International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
Impact Factor (RJIF): 5.64
Journal's Website
IJCCN 2025; 6(2): 16-25
Received: 11-06-2025
Accepted: 13-07-2025

Chandra Sekhar Sanaboina
Professor, Department of CSE, UCEK, JNTU Kakinada, Andhra Pradesh, India

A Ramya
PG Student, Department of CSE, UCEK, JNTU Kakinada, Andhra Pradesh, India

Corresponding Author:
Chandra Sekhar Sanaboina
Professor, Department of CSE, UCEK, JNTU Kakinada, Andhra Pradesh, India

Enhanced DDoS detection using cnn1d with reciprocal points learning and attention mechanism

Chandra Sekhar Sanaboina and A Ramya

DOI: https://doi.org/10.33545/27075923.2025.v6.i2a.98

Abstract
With the emergence of complex Distributed Denial-of-Service attacks, conventional Intrusion Detection Systems fail to identify novel never-before seen attacks. This project introduces a better model of detection with the assistance of Open-Set Recognition with Reciprocal Points Learning and again enhanced using Attention mechanism. The CNN1D-RPL model is used by the baseline system to accurately detect known and unknown threats based on Euclidean distance mapping in feature space. The extended proposed system extends this further with the addition of an Attention layer to enable the model to dynamically pay attention to salient features, leading to enhanced detection performance. Tested on CICIDS2017 datasets, the extended system performed better than the baseline method, with an accuracy of 99.95%, confirming the fact that it is appropriate for detection of unknown DDoS activity. This combined architecture offers efficient feature extraction, intelligent filtering, and adaptability with incremental learning, and is therefore a valuable tool for real-world cybersecurity applications.

Keywords: DDoS Detection, RPL, CNN1D, Attention Mechanism, Unknown Attack Detection, Deep Learning

1. Introduction
The internet stands at the forefront of the very fabric of the being in the globalized world today, which makes communication, commerce, education, healthcare, entertainment, and many others possible. As the appetite for online services continues to increase, so too have the sophistication and extent of cyber risks. Of them, DDoS attacks are currently one of the most widespread and paralyzing forms of cyberattacks organizations are exposed to worldwide. The intention of such an attack is to overwhelm the target server, network, or service with tremendous volumes of spurious traffic so that it becomes inaccessible to valid users. The effect can be cataclysmic, from service downtime, financial loss, to reputational damage. The most ominous aspect of DDoS attacks is that they keep evolving. The attackers simply discover new ways of evading traditional defenses, and too many current IDS are operating on a "closed-set" assumption that is trained on known attack patterns alone. Strong at the task of reacting to known threats, these systems are not generally architected to react to newly unknown (unknown) threats, leaving organizations open to being attacked. Actually, that is a critical flaw, in that an attacker will simply alter existing threats or generate new threats entirely. To assist in alleviating this issue, there are more flexible solutions that can identify known and unknown attacks. That is where Open-Set Recognition enters the picture. OSR enables models not only to identify known threats but also to identify when an input is not one of the learned classes essentially, the machine which can say, "The study don't know this, but it's suspicious." This is crucial in the cybersecurity domain, as new types of threats emerge on a regular basis.
One of the encouraging OSR approaches is Reciprocal Points Learning (RPL), a distance-based technique that predicts an incoming data point (e.g., network traffic sample) to be far from known data clusters in feature space. If far, the model labels it as possibly unknown. This technique discriminates well from unknown and known samples without being pre-disrupted by unknown attacks. For instance, if one've never seen anything but dogs and cats, one may confuse a rabbit with a cat. But with OSR and RPL concepts, one can say, "This is not a dog or a cat it could be something new." And in cyber security, this is utilized to distinguish known bad traffic from new anomalies. Although deep learning-based models such as Convolutional Neural Networks excel in learning to automatically extract features

and pattern-recognize in complex data such as network traffic logs, they remain incomplete on unknown attacks without the infusion of OSR and RPL. The second enrichment comes from attention mechanisms, which simulate the human capacity to focus on the most salient information and pay less attention to details. In big, feature-rich data sets, attention layers allow models to filter out noise and focus on key features, enhancing detection accuracy.

Real-world DDoS detection systems also have to keep themselves updated. Incremental learning allows models to learn from novel data without having to re-start, without forgetting knowledge already acquired like a working professional learning at work without forgetting know-how already known. The efficacy of such systems is tested with benchmark dataset like CICIDS2017. Such datasets include diverse benign and malicious traffic samples, which enable researchers to train on known attacks and test on unknown attacks to gauge generalization ability. Testing is not just accuracy-based but precision (accuracy of detected attacks), recall (number of actual attacks found), and F1-score (precision-recall trade-off). As cyberattacks grow larger in size and more complex in nature, intelligent, adaptive, and power-frugal detection methodologies are the future. To eliminate this constraint, the OSR and RPL methods enable detection of novel threats without pre-training as opposed to closed-set models. Along with the application of attention mechanisms and incremental learning applications, they serve as a basis for lean cyber security solutions that provide confidentiality (e.g. data protection), availability of services and reactivity to ever-changing threats, in real-time cost-effective manner.

2. Literature Review

This study introduces a classification and prediction framework that integrates machine learning with advanced feature engineering techniques to effectively identify and forecast DDoS attacks. The framework demonstrates robustness through its scalability, adaptability to varying traffic conditions, and consistently high detection performance across heterogeneous network environments [1]. An optimized radial basis function neural network weights and centers using a cuckoo search algorithm for better convergence rate and lower classification error, particularly in heavy-traffic and noisy data environments [2]. A profound CNN ensemble model for SDN learned several CNNs from various traffic viewpoints, combining their prediction to enhance robustness and decrease overfitting, achieving greater accuracy and fewer false positives than individual CNN models [3]. An SDN online learning ensemble model handled streaming traffic in real-time, allowing for adaptive updates without full retraining, drastically reducing detection delay while retaining accuracy in dynamic attack situations [4]. One evolutionary support vector machine (SVM) technique employed evolutionary computation to perform kernel and regularization parameters automatically, improving model generalization, convergence, and accuracy [5].

