we replaced the value with 10E10.
- For features with negative values, we replaced the negative value with 0.

4.2.2 Feature Transformation

In this research, we have referred to the processing methods of Chapaneri et al. in the article [21] during the data transformation process. The feature value is transformed according to the following formula:

$$X \leftarrow \frac{log_{10}(X+1)}{10} \tag{9}$$

After data are transformed, the values of all features will be in the range [0, 1].

4.3 Experimental Environment

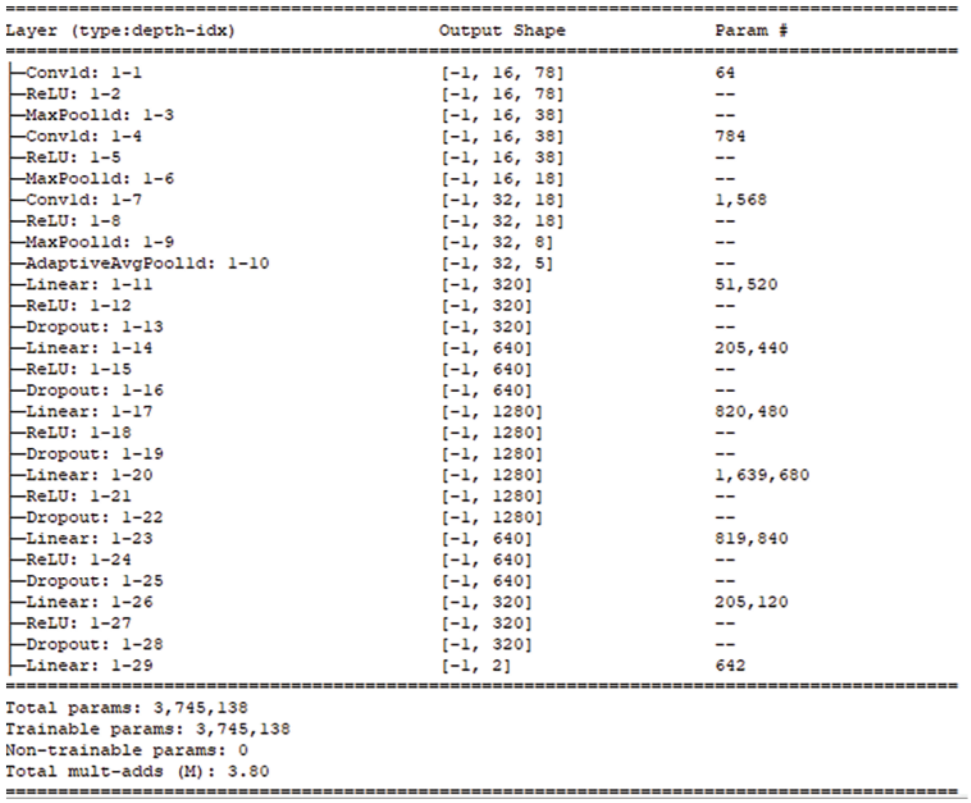
In this research, we utilized a workstation with the Ubuntu 20.04 OS. Our workstation is equipped with an AMD Ryzen 5700X 8C16T processor, 96 GB DDR4 memory, and Nvidia RTX3070 and Nvidia RTX2060 as computational accelerators. Regarding the model framework, we undertake development using PyTorch 1.11.0, Sklearn, and Python 3.9.12.

4.4 Model Training

In this research, we have built the 1D AlexNet model using the Pytorch framework and calculated the evaluation metrics using Sklearn. To evaluate the model's effectiveness, we trained the model ten times using a different random number each time. We chose Adam as the optimizer. The detailed settings of the parameters are described in Table 3. And Fig. 4 shows the network model of 1D AlexNet.

