International Journal of Advancing Research, Innovation and Entrepreneurship

Vol 1(2), DOI:10.82036/jr1rgf82, July 2025 *ISSN:2977-9332*

A Deep Learning Technique for DDoS Detection

[1]Hussain Alhaji Hassan, * [1]Nurudeen Mahmud Ibrahim, [2]Kayode Ibrahim Adenuga & [3]John Temitope Ogbiti

[1] Faculty of Computing, Nile University of Nigeria, Abuja

[2]Centre for Research, Innovation, Development and Entrepreneurship (CRIDE), United Kingdom

[3]Department of Computer Science, Edo State University

*Corresponding Author Email address: kayodeadenuga@yahoo.ca

ABSTRACT

Distributed Denial of Service (DDoS) attacks continue to pose serious risks to online infrastructures, with increasingly severe outcomes owing to the swift evolution of information and communication technologies. As these threats develop, the need for effective detection methods has become more urgent. This research tackles the issue by implementing a deep learning-based technique for DDoS detection, specifically using a recurrent neural network (RNN). The model's performance was assessed using critical metrics such as accuracy, precision, recall, and F1-score, achieving impressive outcomes: 99% accuracy, 99% F1-score, 100% recall, and 99% precision, which confirms its dependability in detecting DDoS traffic. The CICDDoS2019 dataset, which is a well-regarded benchmark within the field of cybersecurity, served as the basis for model training and assessment. Data quality was ensured through preprocessing steps including noise filtering, addressing missing values, and feature transformation via one-hot encoding. The RNN model was also compared with a Convolutional Neural Network (CNN) to assess its effectiveness. The results show that RNN-based models can be a good way to boost network security, and future studies might investigate combining different deep learning methods and using them in real-time for better flexibility.

Keywords: *Network Security, DDoS Detection, Deep Learning, Machine Learning, Recurrent Neural Network.*

1 INTRODUCTION

Over the years, various types of attacks have been directed at online apps and internet services. Among these, DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks have the potential to halt or impair client services, which can occasionally result in significant financial losses and harm to a company's reputation for several internet enterprises (Balandina et al., 2015). DDoS attacks block legitimate users from accessing services like websites and email by assembling several devices against a single target. They are the most frequent and significant attacks from and against cloud computing, fifth generation (5G) communication networks, and Internet of Things (IoT) devices. Based on the volume of traffic they produce, DDoS assaults can be divided into two primary classes: high-rate and low-rate attacks. Low-rate attacks can stop or reduce the target's service quality, even with little traffic. An attacker does this by transmitting data in periodic pulses rather than in continuous flows (Beigh, 2014). This technique significantly impacts network performance, resulting in instability that could render the network unusable. The two main categories of this attack are resource depletion and bandwidth. Resource depletion targets cloud resources, rendering them inaccessible to authorised users. Agent software on botnets, also referred to as compromised PCs, carries out the DDoS assault. To determine which agents are active and plan an attack, the attacker can communicate with many handlers. Behaviour-based detection, another name for intrusion anomaly-based intrusion detection systems, is the main method used to find them. Its foundation lies in contrasting predictable patterns of behaviour with unexpected ones while observing daily activities (Bhavsar & Waghmare, 2013). A new type of DDoS assault has surfaced that mimics the genuine traffic patterns of service customers and avoids detection. While this type of assault may not cause a service outage, it has the potential to reduce the quality of the provided service. DDoS assaults can therefore be divided into two categories: Advanced Distributed Denial of Service (ADDoS) attacks, which include the latest stealthy generation of DDoS, and Traditional Distributed Denial of Service (TDDoS) attacks, which encompass the traditional DDoS attacks (Ektefa et al., 2010).