An unsupervised generative adversarial network (GAN)-based system generated synthetic traffic to improve boundary learning for detecting zero-day attacks and performed well on recognizing new malicious patterns without labels beforehand [6]. One of the large-scale detection methods based on big data employing Apache Spark processed national-level, high-speed traffic streams in real time with negligible latency, providing scalability, fault tolerance, and compatibility with monitoring tools [7]. DDoS detection of unknown attacks was addressed through fuzzy C-means clustering with spatial constraints, enhancing cluster quality and distinguishing normal from abnormal traffic even when in disguise [8]. An SDN-optimized AI model with heuristic algorithms attained a high detection rate with low resource utilization, which is ideal for real-time large-scale deployment [9]. A filter-and-wrapper ensemble classifier-based hybrid attribute reduction method eliminated redundant attributes, enhancing classification accuracy as well as robustness to overfitting [10].

Hybrid architecture built upon deep learning that incorporated convolutional neural networks and long short-term memory networks both identified spatial and temporal patterns in network traffic, reducing false positives and enhancing responsiveness to changing attack tactics [11].Gradient boosting-based cloud detection scaled nicely to large volumes of DDoS traffic while providing low-latency decision-making in dynamic environments [12]. An unsupervised clustering method that did not use labeled data identified zero-day attacks efficiently but needed accurate parameter tuning of clustering to achieve stable performance across data sets [13]. A mutual information and recursive feature elimination hybrid feature selection boosted classification performance and minimized computation times in high-dimensional data sets [14]. Blockchain-derived verifications schemes provided immutable and decentralized endorsement of DDoS warnings to enhance trust in cooperative security networks [15].

Reinforcement learning-based traffic management in SDN learned dynamic optimal filtering rules by itself, enhancing mitigation success rates and resource utilization over time [16]. Hyper parameters of DDoS detection models were optimized through genetic algorithms, with greater detection accuracy and minimized training times, making them applicable to large-scale deployment environments [17]. A fog computing-based system made traffic analysis more proximate to IoT data sources, reducing latency and bandwidth utilization while enhancing responsiveness [18]. Transfer learning utilized pre-trained deep models for DDoS detection, allowing rapid adaptation and sustaining high accuracy with little labeled data [19]. A decision tree, random forest, and gradient boosting ensemble improved resilience to multi-vector DDoS attacks while minimizing false positives [20].

Deep reinforcement learning-based defense systems learned real-time countermeasures through interaction with the network environment, improving mitigation efficiency markedly [21]. IoT-targeted intrusion detection models with lightweight machine learning models achieved high accuracy under tight resource constraints, facilitating deployment in massive IoT environments [22]. Federated learning-based approach enabled organizations to jointly train DDoS classification models without exposing raw sensitive data, ensuring privacy alongside collective intelligence [23]. Adaptive thresholding adjusted detection parameters real-time based on normal traffic patterns, enhancing reaction to abrupt spikes at the expense of fewer false alarms [24]. A composite model employing deep auto encoders for high-level feature extraction and SVMs for classification attained high detection accuracy with effective performance [25].

3. Proposed Approach

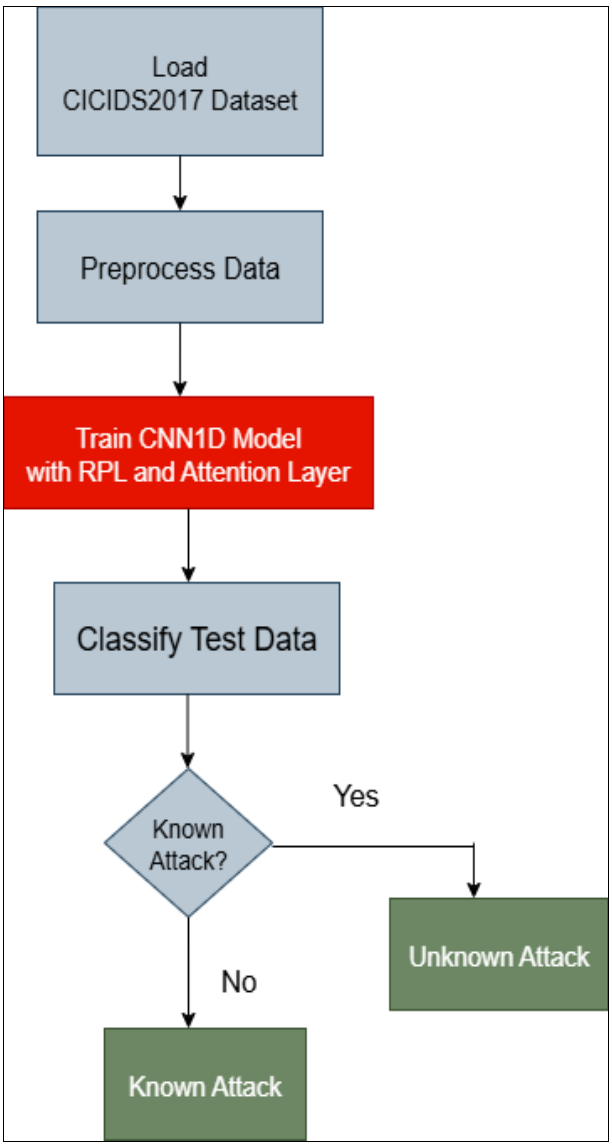

Fig 1: Workflow of the Proposed System

Fig 1 displays the process of the proposed system to identify and distinguish between known and unknown Distributed Denial of Service attacks from the CICIDS2017 dataset. The overall framework consists of CNN1D with Reciprocal Points Learning (RPL) and an Attention process to enhance open-set recognition and make the system more capable of generalizing for unseen attacks.The pipeline is segregated into major steps: loading the dataset, preprocessing, model training, and open-set detection classification.

