Journal of Research in Computer Science and Engineering
Volume 11, Issue 1, January-April 2026
ISSN: 2457-0818 (Online)

DDoS Attack Detection

Roopali Pattankude[1], Supriya Munavalli[2], Ranjita Chougale[3], Nayan Hullikuppi[4] and Vijaylaxmi Nagnur[5]

Student[1, 2, 3 ,4], Assistant Professor[5]

Department of Computer Science and Engineering

Jain College of Engineering and Research, Belagavi

Corresponding Authors' Email: *pattankuderoopali16@gmail.com*

DOI: *https://doi.org/10.5281/zenodo.19204722*

ABSTRACT

DDoS (Distributed Denial of Service) attacks are becoming a real problem for cloud servers and networks, causing major disruptions and financial losses. As technology keeps evolving, Software Defined Networks (SDN) and Machine Learning (ML) are offering new ways to fight back. In this paper, we introduce a machine learning model that can quickly adapt to new types of DDoS attacks as they happen. The model focuses on the most important data, which makes it really good at catching attacks. Our results were pretty impressive, with the model detecting 99.2% of attacks, outperforming others on well-known datasets like UNSW_NB15 and In SDN, We also looked into how the Random Forest algorithm can detect and block DDoS attacks in real-time, especially in cloud systems, by analyzing network traffic. This research shows how effective machine learning can be in improving network security and reducing the harm caused by DDoS attacks. Ultimately, our work offers a strong solution for protecting SDN systems and ensuring cloud services remain safe from the rising threat of cyberattacks.

KEYWORDS: *Distributed Denial of Service (DDoS) Detection, Cloud Computing Security, Software Defined Networking (SDN), Machine Learning Algorithms, Random Forest Classifier, Intrusion Detection System (IDS), UNSW_NB15 Dataset, Network Traffic Analysis.*

INTRODUCTION

Various services like servers, databases, and software over the Internet through virtual resources. Because of the scalability and cost-effectiveness of services, cloud adoption is rapidly increasing worldwide. Distributed denial-of-service (DDoS) attack in cloud computing is a common threat due to the growing adoption of cloud by many organizations. DDoS attack detection using machine learning (ML) techniques has gained popularity because of the ability of ML algorithms to uncover relationships and patterns in data that are not clear to humans.

Crypto coins or crypto currencies normally used as alternative monetary systems on the internet create a stronger passion in cyberspace. Distributed denial-ofservice (DDoS) attacks on the networks of banks and stockbrokers can cause significant disruption on networks within Cyber space, and big financial loss for customers who rely on these services.

A DDoS attack happens when many computers or devices send a huge amount of traffic to one system or network. This heavy flood of requests overloads the system, making it too busy to respond to genuine users. As a result, normal users cannot access websites or services, leading to downtime, financial loss, and frustration. These attacks are becoming stronger because attackers now use large groups of infected computers, also called botnets. Many of these devices are simple gadgets like cameras, routers, or IoT devices that are connected to the internet without proper security.

Over the years, attackers have developed different types of DDoS attacks. Some try to block the network bandwidth, others target weaknesses in communication protocols, and some directly overload web applications. Each type of attack disrupts the system in its own way, and detecting them is difficult because the attack traffic often looks almost the same as normal user traffic.

Old security tools like firewalls and fixed rules are no longer enough to stop these attacks. This is because internet traffic changes quickly, and attackers keep finding new ways to create trouble. To deal with this, specialists now use modern methods that carefully study how data moves across the network and decide what looks normal and what looks suspicious. The main aim of our work is to build a system that can quickly and accurately separate normal traffic

from attack traffic while it is happening in real time. To achieve this, we use methods like Random Forest, Logistic Regression, Support Vector Machine (SVM), and Neural Networks. These methods try out different approaches and see which one is works best for quick detection and high accuracy. By training our system with real traffic data, it can learn to recognize when an attack begins. Through this comparison, we can identify which method provides the most accurate and quick results. This work is very important because preventing DDoS attacks not only keeps services secure but also ensures that genuine users can continue their activities without interruption. As the number of internet- connected devices keeps increasing — from small household gadgets to large cloud systems — the need for a strong and reliable DDoS detection system is becoming more important than ever.