Attacks by intruders or attackers now target more than only the networking infrastructure due to the proliferation of communication technologies and the development of network technology (Erjavac et al., 2022). To counteract such attacks and safeguard their systems, system administrators use intrusion detection tools (Gao et al., 2020). DDOS Attack Detection was designed to monitor systems and issue alerts whenever any suspicious activity occurs. However, because they don't offer a complete solution to the issue, traditional IDS have intrinsic limits. Although they look for indications of malicious activity in network data, they frequently have trouble correctly identifying malicious activity, which leads to false positives or fails to sound an alarm when the network is operating regularly (Gao et al., 2020). Furthermore, to extract regular patterns from audit data, machine learning algorithms like

Vol 1(2), DOI:10.82036/jr1rgf82, July 2025 ISSN:2977-9332

neural networks and Convolutional Neural Networks (CNN) have been created (Gao et al., 2020). These methods are constrained, nevertheless, due to the limitations of the rule-to-audit record. Researchers have conducted numerous studies on DDoS attack detection. To address these challenges, recent research has increasingly focused on leveraging deep learning techniques for more accurate and adaptive DDoS detection. This study proposes the use of Recurrent Neural Networks (RNNs) to effectively identify DDoS attacks based on network traffic behaviours. The aim is to enhance detection accuracy while minimising false positives, thereby improving overall network security. The remainder of the paper is organised as follows: Section 2 presents the literature review and related work; section 3 discusses the research methodology; section 4 discusses the result and analysis, while section 5 concludes the paper.

2 LITERATURE REVIEW/RELATED WORKS

Over the years, a significant amount of research has been dedicated to improving how we detect intrusions and Distributed Denial-of-Service (DDoS) attacks, particularly using machine learning and deep learning. This section takes a closer look at some of the key studies that have helped move the field forward.

In their 2019 study, Wu and Guo explored different techniques for selecting and classifying features such as Correlation-based Feature Selection (CFS), Principal Component Analysis (PCA), and Information Gain Ratio (IGR) to reduce redundant data. They then tested various classification algorithms, including Support Vector Machines (SVM), k-Nearest Neighbours (k-NN), Neural Networks (NN), Decision Trees (DT), and Naïve Bayes (NB). Using the NSL-KDD dataset, they found that k-NN performed best among the classifiers, while IGR was the most effective feature selection method. Together, these helped improve the quality of data analysis and classification.

Tian et al. (2020) introduced a new approach to intrusion detection by combining Probabilistic Neural Networks (PNN) with Deep Belief Networks (DBN). When tested on the well-known KDD Cup 1999 dataset, their model outperformed more traditional methods. This success was largely due to its ability to turn raw data into lower-dimensional representations using nonlinear learning making the classification process more accurate.

In another study, Peng et al. (2019) built a cyberattack classification system using a deep neural network model. The system had three main steps: data collection, preprocessing, and classification. With 86 input units, a learning rate of 0.01, and 10 training epochs, the model achieved impressive accuracy nearly 96.30% on the SVM classifier, using global optical parameters. When compared with other machine learning models like k-NN, linear regression, and recurrent neural networks, the SVM-based system consistently came out ahead.

Wei et al. (2019) took a hybrid approach, combining both machine learning and deep learning methods to build an anomaly-based intrusion detection system. Using the NSL-KDD dataset, they compared deep learning models like Deep Convolutional Neural Networks (DCNN) and Long Short-Term Memory networks (LSTM) with traditional classifiers such as k-NN, SVM, recurrent neural networks, and decision trees. Their model reached an accuracy of around 85–89%, showing that their method was effective in spotting unusual patterns in network traffic.

Liang and Pan (2019) also contributed to the field with a multi-channel intrusion detection system based on LSTM recurrent neural networks (LSTM-RNNs). Their system involved several stages, including preprocessing, feature abstraction, multi-channel training, and detection. When tested on the NSL-KDD dataset, it delivered excellent results, an accuracy of about 98.94% and a detection rate of 99.23%, clearly demonstrating its ability to reliably identify intrusions.

Finally, Yong and Bo (2019) developed a multi-layered hybrid network intrusion detection system. They tested its performance using the NSL-KDD dataset and applied a range of classifiers, including Naïve Bayes, SVM, and decision trees. Their hybrid system achieved around 91% accuracy, making it a strong candidate for effective intrusion detection.

Overall, these studies highlight some of the key limitations of traditional methods, especially when it comes to issues like false positives and false negatives. These shortcomings stress the importance of developing more advanced solutions, particularly for DDoS detection in today's increasingly connected world. While machine learning has shown promise, many approaches still rely on rigid rule-based systems that struggle to adapt to constantly changing attack patterns. Although there has been substantial progress, there is a need for smarter, more adaptable, and more resilient detection systems to keep up with evolving threats.