The CICIDS2017 dataset is first loaded, with Wednesday and Friday traffic patterns employed to simulate a combination of benign and attack instances. The data is then subject to rigorous preprocessing, including missing value handling, feature encoding, and normalization, followed by the splitting of data into a training subset and a test subset. Training is performed using a customized CNN1D model that learns temporal and spatial representations of the network traffic. For class discriminability optimization, a Reciprocal Points Learning (RPL) module computes each sample's distance from the centers of classes, facilitating better separation between unknown and known attack samples.

Further, an Attention layer is incorporated in the CNN1D-RPL architecture to highlight important input features. This framework dynamically weights features such that the model concentrates on significant patterns connected with various attack classes. At classification, outputs are run through an open-set recognition test, which identifies if a sample pertains to a recognized class or is an unseen attack. Decisions follow from learned distance thresholds in RPL, with samples outside recognized areas being classified as unknown attacks. Such a design allows the system to accurately detect well-known attacks and identify new DDoS behaviors, which makes the intrusion detection system stronger and more reliable.

3.1 Dataset

The CICIDS2017 dataset, created by the CIC, is realistic and labeled benchmark dataset commonly applied to research in network intrusion detection. The dataset mimics normal and attack traffic in a typical enterprise network environment from real human behavior and common attack configurations. The dataset was captured over five days, with each day subjected to a varying type of attack. Network traffic was captured and analyzed with the CICFlowMeter tool that derives 80+ flow-based features like flow duration, total forward/backward packets, packet size average, inter-arrival times, and header flags. These features embody both time-based and statistical properties of traffic, and thus the dataset is ideally suited for machine learning and deep learning-based solutions in cybersecurity.

This research makes use of the CICIDS2017 dataset, focusing on the Wednesday and Friday traffic data.The Wednesday data have 692,703 records, which include normal traffic and other types of DoS attacks such as DoS Hulk, DoS GoldenEye, DoS Slowloris, and DoS Slowhttptest. Friday data have 190,911 records, which include a mix of benign traffic, Botnet traffic, and DDoS attacks. Following preprocessing, there were 79 numeric features to train the model, e.g., important features like Flow Duration, Fwd Packet Length Max, Bwd Packet Length Mean, Flow IAT Std, Fwd IAT Min, Bwd PSH Flags, and Average Packet Size. Non-numeric and non-pivotal columns (e.g., Timestamp, Label text, Flow ID) were removed as they are not applicable to the study. This feature-cleaned and feature-selected dataset was then used to train a deep hybrid detection model incorporating CNN1D, Reciprocal Points Learning (RPL), and attention mechanisms to detect known and unknown DDoS threats.

3.2 Data Collection and Pre-processing

The experiment starts with the acquisition of labeled network traffic records from benchmark corpora in order to have a representative set of benign and malicious patterns. The Wednesday dataset from CICIDS2017 is used to model known traffic and normal attacks for training purposes, while the Friday dataset is left for testing the capacity of the model to recognize unknown attacks. Such partitioning gives a realistic open-set recognition environment, where the model is subjected to novel, unseen types of attacks at evaluation.

Before training models, raw data undergo various preprocessing steps to enhance data quality and compatibility with deep learning and machine learning algorithms. Missing and incomplete values are either discarded or filled using methods to prevent biased learning of models. Categorical attack type and normal traffic labels

are converted into numeric labels through label encoding so the algorithms can learn them as distinct classes. Normalization enters to prevent scale differences between features scaling all numeric values to a uniform range, typically 0 to 1enabling faster training and more stable convergence.

Additional preprocessing can include feature elimination or dimension reduction to remove redundant features and retain only informative features. Not only does this speed up computation, but also overfitting is reduced by removing unnecessary noise. The data are shuffled randomly to avoid order bias and then split into a training subset (80%) and a test subset (20%) with identical class distribution in the two subsets. The training subset is used to adjust model parameters by fine-tuning, and the test subset is set aside for use only in unbiased performance estimation. This properly organized data preprocessing chain gives the model pure, uniform, and realistic input lending a solid basis for precise and trustworthy detection of DDoS attacks both in known and unknown situations.

3.3 Feature Extraction with CNN1D

A one-dimensional Convolutional Neural Network learns patterns in space and time from traffic patterns. The CNN1D architecture is made of several convolutional layers followed by Parametric Rectified Linear Unit activation and max-pooling layers. These assist in learning meaningful patterns in network flows that show probable DDoS activity. PReLU is used in place of the standard ReLU since it has a learnable parameter, offering greater flexibility in learning features without introducing the higher risk of vanishing gradients. The feature maps from the CNN layer are flattened and fed into a dense (fully connected) layer that maps the learned representations into fixed-size feature vectors.

3.4 Integration of Reciprocal Points Learning

For unknown attack identification, the model uses Reciprocal Points Learning (RPL), a distance-based approach. During training, RPL calculates Euclidean distances between feature vectors and known class centers. Learning these distances allows the model to ascertain how far an input is from recognized categories. During testing, if a feature is distant from all recognized class centers, it is classified as "unknown." This open-set feature allows the system to identify and isolate new types of attacks outside the training set, improving overall robustness and usability in real-world applications.

3.5 Attention Mechanism for Enhanced Learning

To increase precision and focus of the CNN-RPL architecture, an Attention mechanism is incorporated into the improved model. The Attention layer places dynamic weights on input features, allowing the network to pay greater attention to key information such as IP headers, traffic rate, or packet sizewhile ignoring redundant information. This mechanism mimics human decision-making, enhancing the ability of the model to detect faint patterns that are indicative of cyberattacks. Attention makes relevant features contribute more to the prediction, improving detection accuracy and removing false positives.