LITERATURE REVIEW

Over the past ten years, DDoS attacks have become a major headache for companies that depend on cloud services [3]. They flood servers and networks with so much traffic that real users often cannot access the services they need. Because attackers keep changing tactics, old defenses like firewalls and simple rule-based filters often fall short [6].

At first, researchers used classic machine- learning tools — Decision Trees, Naïve Bayes, SVMs, and Random Forests [1]. Those methods did okay: Random Forests in particular scored high on datasets such as NSL-KDD and UNSW_NB15 [1]. SVM worked well in some IoT and SDN setups, but it is heavy on computing and does not scale easily [4]. Another problem with these traditional approaches was too many false alarms, and they often could not keep up when attack methods changed [9].

To fix this, people moved to deep learning. CNNs turned out to be good at spotting hidden patterns in traffic, and LSTMs handled time-based traffic behavior well (for example, in CICIDS2017) [12]. Auto encoders combined with basic MLPs made things easier by automatically highlighting the key features in the network traffic [15]. Overall, Deep Neural Networks (DNNs) have been the most consistent, reaching around 96–98% accuracy on datasets like NSL-KDD, CICIDS2017, and CSE-CIC-IDS2018 [11].

Lately, researchers have mixed and matched methods — hybrid and ensemble approaches like AdaBoost, XGBoost, and bagging — and sometimes they achieved near-perfect scores

on datasets such as UNSW_NB15 [14][20].

These combined methods also help prevent overfitting — that is when a model does really well in tests but struggles when faced with real-world traffic [7]. Some other helpful methods include studying traffic patterns, such as using entropy [6], automatically adjusting firewall rules through reinforcement techniques [25], and applying federated learning so models can improve without sharing private data [21].

Even with these improvements, challenges remain. Most models are tried on just a simple dataset, so we do not really know how they will perform on other real-world network traffic [3]. Deep learning models also need a lot of computing power, which makes it hard to use them instantly or in real time [11].

In short: traditional methods like Random Forest can still be useful, but deep learning—especially DNNs — gives better and good accuracy and flexibility for complex DDoS attacks. Ensembles make detection stronger and best, but future work must focus on realtime networks, scalable solutions that work across varied datasets and keep false positives low [14].

RELATED WORK

Researchers across the world have studied DDoS detection for many years. With the rise of cloud computing and IoT device, the importance of detecting such attacks has grown even more.

Kumar et al. [1] showed that machine-learning methods like Random Forest perform better than older rule-based systems. Priyadarshini and Barik [2] tried deep learning models in cloud environments and achieved high detection accuracy, though they required heavy computation.

Khater et al. [5] used different deep learning models for DDoS detection and reported good results than single classifiers. Li et al. [7] looked at different ways to spot unusual activity in cloud systems and highlighted something important — when devices have limited power or memory, it is better to use lightweight models that do not demand too much from them. Mahmoud et al. [9] worked on lightweight ML models that still managed to maintain

good accuracy.

Some studies have focused on real- time detection. On the other hand, Luo et al. [13] used advanced graphbased methods to speed up how quickly attacks can be identified. Patel and Shah [14] worked on lightweight deep learning models that are better suited for IoT and cloud environments.

Another recent trend in research is the use of federated learning. Javed et al. [15] introduced a system where multiple organizations can work together to train models without directly sharing their raw data, which improves both privacy and scalability.

From what we have seen in earlier studies, using machine learning and deep learning tends to catch DDoS attacks more accurately than traditional, rule-based methods. These newer approaches can spot patterns and adapt better, making them more effective at dealing with the complexity of modern cyber threats.

In our project, we set out to address these issues by testing and comparing different approaches—Random Forest, Logistic Regression—to find out which one offers the best balance of speed, accuracy, and efficiency when analyzing real network traffic.