Table 3: Training parameters

Parameters	Value
Learning rate	3.00E-03
Weight decay	3.00E-05
Optimizer	Adam
Batch size	1024
Training split ratio	0.8 training, 0.2 testing
Random seeds	0, 22, 42, 123, 222, 367, 419, 579, 623, 746, 844, 918, 1023, 1344, 65536, 815149



```
==========================================================================================
Layer (type:depth-idx)                   Output Shape              Param #
==========================================================================================
├─Conv1d: 1-1                            [-1, 16, 78]              64
├─ReLU: 1-2                              [-1, 16, 78]              --
├─MaxPool1d: 1-3                         [-1, 16, 38]              --
├─Conv1d: 1-4                            [-1, 16, 38]              784
├─ReLU: 1-5                              [-1, 16, 38]              --
├─MaxPool1d: 1-6                         [-1, 16, 18]              --
├─Conv1d: 1-7                            [-1, 32, 18]              1,568
├─ReLU: 1-8                              [-1, 32, 18]              --
├─MaxPool1d: 1-9                         [-1, 32, 8]               --
├─AdaptiveAvgPool1d: 1-10                [-1, 32, 5]               --
├─Linear: 1-11                           [-1, 320]                 51,520
├─ReLU: 1-12                             [-1, 320]                 --
├─Dropout: 1-13                          [-1, 320]                 --
├─Linear: 1-14                           [-1, 640]                 205,440
├─ReLU: 1-15                             [-1, 640]                 --
├─Dropout: 1-16                          [-1, 640]                 --
├─Linear: 1-17                           [-1, 1280]                820,480
├─ReLU: 1-18                             [-1, 1280]                --
├─Dropout: 1-19                          [-1, 1280]                --
├─Linear: 1-20                           [-1, 1280]                1,639,680
├─ReLU: 1-21                             [-1, 1280]                --
├─Dropout: 1-22                          [-1, 1280]                --
├─Linear: 1-23                           [-1, 640]                 819,840
├─ReLU: 1-24                             [-1, 640]                 --
├─Dropout: 1-25                          [-1, 640]                 --
├─Linear: 1-26                           [-1, 320]                 205,120
├─ReLU: 1-27                             [-1, 320]                 --
├─Dropout: 1-28                          [-1, 320]                 --
├─Linear: 1-29                           [-1, 2]                   642
==========================================================================================
Total params: 3,745,138
Trainable params: 3,745,138
Non-trainable params: 0
Total mult-adds (M): 3.80
==========================================================================================
```

Figure 4: 1D AlexNet model architecture

4.5 Evaluation Metrics

In machine learning and pattern recognition, evaluation metrics serve as quantifiable measures to gauge model performance and effectiveness. These metrics assess and compare a model's performance on a specific task or problem. In the context of this research, we used the following metrics:

- Accuracy: Evaluates the accuracy of model predictions.
- Precision: Assess the ratio of true positive predictions to the total predicted positive samples.
- Recall: Assess the ratio of true positive predictions to the total true positive samples.
- F1 score: A comprehensive evaluation metric by considering both precision and recall.

These metrics will measure the model's performance in distinguishing between different classes. Table 4 is the definition of the confusion matrix in machine learning.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \tag{10}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{11}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{12}$$

$$\text{F1 score} = \frac{2 * Precision * Recall}{Precision + Recall} \tag{13}$$

Table 4: Confusion matrix

	Attack	Normal
Attack	TP (True Positive)	FP (False Positive)
Normal	FN (False Negative)	TN (True Negative)

4.6 Known DDoS Detection

For known DDoS detection, we utilized CICIDS2017 Wednesday dataset for the training model. Initially, we trained the 1D AlexNet model and visualized the 2-feature output from the 1D AlexNet module in feature space, as shown in Fig. 5. We observed that the training process made the distribution of the known classes more dispersed. In some cases, the distribution areas of known classes have overlapped with one another.

Therefore, we continued to modify 1D AlexNet several times to improve the result. We have tried to increase the number of convolutional layers of the 1D AlexNet. After numerous improvements, we achieved the desired outcomes. Fig. 6 shows that the result of our final model (Fig. 3) improves significantly compared to the initial model in terms of the distribution of known datasets.

Furthermore, we obtained excellent results as shown in Fig. 7, when evaluating known attacks by using the same CICIDS2017 Wednesday dataset. All evaluation metrics exceed 0.98.