3.6 Open-Set Recognition and Classification

OSR is the theoretical framework upon which the CNNRPL models work It provides for the possibility that at test time, if a traffic pattern is not in one of the identified classes the model does not demandclassification but marks it as "unknown." This feature is critical in dynamic environments where attackers continually introduce new traffic signatures. The unknown samples can then be examined, annotated by security analysts, and incrementally used to retrain the model making it adaptive in the long term without complete retraining.

3.7 Validation Metrics

Standard metrics that are frequently used in classification tasks are used to assess the model's performance. Graphical results such as ROC curves, accuracy/loss plot, and comparison plot are used to view and compare the system performance in identifying known and unknown attacks. The metrics are computed for base and extended models to identify the effect introduced by the Attention mechanism.

4. Results and Discussion

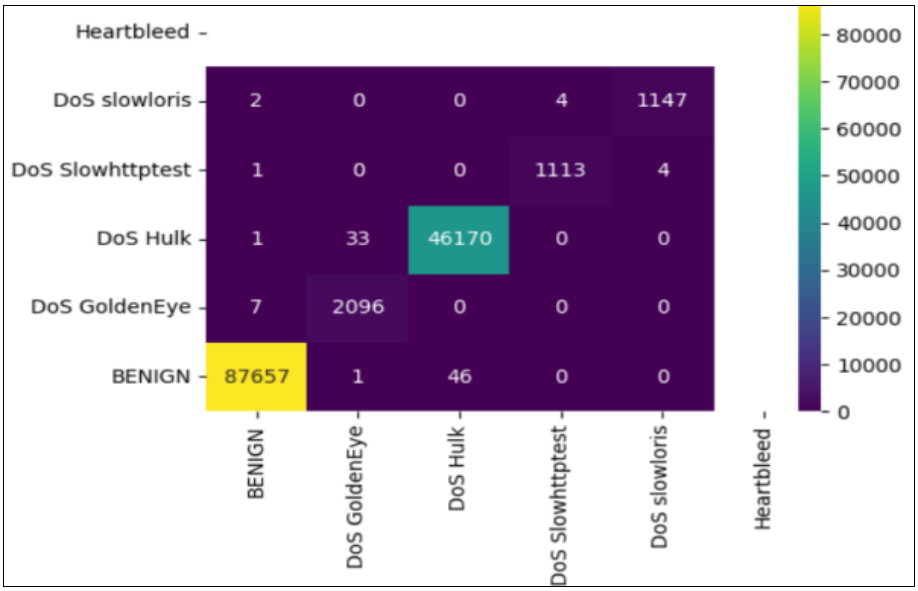

Fig 2: Confusion Matrix for Known Attacks Using CNN1D-RPL Model

With a remarkable accuracy of almost 99.93%, the model is proven to be able to clearly differentiate between various types of categories such as different types of attacks and benign behaviors. The precision rate, at 0.9952, indicates a very low rate of false positives, which means predicted attacks are virtually always true attacks. Recall is at 0.9971, and this is a very high rate of sensitivity with a high ability to identify almost all true positive instances correctly. The F-score at 0.9962 also affirms the well-balanced and consistent behavior, substantiating that the model is well-able to balance both precision and recall. All these metrics, as presented in Fig 2, show in aggregate that the introduced CNN1D-RPL model is extremely efficient in facilitating correct open-set recognition, even under highly complex or dynamic network conditions, to make it a proper candidate for use in advanced intrusion detection systems.

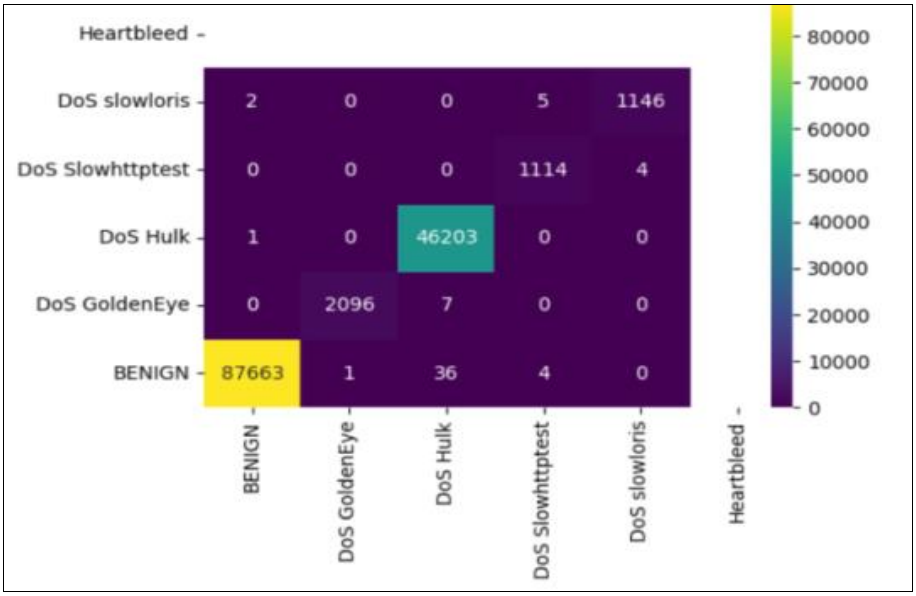

Fig 3: Confusion Matrix for Known Attacks Using CNN1D-RPL-Attention Model

The CNN1D-RPL-Attention Extension model, which was trained from audio data on NLP event features, achieves an accuracy of 99.96%, precision of 0.9974, recall of 0.9973, and F-score of 0.9974. With the hybrid use of CNN layers, RPL, and attention, the model exhibits strong classification performance with low false positives and high true positives. The confusion matrix Fig 3 exemplifies its effectiveness in correctly classifying known attack forms as well as benign events.