METHODOLOGY

The main goal of our project is to create a system that can quickly and reliably spot DDoS (Distributed Denial of Service) attacks in cloud-based networks. To make this happen, we followed a clear, step-by-step approach. We began by gathering real data, then cleaned and organized it to make sure it was ready for analysis. After that, we tried out several different methods to teach the system how to recognize attack patterns. We carefully tested how well each method worked and compared the results to figure out which one was the most accurate and dependable. This helped us choose the best solution for detecting these kinds of threats effectively.

1. Data Collection

For this work, we used the UNSW_NB15 dataset, which is one of the most commonly used datasets in research for DDoS detection. It contains a mix of normal and attack traffic, making

it useful for training and testing machine learning models [1], [2].

2. Data Preprocessing

Since raw network data usually contains missing values, unnecessary columns, and numbers with large differences in scale, we first need to clean and organize the dataset. We removed unnecessary features, handled missing values, and converted the data into a proper format. After that, we applied standardization so that all features are on the same scale, which makes training more effective [3].

3. Feature Selection

Not all features contribute equally to detection. Some may increase complexity without enhancing outcomes. To handle this issue, we used methods like Random Forest ranking to pick out only the most important features [4].

4. Model Training

To find the best way to spot DDoS attacks, we tried out four different types of models—each with its own style of learning and decision-making.

Random Forest (RF) is commonly applied because it can process large datasets effectively while maintaining accuracy and consistency. Logistic Regression (LR) is simpler in design, yet it performs quickly and is reliable for distinguishing between normal traffic and suspicious activity. The Multi-Layer Perceptron (MLP), belonging to the neural network family, enhances detection by learning deeper patterns in the data, which helps in identifying attacks that are harder to catch with basic approaches.

The dataset was divided into 70% training and 30% testing, making sure the data balance between attack and normal traffic was maintained.

5. Model Evaluation

To test the models, we used metrics like accuracy, precision, recall, and F1-score. These measures give us a clear picture of how well each model is performing, especially when the data is unbalanced. We also used confusion matrices to see exactly where the models made errors [9].

6. ROC and AUC Analysis

Apart from accuracy, we also looked at ROC curves and AUC values, which help us understand how well each model can separate attack traffic from normal traffic [10].

7. Model Comparison

Finally, we compared all models to see which one gives the best trade-off between accuracy, detection speed, and efficiency. This helps in selecting the most suitable model for real-time DDoS detection [11].

8. Real-time Detection and Mitigation

The models are tied into a simple Flask interface that looks at network traffic as it happens. Instead of waiting to collect data first, the system checks each flow on the spot and tries to notice if anything looks out of place.

RESULTS

A. Confusion Matrices of ML Models

Fig. 1- The confusion matrices offer a practical, easy-to-compare view of how each model Random Forest, MLP, and Logistic Regression actually performs. Instead of relying only on accuracy numbers, these charts show exactly where each model gets things right or wrong, especially when distinguishing normal traffic from maliciousactivity.

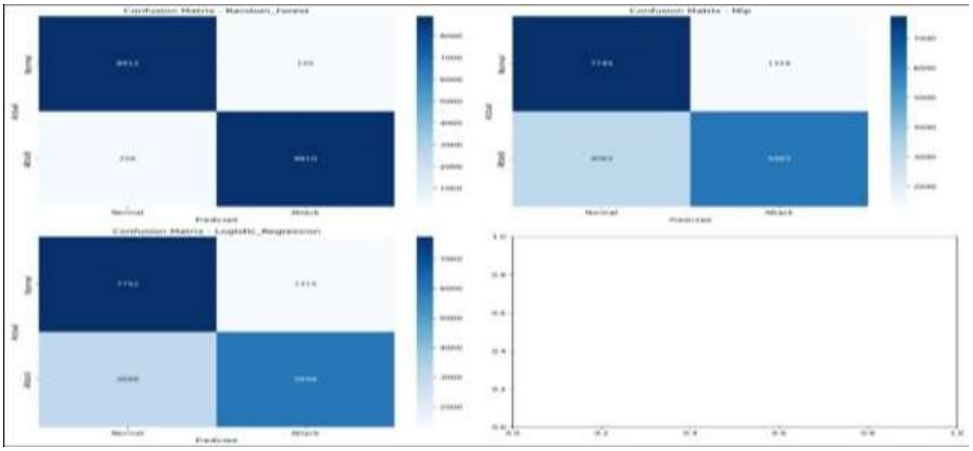

Figure 1: Confusion Matrix

B. Feature Importance – Random Forest

Fig. 2 shows, which network features the Random Forest model pays the most attention to.