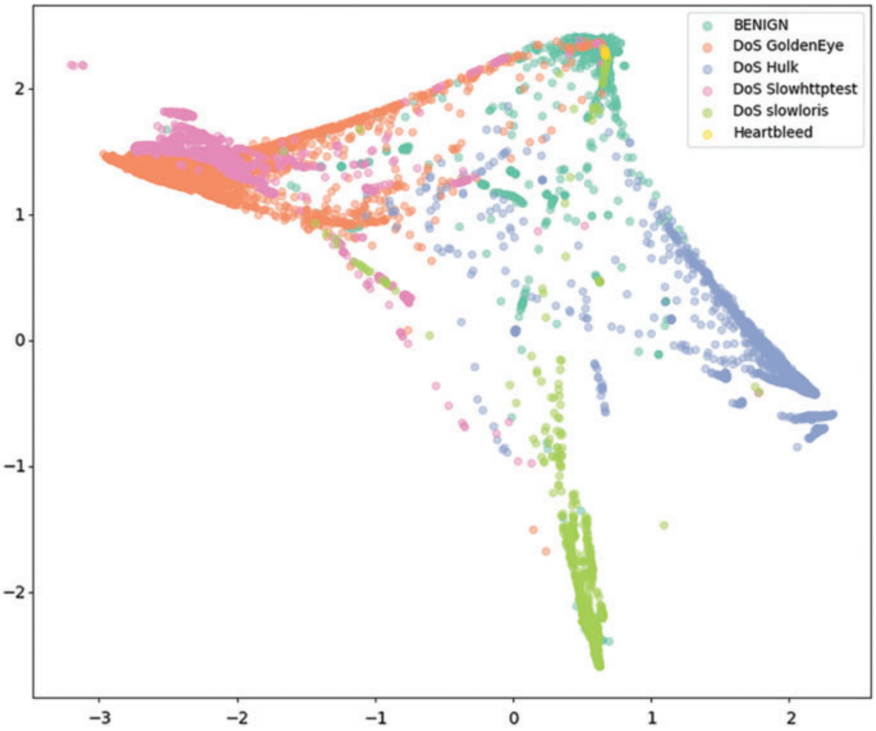


Figure 5: Unmodified 1D AlexNet

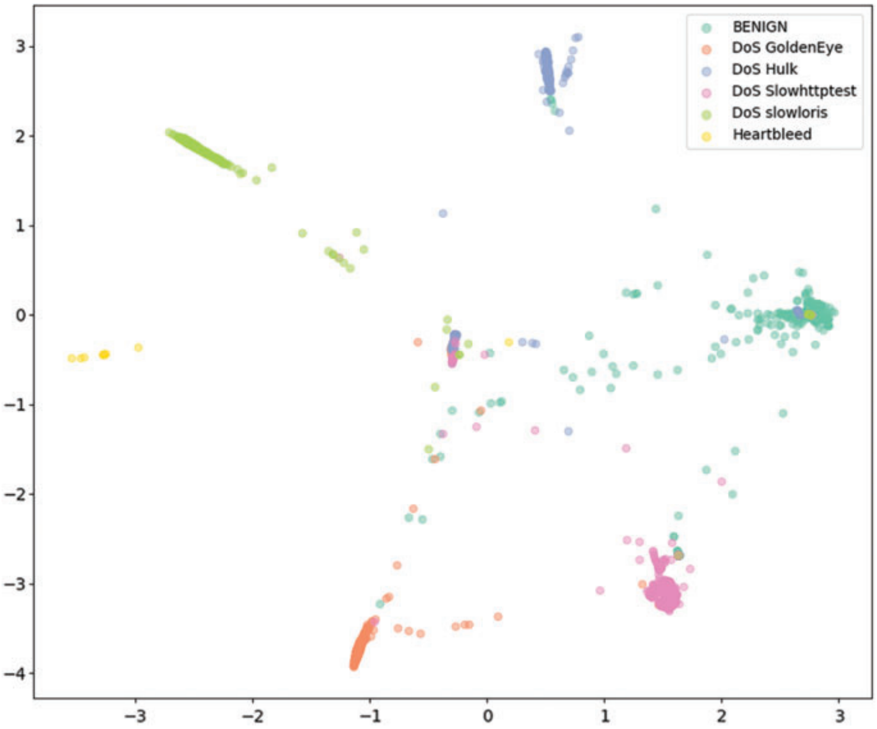
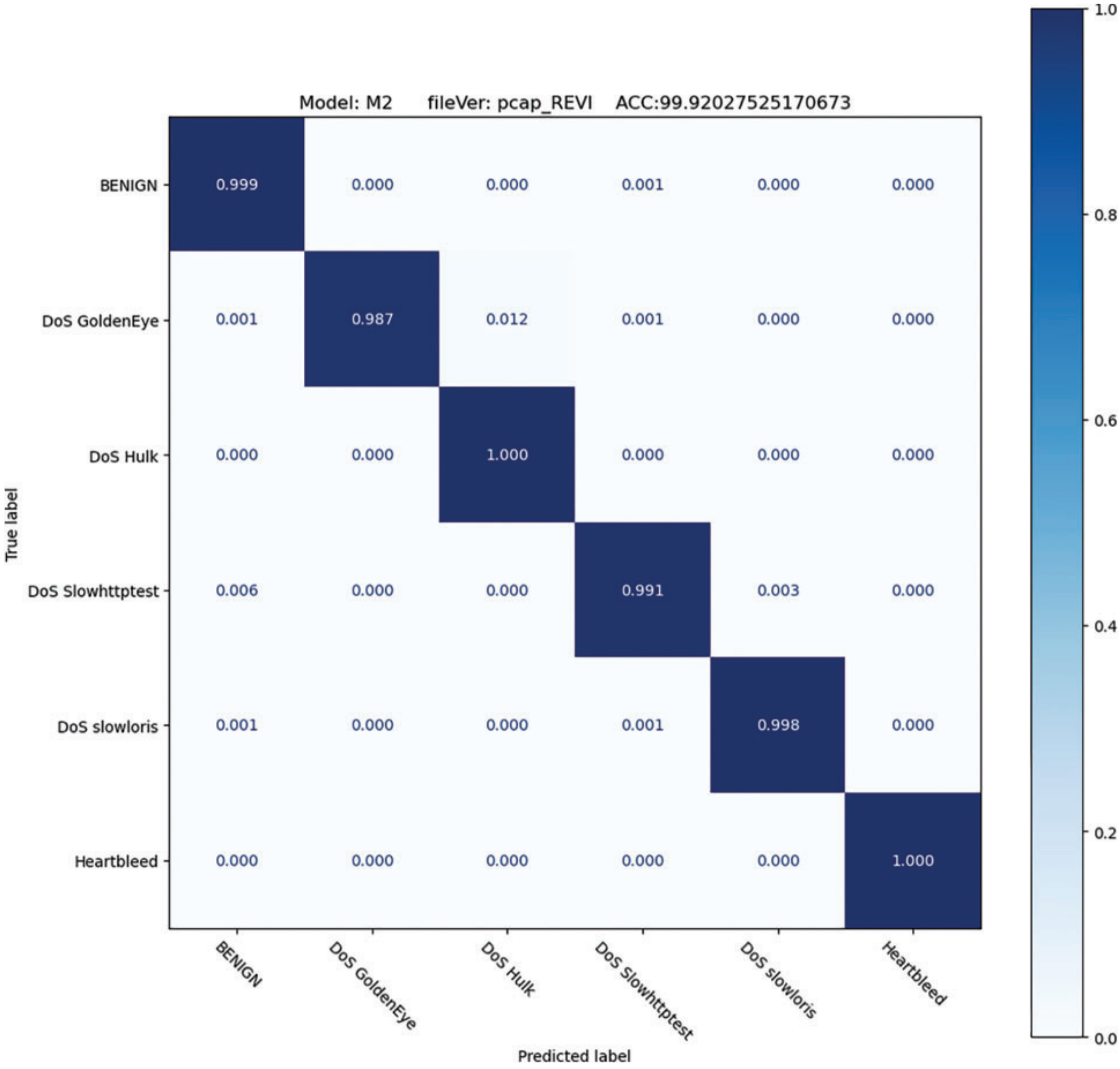