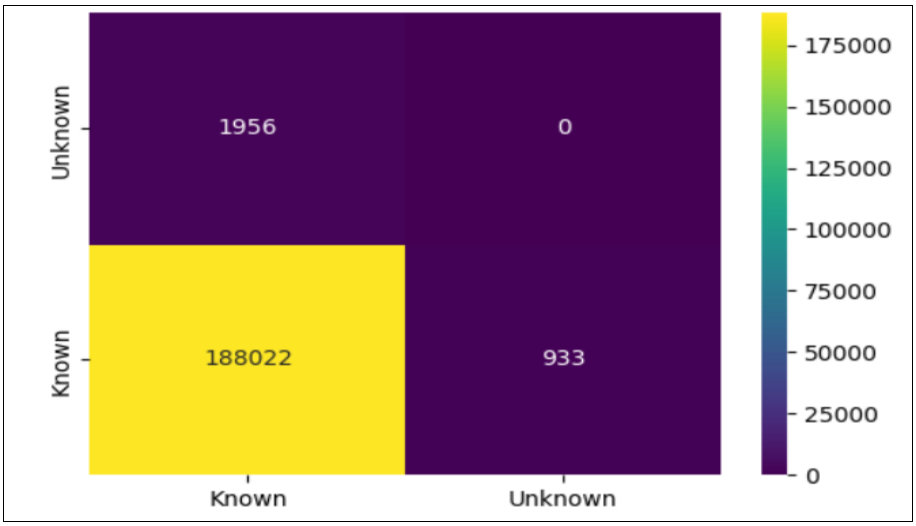

Fig 4: Confusion Matrix on Unknown Data Using CNN1D-RPL

Testing the suggested CNN1D-RPL model on an unseen dataset yields a satisfactory accuracy of around 98.49%. The confusion matrix gives additional insight into the discrimination capability of the model; a wide majority of the instances are rightly classified as "Known," and the "Unknown" samples are well detected with comparatively fewer misclassifications. The diagonal entries validate high levels of accurate prediction for both classes, while values away from the diagonal misclassifications are small. This performance, Fig 4, highlights the strength of the model in separating familiar patterns from truly novel inputs, exhibiting performance suitable for use cases needing stable identification of unknown or out-of-distribution data. These outcomes are especially critical in practical situations, where the occurrence of unexpected data is inevitable and model flexibility is essential.

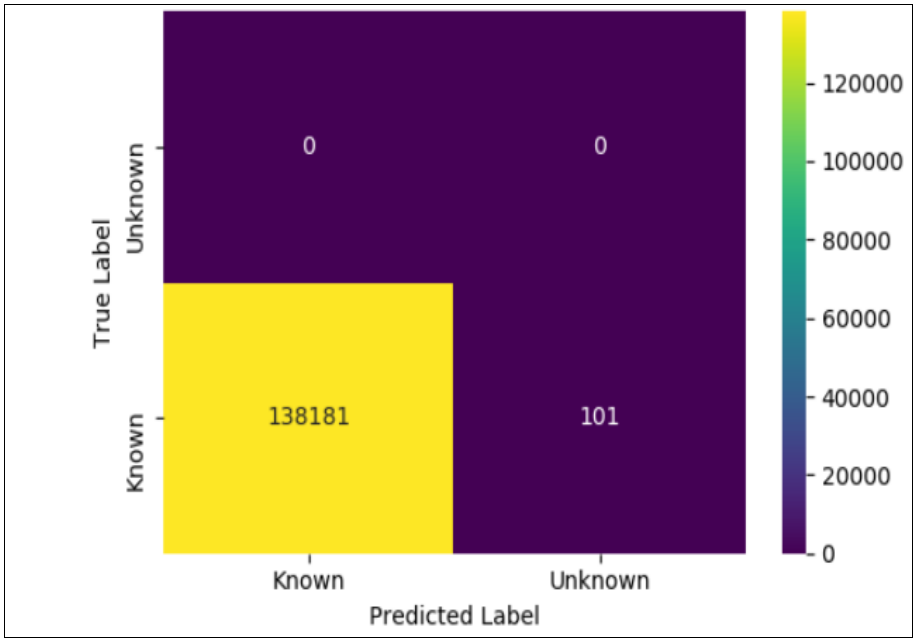

Fig 5: Confusion Matrix on Unknown Data Using CNN1D-RPL+Attention

The outcomes presented in Fig 5 demonstrate the performance of the "Extension CNN1D-RPL+Attention" model on a new dataset, to classify between "Known" and "Unknown" instances using prediction confidence. The model delivered a remarkably high accuracy of 0.9993. In the confusion matrix, among 138,282 test instances, it correctly labeled 138,181 as "Known" and mislabeled just 101 as "Unknown." There were no actual "Unknown" instances, as shown by zero values in the respective row. This shows the model's high capability to identify known ones and its consistency under the enforced 0.90 confidence threshold.

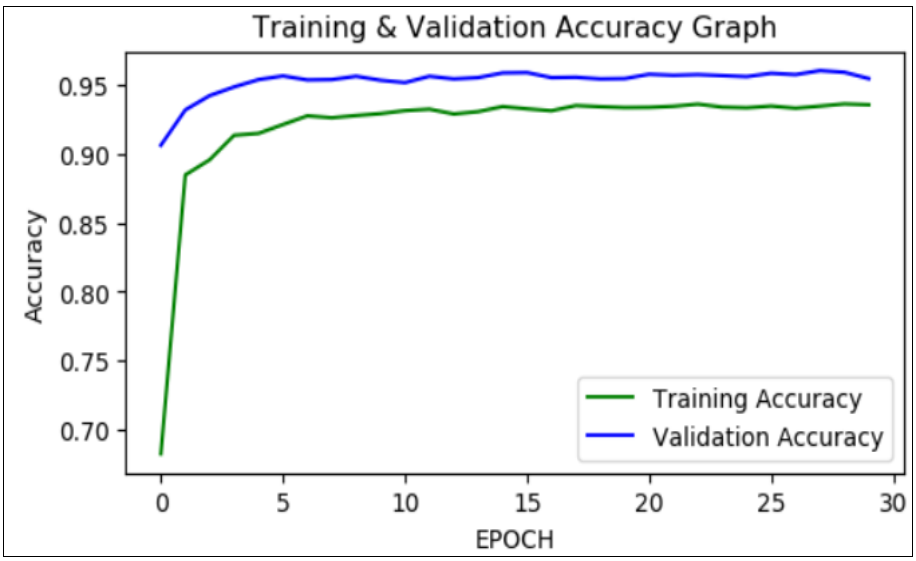

Fig 6: Training and validation accuracy curve for CNN1D+RPL model.