3 METHODOLOGY

This section outlines the approach employed in the study, highlighting the primary stages, tools, and methods used in developing and testing a robust intrusion detection system designed to counter Distributed Denial of Service (DDoS) attacks.

3.1 RESEARCH FRAMEWORK

Data Preparation, Method Development, Testing and Evaluation were the three stages of the research, which was conducted according to a defined framework. Clarity and conformity to the goals of the study were guaranteed by this method. The sequential steps—Data Acquisition,

Vol 1(2), DOI:10.82036/jr1rgf82, July 2025 ISSN:2977-9332

Preprocessing, Feature Selection, Model Development, and System Evaluation.

3.2 Phase 1: Data Preparation

The CICDDoS2019 dataset (Sharafaldin et al., 2018) was chosen for DDoS detection. Preprocessing the data was essential to `guaranteeing its uniformity and quality. Among the steps were:

i. Noise Filtering: Noisy and incorrect data were eliminated.
ii. Managing Missing Values: Techniques such as imputing missing data or disregarding partial records were used.
iii. Feature Selection: To find discriminative characteristics essential for DDoS detection, One Hot Encoder (OHE) was used (Pedregosa et al., 2011).

3.3 Phase 2: Model Development

During this phase there is a Recurrent Neural Network (RNN). For the training purpose the dataset was split into 70% while 30% was used for testing.

3.4 Phase 3: Testing and Evaluation

Model performance was assessed during the evaluation phase utilizing measures such as F1 Score, Accuracy, Precision and Recall.

3.5 Experimental Setup

The Google Collaboratory platform was used in the experimental setup of the Enhanced DDOS Detection Using deep Learning. Recurrent neural networks and MLP (Multi-Layer Perceptron) algorithms were used in the system's development, along with one-way ANOVA for feature selection. To use as the data source for the experiments, a portion of the CICDDOS 2019 dataset was taken from the Kaggle repository.

3.6 Dataset

The CICDDOS 2019 DDos detection dataset was used in this investigation. It includes nine different kinds of attacks, such as worms, backdoors, fuzzers, and DoS (Denial of Service) assaults. The dataset offers a thorough depiction of network traffic because it is made up of raw network packets. There are 175,341 records in the training set and 82,332 records in the testing set. These data cover both typical network traffic and a broad variety of attack methods, enabling a comprehensive investigation and assessment of the suggested models.

3.7 Implementation Tools

Because of its rich libraries for data processing and machine learning, as well as its ease of use and versatility, Python was used in the research to develop the system. Python's support for numerous paradigms and disciplined design philosophy made it easier to create a system that is both scalable and effective.

4 RESULTS AND DISCUSSION

With an accuracy and recall score of 0.99, the Recurrent Neural Network (RNN), as displayed in Table I and Figure 1, demonstrated outstanding performance and a strong ability to accurately categorize instances and identify positive cases with negligible omissions. Its F1-score of 0.98 indicates a balanced performance between precision and recall, while its precision score of 0.98 indicates dependability in reducing false positives. These measures show how well and robustly the RNN handles the task at hand with high sensitivity and overall accuracy.

With accuracy and recall scores of 0.99, the Recurrent Neural Network (RNN) and the Multilayer Perceptron (MLP) demonstrate remarkable performance, highlighting their capacity to accurately anticipate instances across all classes and successfully locate pertinent positive situations. The MLP, however, has a little advantage over the RNN (0.98) according to the F1-score, which shows that it strikes a somewhat better balance between recall and precision. Both models' high precision of 0.98 indicates their dependability in identifying positive cases. Although both models exhibit excellent performance, the MLP is marginally more adaptable for tasks that call for a balance between false positives and false negatives because to its higher F1-score, which represents its stronger robustness in minimizing errors and preserving equilibrium in classification performance.