Figure 6: Final 1D AlexNet model with fully connected layer



	BENIGN	DoS GoldenEye	DoS Hulk	DoS Slowhttptest	DoS slowloris	Heartbleed
BENIGN	0.999	0.000	0.000	0.001	0.000	0.000
DoS GoldenEye	0.001	0.987	0.012	0.001	0.000	0.000
DoS Hulk	0.000	0.000	1.000	0.000	0.000	0.000
DoS Slowhttptest	0.006	0.000	0.000	0.991	0.003	0.000
DoS slowloris	0.001	0.000	0.000	0.001	0.998	0.000
Heartbleed	0.000	0.000	0.000	0.000	0.000	1.000

Figure 7: Known attack evaluation matrix

4.7 Unknown DDoS Detection

4.7.1 Unknown Attack Detection with 1D AlexNet

The 1D AlexNet model has shown good performance against known attacks. Next, we continued to evaluate the ability to defend against unknown attacks. Firstly, we used the CICIDS2017 Friday dataset to evaluate the trained model. Table 5 shows the results and correlation comparisons.

Table 5: Unknown DDoS detection performance for the CICIDS2017 dataset

Dataset	Accuracy	Precision	Recall	F1 score
CICIDS2017 Wednesday	0.9972	0.9942	0.9983	0.9962
CICIDS2017 Friday	0.7910	0.9925	0.6363	0.7755

When evaluating by CICIDS2017 Friday dataset, the accuracy is 0.7910 and other metrics are mostly at an average level. Because the CICIDS2017 Friday and CICIDS2017 Wednesday datasets are collected in the same environment. They have a certain similarity, especially in the BEGIGN traffic. However, the results show that the standalone model is not good enough to identify novel attacks.

Next, we used the CICDDoS2019 dataset to further evaluate the model. Table 6 shows the results and correlation comparison for the CICDDoS2019 dataset.

Table 6: Unknown DDoS detection performance for the CICDDoS2019 dataset

Dataset	Accuracy	Precision	Recall	F1 score
CICIDS2017 Wednesday	0.9972	0.9942	0.9983	0.9962
CICIDS2017 Friday	0.7910	0.9925	0.6363	0.7755
CICDDoS2019 DNS	0.0006	0.3795	4.75E-05	9.50E-05
CICDDoS2019 LDAP	0.0022	0.0462	9.49E-06	1.90E-05
CICDDoS2019 MSSQL	0.0004	0.3951	2.84E-05	5.68E-05
CICDDoS2019 NTP	0.0123	0.6402	0.0012	0.0025
CICDDoS2019 NetBIOS	0.0003	0.625	3.33E-05	6.66E-05
CICDDoS2019 Portmap	0.0236	0.1192	0.0001	0.0003
CICDDoS2019 SNMP	0.0002	0.5089	4.98E-05	9.96E-05
CICDDoS2019 SSDP	0.0004	0.775	0.0017	0.0035
CICDDoS2019 Syn	0.0095	0.775	0.0017	0.0035
CICDDoS2019 UDP	0.0009	0.7687	0.0002	0.0004

The results are really bad when evaluating the model by CICDDoS2019. Because the CICDDoS2019 and CICIDS2017 datasets are different. Even though they are collected by the same organization Canadian Institute of Cyber Security (CIC). They have different simulation environments and the collected features are not the same. The attack pattern of CICDDoS2019 is strange to the trained model. That fooled the model into thinking the novel attacks were regular accesses. Therefore, we need to combine the model with an Unknown DDoS Detecting module to enhance the system's capabilities.