Instead of guessing what the model is reacting to, this chart lays it out clearly.Seeing these ranked makes it easier to understand what the model thinks is suspicious. This helps when improving the system later because you know exactly which parts of the traffic deserve morefocus.

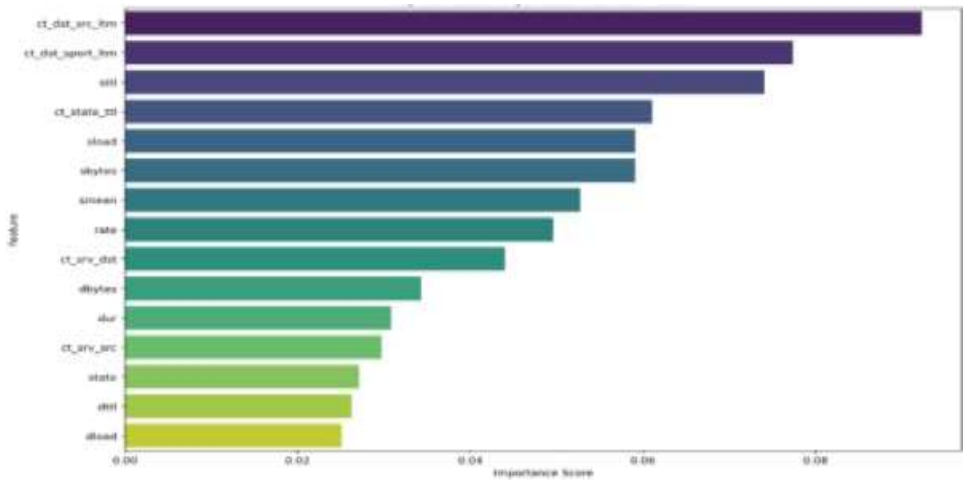

Figure 2: Feature Importance – Random Forest

C. DDoS Feature Correlation

Fig. 3 is a heatmap that shows how different network features relate to each other and to the attack label. The colors make it simple to spot which behaviors move together and which ones move in opposite directions. Strong colors—either dark red or blue—mean there's a clear connection. This helps in understanding which traffic patterns usually show up when an attack is happening. It's a straightforward way to see relationships that might be hard to notice just by looking at the raw numbers.