TABLE I: RESULT

Models	Accuracy	Recall	F1-Score	Precision
RNN	0.99	0.99	0.98	0.98
CNN	0.99	0.99	0.98	0.98

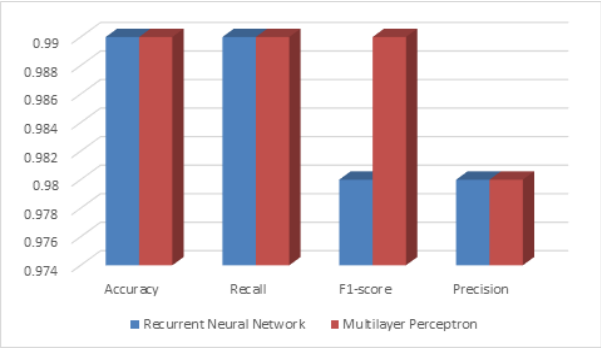


Figure 1: Result

Vol 1(2), DOI:10.82036/jr1rgf82, July 2025 ISSN:2977-9332

4 CONCLUSION

This study demonstrates the strong potential of Recurrent Neural Networks (RNNs) in detecting Distributed Denial of Service (DDoS) attacks, achieving impressive performance metrics: 99% accuracy, 99% recall, 99% precision, and 98% F1-score. These results highlight the practical effectiveness of RNNs in identifying and classifying malicious traffic with high reliability and minimal false positives. From a theoretical perspective, the findings add to the growing evidence that deep learning models are well-suited for cybersecurity tasks. In practice, RNNs can significantly enhance the capabilities of intrusion detection systems, especially in dynamic and high-volume network environments. However, this study is limited by its use of a single dataset (CICDDoS2019), which may not reflect the full range of attack patterns in real-world scenarios. Future research should explore hybrid models, such as combining RNNs with CNNs or Transformers to further improve detection performance. It would also be valuable to evaluate these models using real-time traffic, consider their scalability, and assess their resilience to adversarial attacks. Incorporating model explainability could additionally help build trust and transparency in security operations.

REFERENCES

Balandina, E., Balandin, S., Koucheryavy, Y., & Mouromtsev, D. (2015, July). IoT use cases in healthcare and tourism. In *2015 IEEE 17th conference on business informatics* (Vol. 2, pp. 37-44). IEEE.

Beigh, B. M. (2014). A new classification scheme for intrusion detection systems. *Int. J. Comput. Netw. Inf. Secur*, *6*(8), 56.

Bhavsar, Y. B., & Waghmare, K. C. (2013). Intrusion detection system using data mining technique: Support vector machine. *International Journal of Emerging Technology and Advanced Engineering*, *3*(3), 581-586..

Ektefa, M., Memar, S., Sidi, F., & Affendey, L. S. (2010, March). Intrusion detection using data mining techniques. In *2010 International Conference on Information Retrieval & Knowledge Management (CAMP)* (pp. 200-203). IEEE.

Erjavac, I., Kalafatovic, D., & Mauša, G. (2022). Coupled encoding methods for antimicrobial peptide prediction: how sensitive is a highly accurate model? *Artificial intelligence in the life sciences*, *2*, 100034.

Gao, K., Mei, G., Piccialli, F., Cuomo, S., Tu, J., & Huo, Z. (2020). Julia language in machine learning: Algorithms, applications, and open issues. *Computer Science Review*, *37*, 100254.

Liang D, Pan P (2019). "Research on intrusion detection based on improved DBN-ELM," in 2019 international conference on communications, information system and computer engineering (CISCE). 2019;495- 499.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. *the Journal of machine Learning research*, *12*, 2825-2830.

Peng, W., Kong, X., Peng, G., Li, X., & Wang, Z. (2019). Network intrusion detection based on deep learning. In *2019 International Conference on Communications, Information System and Computer Engineering (CISCE)* (pp. 431-435). IEEE.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, *1*(2018), 108-116.

Tian Q, Han D, Li K-C, Liu X, Duan L. (2020) Castiglione, An intrusion detection approach based on an improved Machine belief network, *Applied Intelligence*.;50:3162-3178.

Wei P, Li Y, Zhang Z, Hu T, Li Z, Liu D (2019). "An optimization method for intrusion detection classification model based on Machine belief network," IEEE Access. 2019;7:87593-87605.

Yong L, Bo Z (2019). "An intrusion detection model based on multi-scale CNN," in 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). 2019;214- 218.