4.7.2 Unknown Attack Detection Module

In this research, we calculated the Outlier Detection Rate (ODR) to determine the efficiency of the Unknown DDoS Detecting module. The formula of ODR is as follows:

$$ODR = \frac{N_{Outlier}}{N} \tag{14}$$

where $N_{Outlier}$ is the number of unknown samples that our system believes should be reviewed by network experts, and N is the total number of samples in the procedure.

The CICIDS2017 Friday and CICIDS2017 Wednesday are collected in the same environment and are quite similar. Therefore, the ODR of CICIDS2017 Friday is only 0.082. However, other CICDDoD2019 datasets have very high ODR of over 0.99. Table 7 shows that our Unknown DDoS Detecting module has very high performance when identifying outlier samples.

Table 7: The outcome of the Unknown DDoS detecting module

Dataset	ODR
CICIDS2017 Friday	0.0842
CICDDoS2019 DNS	0.9999
CICDDoS2019 LDAP	0.9998
CICDDoS2019 MSSQL	0.9999
CICDDoS2019 NTP	0.9987
CICDDoS2019 NetBIOS	0.9996
CICDDoS2019 Portmap	0.9983
CICDDoS2019 SNMP	0.9999
CICDDoS2019 SSDP	0.9999
CICDDoS2019 Syn	0.9990
CICDDoS2019 UDP	0.9999

4.7.3 Incremental Learning

After being processed by the Unknown DDoS Detecting module, suspicious samples will be analyzed and labeled by network experts. Next, new labeled data will be used for the incremental learning process. This process improves the machine learning model without the need to retrain it from scratch. The incremental learning ensures continuous operation of the system as well as full updates on new real-life cyber attack patterns. Table 8 shows the outcomes of the model after incremental learning.

Table 8: Our model outcomes post incremental learning

Dataset	Incremental learning	Accuracy	Precision	Recall	F1 score
CICIDS2017 Wednesday	*Before*	0.9972	0.9942	0.9983	0.9962
	After	0.9976	0.9944	0.9991	0.9968
CICIDS2017 Friday	*Before*	0.7910	0.9925	0.6363	0.7755
	After	0.9926	0.9985	0.9885	0.9934
CICDDoS2019 DNS	*Before*	0.0006	0.3795	4.75E-05	9.50E-05
	After	0.9999	0.9999	0.9999	0.9999
CICDDoS2019 LDAP	*Before*	0.0022	0.0462	9.49E-06	1.90E-05
	After	0.9998	0.9999	0.9998	0.9999

(Continued)

Table 8 (continued)

Dataset	Incremental learning	Accuracy	Precision	Recall	F1 score
CICDDoS2019 MSSQL	*Before*	0.0004	0.3951	2.84E-05	5.68E-05
	After	0.9999	0.9999	0.9999	0.9999
CICDDoS2019 NTP	*Before*	0.0123	0.6402	0.0012	0.0025
	After	0.9991	0.9996	0.9994	0.9995
CICDDoS2019 NetBIOS	*Before*	0.0003	0.625	3.33E-05	6.66E-05
	After	0.9999	0.9999	0.9999	0.9999
CICDDoS2019 Portmap	*Before*	0.0236	0.1192	0.0001	0.0003
	After	0.9965	0.9993	0.997	0.9982
CICDDoS2019 SNMP	*Before*	0.0002	0.5089	4.98E-05	9.96E-05
	After	0.9999	0.9999	0.9999	0.9999
CICDDoS2019 SSDP	*Before*	0.0004	0.775	0.0017	0.0035
	After	0.9998	0.9999	0.9999	0.9999
CICDDoS2019 Syn	*Before*	0.0095	0.775	0.0017	0.0035
	After	0.9995	0.9997	0.9997	0.9997
CICDDoS2019 UDP	*Before*	0.0009	0.7687	0.0002	0.0004
	After	0.9999	0.9999	0.9999	0.9999

After incremental learning, the model's performance has significantly improved. For the CICIDS2017 Friday dataset, despite the ODR rate being only 0.0842, it has led to an increase in accuracy of approximately 0.2. For the CICDDoS2019 dataset, the measured metrics exceeded expectations when all surpassed 0.98. This proves the module combined FCM and SLCPL is effective in distinguishing known and unknown traffic. Most of the samples determined as unknown traffic are strange to the system and can enhance the system's performance. Therefore, the system's capability to detect unknown attacks is guaranteed at the highest level.

4.8 Comparison of the Proposed Method with the Existing Works

We used a lot of recent research in detecting DDoS attacks for the comparison. Chosen algorithms include Deep Neural Network with Genetic Algorithms (2023) [28], Multilayer Perceptron (2023) [29], and Convolutional Neural Network featuring Geometrical Metric (2023) [34]. All algorithms were evaluated on the CICIDS2017 dataset for known attack detection. Table 9 shows the comparisions of our method with recent ML algorithms.