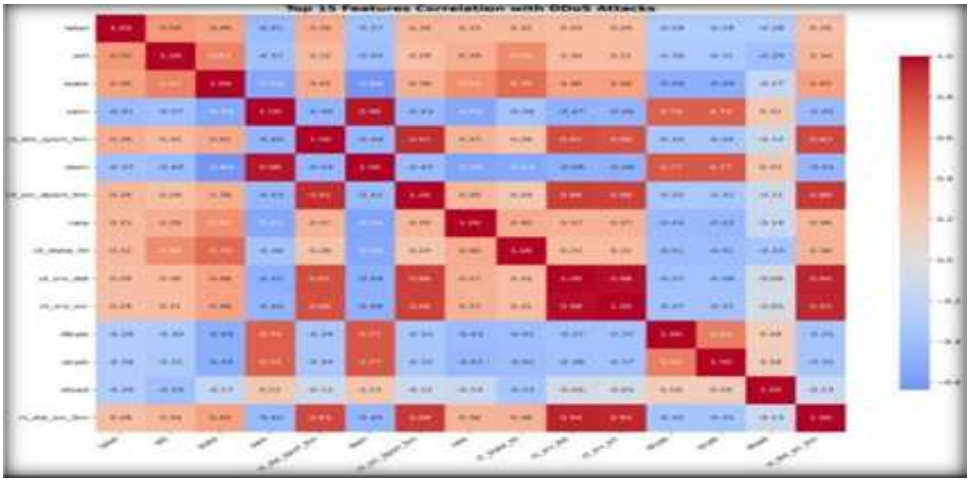

Figure 3: DDoS Feature Correlation

D. ROC Curve Comparison

In Fig. 4, the ROC curves of the three models are shown together. This graph basically helps you see how well each model separates normal traffic from attack traffic. When comparing the AUC values, it's obvious that the Random Forest model performs better than the other two. This figure makes it easy to pick the model that you can trust the most for the detection system.

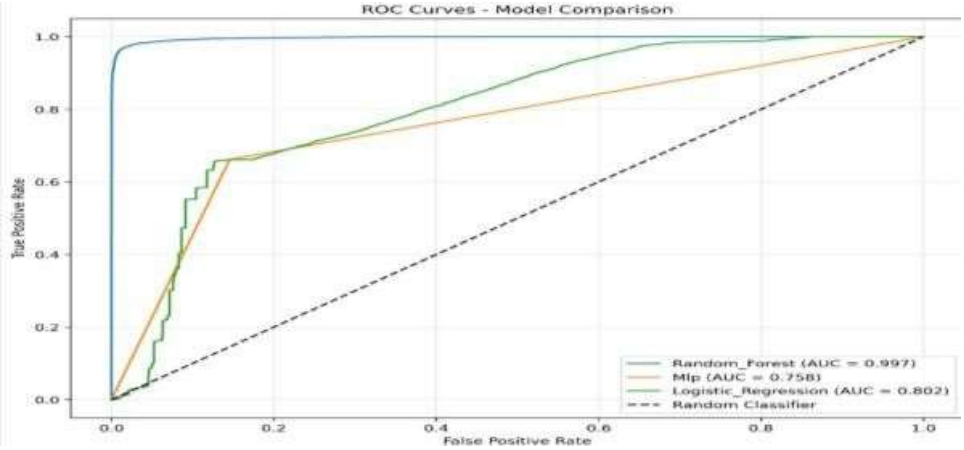

Figure 4: ROC Curve Comparison

E. DDoS Detection Dashboard

In Fig. 4, the ROC curves of the three models are shown together. This graph basically helps you see how well each model separates normal traffic from attack traffic. When comparing the AUC values, it's obvious that the Random Forest model performs better than the other two. This figure makes it easy to pick the model that you can trust the most for the detection system.

Figure 5: DDoS Detection Dashboard

F. Live Traffic Rate Monitor

Fig. 6 displays a live graph of network traffic, showing both Mbps and packets per second. The graph makes it easy to notice sudden spikes or drops in traffic, which can be the first signs of an attack. With this live view, operators can react faster and catch unusual activity as soon as it starts.

Figure 6: Live Traffic Rate Monitor

G. Recent Threats Panel

Fig. 7 lists the threats the system has detected recently. Each entry shows when it happened, where it came from, what type of attack it was, how serious it was, and the model's confidence. This panel makes it quick and simple to review recent events and see patterns if similar attacks happen repeatedly.