The trend in accuracy seen in the graph shows how the performance of the neural network model becomes better as training progresses. Both training and validation accuracy plots show a steep initial rise, which signifies the high rate of learning at the initial epochs. These curves start leveling off as training progresses, which means that the model is approaching the peak performance level. Validation accuracy is always high and tracks training accuracy closely, showing that the model has good generalization to new data. This steady performance on both data sets is evidence of good learning with little overfitting, and the model is stable for real-world classification tasks. Fig 6 illustrates the progression in accuracy over epochs, which verifies that the model has stable and consistent learning behavior.

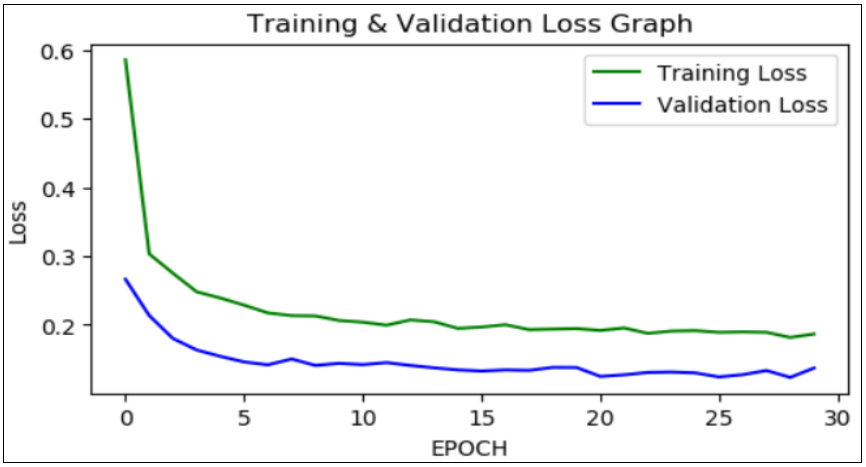

Fig 7: Training and Validation Loss Curve for CNN1D+RPL model

A consistent drop in both the training and validation loss across consecutive epochs illustrates the performance improvement of the model and effective learning process. The falling loss values with the passing of each epoch indicate the model's capacity for capturing underlying trends in data more accurately, increasingly minimizing prediction errors. The final intersection of the two loss curves at smaller values reflects an optimal process of optimization, with the model parameters well adjusted without indications of overfitting. This close correspondence of training and validation loss shows excellent generalization capability, proving that the model not only works on the training set but also on novel examples. Fig 7 clearly shows the pattern of loss progression, demonstrating the model's performance and stability throughout training.

Table 1: Comparison of Classification Metrics for SVM, KNN, Proposed CNN1D-RPL, and CNN1D-RPL with Attention

Algorithm Name	Accuracy	Precision	Recall	F1 Score
SVM	98.30%	0.992434	0.918356	0.952698
KNN	99.20%	0.961503	0.944533	0.949158
Propose CNN1D-RPL	99.93%	0.995172	0.997145	0.996150
Extension CNN1D+RPL+Attention	99.95%	0.997413	0.997307	0.997358

Table 1 presents a comparison of algorithms for detecting DDoS, and it finds that legacy models such as SVM and KNN perform well but are outperformed by advanced deep learning models. Note that the Extension CNN1D+RPL+Attention model achieves the highest accuracy rate (99.95%) and F1 score (0.9974). This indicates that the use of attention mechanisms in Reciprocal Points Learning greatly improves the detection accuracy as well as precision-recall trade-off balance and is thus the best method among those experimented with for DDoS attack detection.

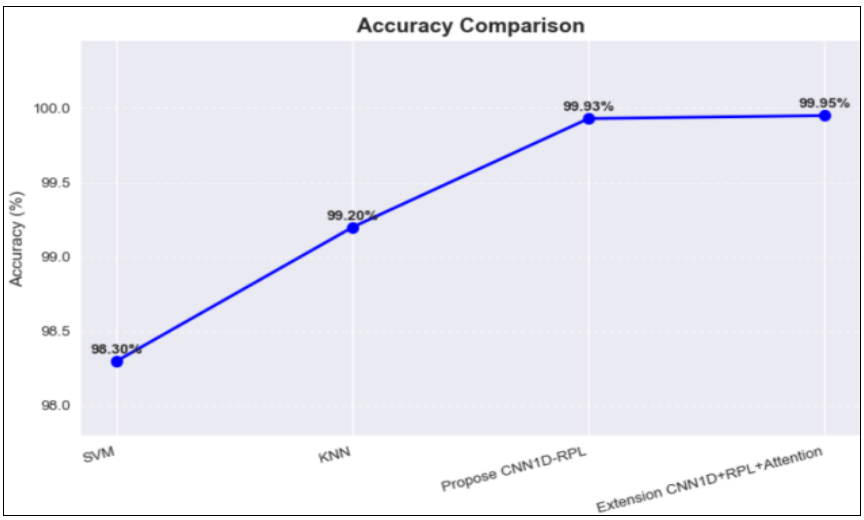

Fig 8: Comparison of Accuracy Using Different Methods

Figure 8 illustrates that performance enhances from conventional to sophisticated models SVM (98.30%) and KNN (99.20%) are overshadowed by the Proposed CNN1D-RPL (99.93%), with the highest accuracy being achieved by the CNN1D+RPL+Attention model (99.95%), as it proves that incorporating Reciprocal Points Learning with attention results in almost perfect DDoS detection.