Table 9: Our method in the comparison with recent ML algorithms on CICIDS2017

Method	Accuracy	Precision	Recall
DNN-GA (2023)	0.9906	0.9896	0.9915
MLP (2023)	0.992	0.971	0.966
CNN-Geo (2023)	**0.9979**	**0.9962**	0.9944
Proposed method	0.9976	0.9944	**0.9991**

The performance metrics of our proposed method are slightly larger than DNN-GA and MLP. They have accuracy, precision, and recall of approximately 0.99. Compared with the CNN-Geo algorithm, the proposed method has similar performance with negligible differences.

Next, we continued to compare with other algorithms in detecting unknown attacks. The algorithms we chose to compare include GMM (2021) [21], DBSCAN with Random Forest (DBSCAN-RF) (2022) [27], DBSCAN with SVM (DBSCAN-SVM) (2022) [27], One-Dimensional Deep High-Resolution Network with One-Class SVM (1D-DHRNet-OCSVM) (2022) [30], and CNN featuring Geometrical Metric (CNN-Geo) (2023) [34]. All algorithms are trained on the CICIDS2017 dataset and evaluated on other datasets. The performance metrics of the overall system are listed in the Table 10.

Table 10: Our method in comparison with recent ML algorithms in unknown DDoS attack detection

Method	Accuracy	Precision	Recall
GMM (2021)	–	0.9700	0.95
DBSCAN-RF (2022)	0.148	0.998	0.145
DBSCAN-SVM (2022)	0.314	0.998	0.312
1D-DHRNet-OCSVM (2022)	0.992	0.999	0.991
CNN-Geo (2023)	0.996	0.997	0.996
Proposed method	**0.996**	**0.999**	**0.997**

Compared with DBSCAN-SVM and DBSCAN-RF methods, our method has much more outstanding performance metrics. Compared with GMM (2021), 1D-DHRNet-OCSVM (2022), and CNN-Geo (2023), our method has slightly larger metrics. Combining the two cases of known and unknown attack detection, our performance is equal to or more outstanding than other methods. This proves that our research has caught up and surpassed recent outstanding research.

4.9 Discussion

The validity of a study is a concern that we prioritize throughout our research. For internal validity, we are meticulous in applying methods, algorithms, and experimental procedures in the fields of machine learning and deep learning. We have used multiple random seeds, as well as dropout techniques to avoid overfitting, during both model training and evaluation. Regarding external validity, in this research, we utilized two main datasets, CICIDS2017 and CICDDoS2019. The validity of these datasets will significantly impact the applicability of our model in real-world scenarios. These are two well-known and standard datasets in the broader field of network attack detection, including specific DDoS attacks. All of these efforts are aimed at ensuring the reliability of our research.

However, new attack methods and their variants are continually evolving. Deploying an unknown attack detection module along with ongoing support from network experts and machine learning incremental learning techniques forms a robust combination that enhances the system's capabilities over time. While the defense of our system has demonstrated effectiveness against a variety of DDoS attacks, it is essential to recognize certain limitations. This is particularly evident when confronting Layer 7 (L7) DDoS attacks and the intricate strategies employed in adversarial scenarios.

As mentioned, our proposed model heavily relies on two primary datasets, CICIDS2017 and CICDDoS2019, focused predominantly on DDoS attacks at Layer 3 and Layer 4. This specialization in lower network layers may result in inadequacies in addressing the distinct characteristics of DDoS attacks at the L7 layer, the Application layer. Notably, L7 DDoS attacks pose a unique challenge as they exploit vulnerabilities within applications, services, or protocols, diverging from conventional approaches that target network infrastructure. Detection mechanisms may encounter challenges in discerning benign from harmful activities at this granular level. Techniques such as encryption-based intrusion and complex application-layer exploitation, while effective, may incur significant processing costs on lightweight systems, impacting overall performance and response times during high-intensity attacks.

Furthermore, our system has not been studied to face adversarial DDoS attacks, a major evolving threat. These attacks dynamically adjust in attack types, IP address manipulation, and various attack vectors, deliberately employed to complicate defense mechanisms.

In summary, minimizing L7 DDoS attacks and adversarial DDoS attacks requires a sophisticated and adaptive approach, while acknowledging the limitations mentioned above. Traditional mitigation strategies may not be sufficient, and research on advanced techniques needs to be conducted and implemented.

5 Conclusion and Future Work

Today, business service providers are striving to achieve stable service quality, which has become their important goal. However, some individuals view DDoS attacks as a way to generate revenue. DDoS attacks are becoming increasingly diverse and complex. Meanwhile, intrusion detection systems trained on limited datasets find it difficult to identify novel, unknown attacks. To solve this challenge, our research proposes a hybrid approach that combines the characteristics of supervised and unsupervised techniques. We have adopted the 1D AlexNet network as our main technique. We improved the 1D AlexNet network several times to achieve the desired model. Additionally, the combination of FCM and SCLPL was successful in identifying unknown attacks with very high efficiency. Then, we ask the help of network experts to label suspicious traffic and use reinforcement learning methods to enhance the model. As a result, the improved 1D AlexNet model achieved very high performance, with an accuracy of up to 99.8% for known attacks and 99.7% for unknown attacks. The proposed system has demonstrated strong defense capabilities against both known and unknown attacks.