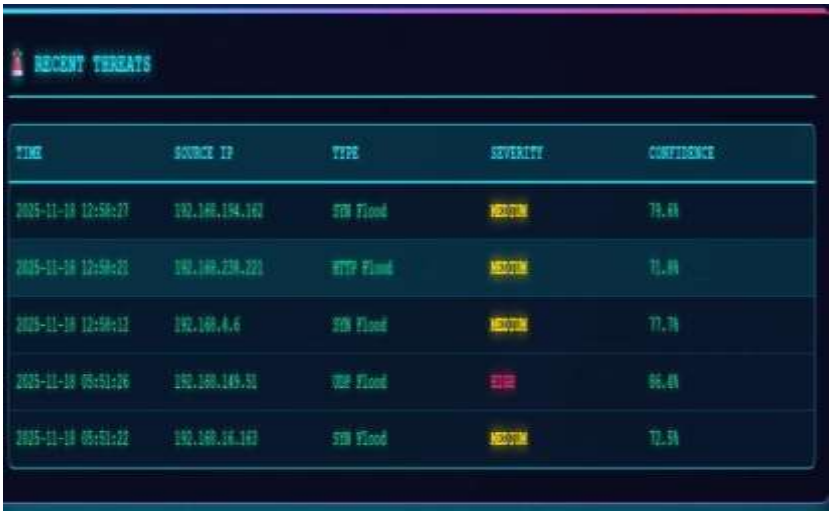

Figure 7: Recent Threats Panel

H. Real-Time Traffic Monitor

ableFig. 8 provides a detailed, live view of network traffic. It shows which IP addresses are connected, what protocols they are using, how long the connections have lasted, and their current status. This helps operators see if the traffic is normal or suspicious.It's very useful for examining or verifying unusual activity as it happens.

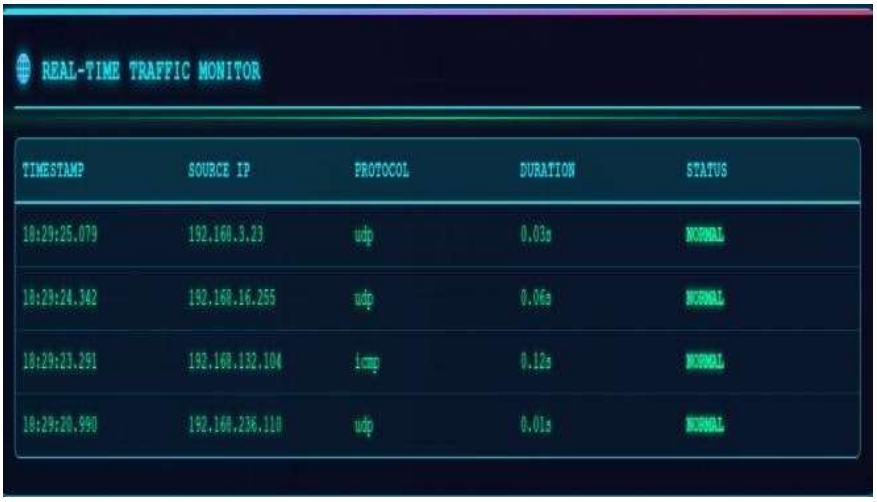

Figure 8: Real-Time Traffic Monitor Table I.Historical Data Viewer

Fig. 9 shows a summary of network activity for a chosen date. You can see the total traffic, how much of it was identified as attack traffic, and a bar chart that breaks down the types of attacks that occurred.This view is helpful for looking back, spotting trends, and reviewing incidents to understand what happened on a particular day.

Figure 9: Historical Data Viewer

I. Threat Intelligence Insights

Fig. 10 highlights the most important findings from the system. It lists the IP addresses that seem most suspicious, along with their threat scores. It also shows which attack types happen most often and how long they usually last.This gives a bigger picture of the network threats and helps the team focus on the most pressing risks.