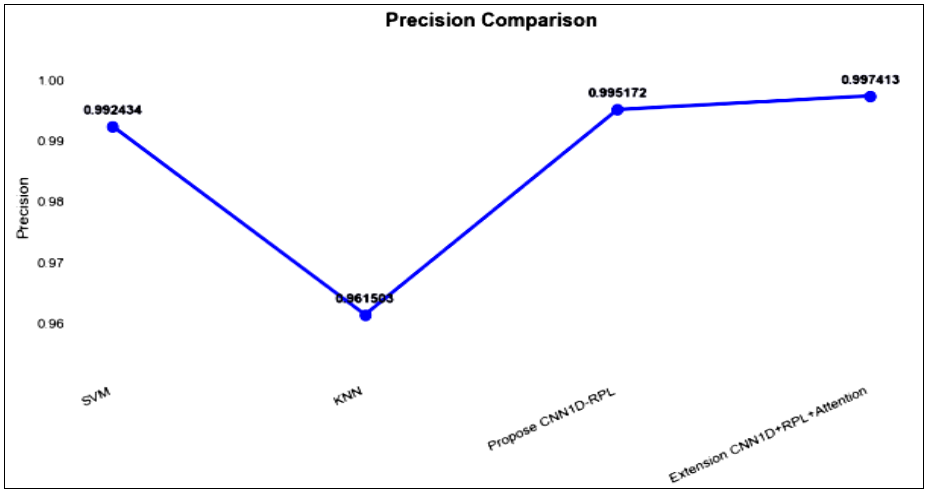

Fig 9: Comparison of Precision Using Different Methods

Fig 9 presents the precision comparison of SVM, KNN, Proposed CNN1D-RPL, and Extension CNN1D+RPL+Attention models. SVM posts a high precision of 0.992434, while KNN has a significant drop to 0.961503, which reflects greater false positives. The Proposed CNN1D-RPL increases precision to 0.995172, and attention-based extension increases it further to 0.997413. These findings emphasize that deep learning models, particularly those that incorporate Reciprocal Points Learning with the attention mechanism, show better ability in minimizing false positives and providing more accurate DDoS attack detection.

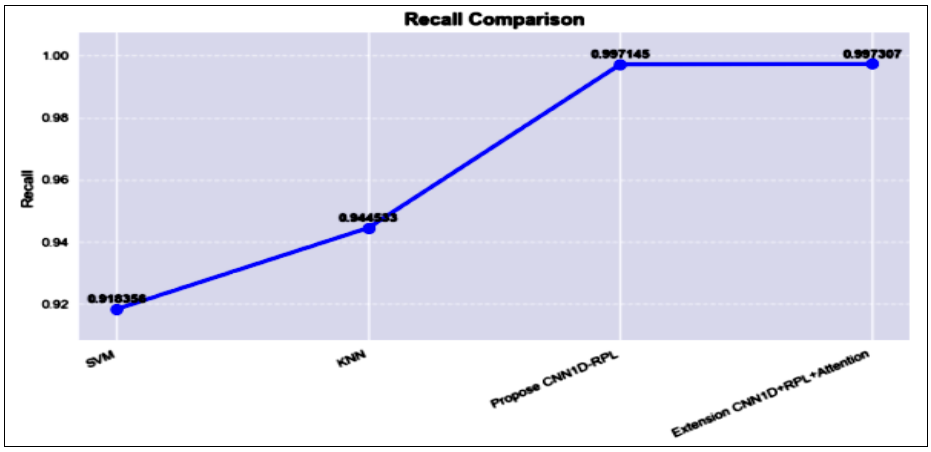

Fig 10: Comparison of Recall Using Different Methods

Fig 10 indicates that recall increases from SVM (0.9184) and KNN (0.9445) to the Proposed CNN1D-RPL (0.9971), with the Extension CNN1D+RPL+Attention having the highest (0.9973). This demonstrates that the integration of Reciprocal Points Learning together with attention significantly enhances the accurate identification of attacks and reduces false negatives in DDoS detection.

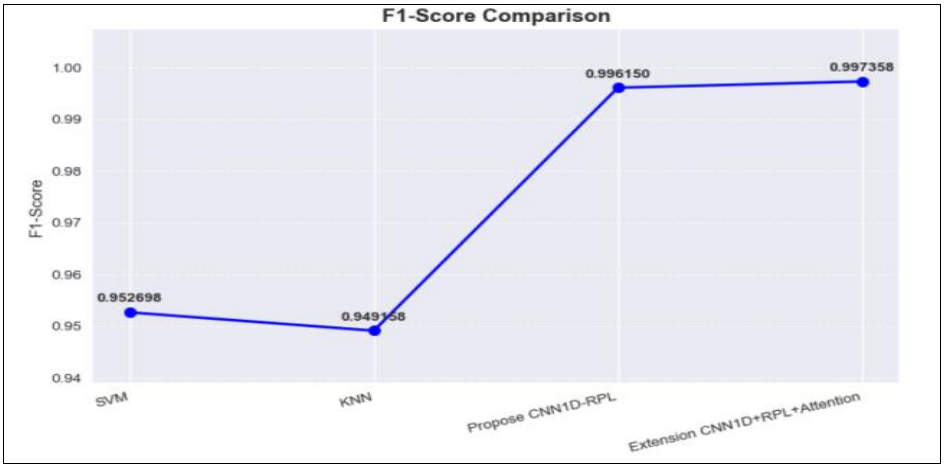

Fig 11: Comparison of F1 Score Using Different Methods

Fig 11 demonstrates that deep learning-based models perform better than classical ones in F1-score SVM (0.9527) and KNN (0.9492) are beaten by the Proposed CNN1D-RPL (0.9962), and further adding attention gets the highest result (0.9974), demonstrating superior precision-recall trade-off and robust DDoS detection.