Currently, the unknown detection method by using SCLPL and FCM is not only compatible with the 1D AlexNet model but can also be extended to other CNN-based models. This opens up research opportunities for the future. We plan to do more research with more complex CNN models as the core of the system to replace 1D AlexNet. Alongside that, we will try the integration of other unknown detection methods. The diversity of unknown detection methods ensures that our system is sensitive enough to detect novel attacks. All these methods aim to ensure the strong defense capabilities of the IDS system against the complex developments on the internet.

Acknowledgement: We would like to thank the National Science and Technology Council, Taiwan for funding this research. Additionally, we appreciate the financial support from the Institute of IoT Cybersecurity granted with ICP DAS Co., Ltd.

Funding Statement: This research was partly supported by the National Science and Technology Council, Taiwan with Grant Numbers 112-2221-E-992-045, 112-2221-E-992-057-MY3 and 112-2622-8-992-009-TD1.

Author Contributions: Conceptualization, C.-S. Shieh; methodology, T.-L. Nguyen and H. Kao; software, T.-L. Nguyen; validation, T.-T. Nguyen; visualization, H. Kao; writing—draft manuscript preparation, T.-L. Nguyen; writing—review and editing, T.-T. Nguyen and C.-S. Shieh; project funding, C.-S. Shieh and M.-F. Horng; project supervision, M.-F. Horng; project administration, M.-F. Horng. All authors have reviewed and approved the published version of the manuscript.

Availability of Data and Materials: Data supporting the reported results are available upon request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] "DDoS threat report for 2023 Q1," The Cloudflare Blog, Apr. 2023. Accessed: Nov. 02, 2023. [Online]. Available: http://blog.cloudflare.com/ddos-threat-report-2023-q1/

[2] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021. doi: 10.1109/ACCESS.2021.3056614.

[3] S. Ho, S. A. Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 14–25, 2021. doi: 10.1109/OJCS.2021.3050917.

[4] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics*, vol. 9, no. 6, pp. 916–937, 2020. doi: 10.3390/electronics9060916.

[5] C. Geng, S. Huang, and S. Chen, "Recent advances in open set recognition: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 10, pp. 3614–3631, Oct. 2021. doi: 10.1109/TPAMI.2020.2981604.

[6] Z. Xia, P. Wang, G. Dong, and H. Liu, "Spatial location constraint prototype loss for open set recognition," *Comput. Vis. Image Underst.*, vol. 229, pp. 103651, Mar. 2023. doi: 10.1016/j.cviu.2023.103651.

[7] J. C. Bezdek, R. Ehrlich, and W. Full, "FCM: The fuzzy c-means clustering algorithm," *Comput. Geosci.*, vol. 10, no. 2, pp. 2, Jan. 1984. doi: 10.1016/0098-3004(84)90020-7.

[8] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 6, May 2017. doi: 10.1145/3065386.

[9] R. Nishant, M. Kennedy, and J. Corbett, "Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda," *Int. J. Inf. Manag.*, vol. 53, pp. 102104, Aug. 2020. doi: 10.1016/j.ijinfomgt.2020.102104.

[10] J. Cheng, Y. Liu, X. Tang, V. Sheng, M. Li and J. Li, "DDoS attack detection via multi-scale convolutional neural network," *Comput. Mater. Contin.*, vol. 62, no. 3, pp. 3, 2020. doi: 10.32604/cmc.2020.06177.

[11] J. Chen, Y. Yang, K. Hu, H. Zheng, and Z. Wang, "DAD-MCNN: DDoS attack detection via multi-channel CNN," in *Proc. of the 2019 11th Int. Conf. Mach. Learn. Comput.*, New York, USA, Association for Computing Machinery, Feb. 2019, pp. 484–488. doi: 10.1145/3318299.3318329.

[12] S. Kiranyaz, O. Avci, O. Abdeljaber, T. Ince, M. Gabbouj and D. J. Inman, "1D convolutional neural networks and applications: A survey," *Mech. Syst. Signal Process.*, vol. 151, pp. 107398, Apr. 2021. doi: 10.1016/j.ymssp.2020.107398.

[13] E. U. H. Qazi, A. Almorjan, and T. Zia, "A one-dimensional convolutional neural network (1D-CNN) based deep learning system for network intrusion detection," *Appl. Sci.*, vol. 12, no. 16, pp. 16, Jan. 2022. doi: 10.3390/app12167986.

[14] H. Beitollahi, D. M. Sharif, and M. Fazeli, “Application layer DDoS attack detection using cuckoo search algorithm-trained radial basis function,” *IEEE Access*, vol. 10, pp. 63844–63854, 2022. doi: 10.1109/ACCESS.2022.3182818.

[15] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, “Intrusion detection systems using long short-term memory (LSTM),” *J. Big Data*, vol. 8, no. 1, pp. 1, May 2021. doi: 10.1186/s40537-021-00448-4.

[16] A. Bendale and T. E. Boult, “Towards open set deep networks,” in *2016 IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 1563–1572. doi: 10.1109/CVPR.2016.173.

[17] Z. Ge, S. Demyanov, Z. Chen, and R. Garnavi, “Generative openmax for multi-class open set classification,” arXiv:1707.07418., Jul. 24, 2017.

[18] R. Yoshihashi, W. Shao, R. Kawakami, S. You, M. Iida and T. Naemura, “Classification-reconstruction learning for open-set recognition,” *2019 IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 4011–4020. doi: 10.1109/CVPR.2019.00414.

[19] M. Ahmed, A. Naser Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016. doi: 10.1016/j.jnca.2015.11.016.

[20] J. Henrydoss, S. Cruz, E. M. Rudd, M. Gunther, and T. E. Boult, “Incremental open set intrusion recognition using extreme value machine,” in *2017 16th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Cancun, Mexico, Dec. 2017, pp. 1089–1093. doi: 10.1109/ICMLA.2017.000-3.

[21] R. Chapaneri and S. Shah, “Multi-level Gaussian mixture modeling for detection of malicious network traffic,” *J. Supercomput*, vol. 77, no. 5, pp. 5, May 2021. doi: 10.1007/s11227-020-03447-z.

[22] C. S. Shieh, W. W. Lin, T. T. Nguyen, C. H. Chen, M. F. Horng and D. Miu, “Detection of unknown DDoS attacks with deep learning and gaussian mixture model,” *Appl. Sci.*, vol. 11, no. 11, pp. 11, Jan. 2021. doi: 10.3390/app11115213.

[23] K. Yang, J. Zhang, Y. Xu, and J. Chao, “DDoS attacks detection with autoEncoder,” in *2020 IEEE/IFIP Netw. Oper. Manag. Symp.*, Apr. 2020, pp. 1–9. doi: 10.1109/NOMS47738.2020.9110372.

[24] Z. Lin, Y. Shi, and Z. Xue, “IDSGAN: Generative adversarial networks for attack generation against intrusion detection,” in *Advances in Knowledge Discovery and Data Mining:* Berlin, Heidelberg, Springer-Verlag, May 2022, pp. 79–91. doi: 10.1007/978-3-031-05981-0_7.

[25] R. Chauhan and S. Heydari, “Polymorphic adversarial DDoS attack on IDS using GAN,” in *2020 Int. Symp. Net., Comput. Commun. (ISNCC)*, Montreal, QC, Canada, Oct. 2020, pp. 1–6, Oct. 2020. doi: 10.1109/ISNCC49221.2020.9297264.

[26] B. S. Harish and S. V. Aruna kumar, “Anomaly based intrusion detection using modified fuzzy clustering,” *Int. J. Interact. Multimed. Artif. Intell.*, Jan. 2017. doi: 10.9781/ijimai.2017.05.002.

[27] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, “A hybrid machine learning approach for detecting unprecedented DDoS attacks,” *J. Supercomput*, vol. 78, no. 6, pp. 6, Apr. 2022. doi: 10.1007/s11227-021-04253-x.

[28] J. Zhao, M. Xu, Y. Chen, and G. Xu, “A DNN architecture generation method for DDoS detection via genetic alogrithm,” *Future Internet*, vol. 15, no. 4, pp. 4, Apr. 2023. doi: 10.3390/fi15040122.

[29] D. Mohammed Sharif, H. Beitollahi, and M. Fazeli, “Detection of application-Layer DDoS attacks produced by various freely accessible toolkits using machine learning,” *IEEE Access*, vol. 11, pp. 51810–51819, 2023. doi: 10.1109/ACCESS.2023.3280122.

[30] C. S. Shieh, T. T. Nguyen, C. Y. Chen, and M. F. Horng, “Detection of unknown DDoS attack using reconstruct error and one-class SVM featuring stochastic gradient descent,” *Mathematics*, vol. 11, no. 1, pp. 1, Jan. 2023. doi: 10.3390/math11010108.

[31] H. M. Yang, X. Y. Zhang, F. Yin, and C. L. Liu, “Robust classification with convolutional prototype learning,” in *2018 IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 3474–3482. doi: 10.1109/CVPR.2018.00366.

[32] U. O. N. Brunswick, “Intrusion Detection Evaluation Dataset (CIC-IDS2017),” Accessed: Nov. 02, 2023. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[33] U. O. N. Brunswick, “DDoS Evaluation Dataset (CIC-DDoS2019),” Accessed: Nov. 02, 2023. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html

[34] C. S. Shieh, T. T. Nguyen, and M. F. Horng, “Detection of unknown DDoS attack using convolutional neural networks featuring geometrical metric,” *Mathematics*, vol. 11, no. 9, pp. 9, Jan. 2023. doi: 10.3390/math11092145.