5. Conclusion

This study offers a strong and reliable intrusion detection method that uses a mixed deep learning model to detect known and new threats. By integrating CNN1D with Reciprocal Points Learning and an Attention mechanism in the OSR framework, the system is able to overcome the drawback of traditional closed-set models.The suggested extension enables the model to concentrate on important features in the traffic flow, enhancing precision with fewer false positives. The utilization of benchmarking datasets such as CICIDS2017 confirms the model's high accuracy with a detection rate of over 99.95%. Additionally, the system is incremental learning-enabled, allowing ongoing improvement without complete retraining. These capabilities make it exceptionally appropriate for real-time cybersecurity environments, where threats are constantly changing. In all, the suggested approach presents a scalable, optimized, and intelligent means of network defense in today's modern networks, which can effectively counter new cyber threats with more precision and flexibility.

6. Future Work

In future work, the model can be extended by including network attributes like packet payloads and using additional datasets like CICDDoS2019 to improve generalizability. The project can also be extended even more by optimizing the model for real-time usage by reducing computational overhead and making it scalable for large networks. Other deep learning architectures such as LSTM, GRU, or Transformer-based architectures can also be included to further monitor temporal relationships. In parallel, state-of-the-art incremental learning techniques and adversarial defense strategies can be employed to enhance long-term robustness against continuously evolving attack patterns without losing long-term adaptability. Lastly, incorporation of explainable AI methods, edge or cloud-deployment, and integration with threat intelligence platforms would render the framework more applied, comprehensible, and efficient in real-world cybersecurity applications.

References

1. Ismail. A machine learning-based classification and prediction technique for DDoS attacks. IEEE Access. 2022;10:21443-21454.
2. Beitollahi H, Sharif DM, Fazeli M. Application layer DDoS attack detection using cuckoo search algorithm-trained radial basis function. IEEE Access. 2022;10:63844-63854.
3. Haider S, Akhunzada A, Mustafa T, Patel TB, Fernandez A. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. IEEE Access. 2020;8:53972-53983.
4. Alashhab AA, Zahid MS, Isyaku B, Elnour AA, Nagmeldin W, Abdelmaboud A. Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model. IEEE Access. 2024;12:51630-51649.
5. Sahoo KS, Tripathy BK, Naik K, Ramasubbareddy S, Balusamy B, Khari M. An evolutionary SVM model for DDoS attack detection in software defined networks. IEEE Access. 2020;8:132502-132513.
6. Brandão Lent DM, da Silva Ruffo VG, Carvalho LF, Lloret J, Rodrigues JJP, Lemes Proença M. An unsupervised generative adversarial network system to detect DDoS attacks in SDN. IEEE Access. 2024;12:70690-70706.
7. Awan MJ, Farooq U, Babar HMA, Yasin A, Nobanee H, Hussain M, Hakeem O, Zain AM. Real-time DDoS attack detection system using big data approach. Sustainability. 2021;13(19):10743.
8. Nguyen T-L, Kao H, Nguyen T-T, Horng M-F, Shieh C-S. Unknown DDoS attack detection with fuzzy C-means clustering and spatial location constraint prototype loss. Comput Mater Continua. 2024;78(2):2181-2205.
9. Al-Dunainawi Y, Al-Kaseem BR, Al-Raweshidy HS. Optimized artificial intelligence model for DDoS detection in SDN environment. IEEE Access. 2023;11:106733-106748.
10. Hossain MA, Islam MS. Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: a promising solution for robust cybersecurity. Measurement: Sensors. 2024;32:101037.
11. Kim J, Kim H, Shim M, Choi E. CNN-based network intrusion detection against denial-of-service attacks. Electronics. 2020;9(6):916.
12. Hu J, Liu C, Cui Y. An improved CNN approach for network intrusion detection system. Int J Netw Secur. 2021;23(4):569-575.
13. Dhanabal L, Shantharajah SP. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. Int J Adv Res Comput Commun Eng. 2015;4(6):446-452.
14. Scheirer WJ, Jain LP, Boult TE. Probability models for open set recognition. IEEE Trans Pattern Anal Mach Intell. 2014;36(11):2317-2324.
15. Perera P, Patel VM. Deep transfer learning for multiple class novelty detection. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2019. p. 11536-11544.
16. Ge Z, Demyanov S, Chen Z, Garnavi R. Generative OpenMax for multi-class open set classification. 2017.
17. Yoshihashi R, Shao W, Kawakami R, One S, Iida M, Naemura T. Classification-reconstruction learning for open-set recognition. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2019. p. 4011-4020.
18. Ahuja N, Singal G, Mukhopadhyay D, Kumar N. Automated DDoS attack detection in software defined networking. J Netw Comput Appl. 2021;187:103108.
19. Hu J, Lin W, Horng M, Wang H. A class-imbalance aware CNN-based intrusion detection system with fruit fly optimization. Applied Sciences. 2021;11(4):1452-1466.
20. Yang J, Liu Y, Zhou Y. Open-set recognition: a survey. IEEE Trans Pattern Anal Mach Intell. 2021;44(11):7661-7679.
21. Shieh C-S, Liu T-Y, Chang J-M. Unknown DDoS attack detection via Bi-LSTM and Gaussian mixture model with expert feedback. Comput Mater Continua. 2021;68(2):2305-2321.

22. Nguyen T-T, Shieh C-S, Chang J-M. DHRNet: a deep hybrid reconstruction network for unknown DDoS attack detection. Applied Intelligence. 2022;52:6883-6900.
23. Lin W-W, Shieh C-S, Chang J-M. GANDD: generative adversarial network with dual discriminators for unknown DDoS detection. IEEE Access. 2022;10:73455-73468.
24. Huang Y-L, Shieh C-S, Chang J-M. SDGAN: symmetrical discriminator GAN for unknown DDoS attack detection. IEEE Trans Netw Serv Manage. 2022;19(4):5432-5444.
25. Horng M-F, Shieh C-S, Chang J-M. CNN-Geo: geometrical feature-enhanced CNN for unknown DDoS attack detection with incremental learning. J Netw Comput Appl. 2023;210:103566.