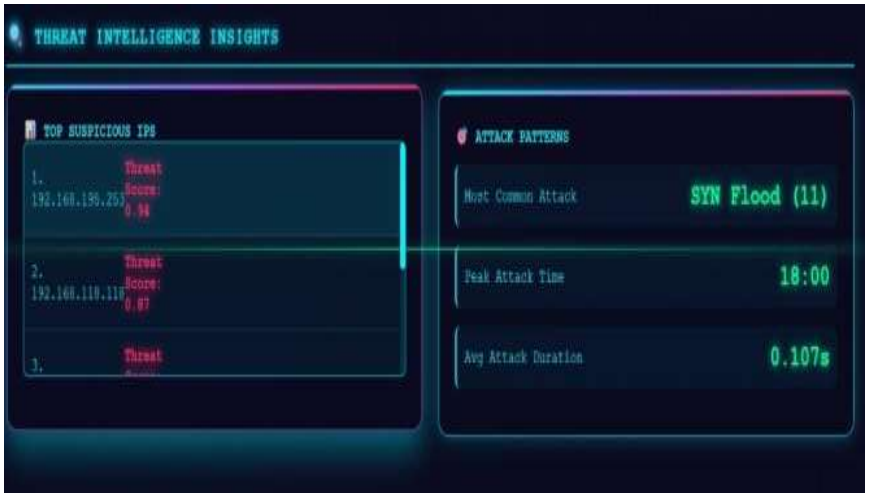

Figure 10: Threat Intelligence Insights

J. Blocked IP Addresses

Fig. 11 lists all the IP addresses the system has blocked, along with the reason for blocking, how severe the threat was, when it was blocked, and when the block will end. This makes it simple to keep track of blocked sources and check whether any of them need to be reviewed or updated later.

Figure 11: Threat Intelligence Insights

CONCLUSION

DDoS attacks remain a serious threat to the security and smooth functioning of cloud and network systems. This study shows that using smarter and more adaptable ways to detect and block these attacks can make a big difference. Solutions that are both flexible and efficient help protect against many kinds of attacks without causing delays or slowing down the system. Going forward, we need to keep making detection methods better, test them in real-life situations, and bring together different security tools to create systems that are stronger and more secure.

REFERENCES

1. R. Kumar, B. Gupta, and A. Sharma, "Machine learning-based DDoS attack detection in cloud computing," Future Generation Computer Systems, vol. 111, pp. 763–779, 2020.
2. R. Priyadarshini and R. K. Barik, "A deep learning-based intelligent framework to detect DDoS attacks in cloud environment," Journal of King Saud University - Computer and Information Sciences, vol. 32, no. 1, pp. 99–109, 2020.
3. G. Somani et al., "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, vol. 167, pp. 20–41, 2020.
4. N. Alrajeh, M. Alazab, and M. Khan, "Anomaly-based detection of DDoS attacks in IoT networks using deep learning," IEEE Access, vol. 8, pp. 132202–132213, 2020.
5. F. Hussain et al., "Machine learning for resource management in cloud and edge computing: An overview," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2008–2031, 2020.
6. H. Beitollahi and G. Deconinck, "Analyzing countermeasures against distributed denial of service attacks," Computer Communications, vol. 160, pp. 16–30, 2020.
7. H. Lin et al., "A multi-layer hybrid model for DDoS attack detection in cloud computing," Future Generation Computer Systems, vol. 115, pp. 436– 448, 2021.
8. E. Bertino and N. Islam, "Botnets and Internet of Things security," Computer, vol. 54, no. 3, pp. 56–64, 2021.
9. S. A. Shah et al., "AI-driven anomaly detection in IoT and cloud computing: A survey of techniques and challenges," IEEE Access, vol. 9, pp. 118206–118225, 2021.
10. Singh and R. Tripathi, "Machine learningbased intrusion detection system for cloud computing," International Journal of Information Security and Privacy, vol. 15, no. 3,

pp. 67–82, 2021.

11. M. Khater et al., "Deep learning for DDoS detection in cloud environments," IEEE Access, vol. 9, pp. 42740–42755, 2021.
12. Y. Li, X. Liu, and C. Wu, "A CNN–RNN hybrid model for detecting DDoS attacks in cloud computing," Computers & Security, vol. 112, p. 102546, 2022.
13. Alqahtani and F. Hussain, "Adaptive learning models for real-time DDoS detection in SDN-enabled cloud computing," IEEE Access, vol. 10, pp. 99812–99827, 2022.
14. Y. Yang et al., "An ensemble deep learning model for DDoS detection in cloud environments," Future Generation Computer Systems, vol. 128, pp. 218–229, 2022.
15. X. Tang and Y. Wang, "Real-time anomaly detection of network traffic in cloud computing using autoencoders," Journal of Network and Computer Applications, vol. 204, p. 103404, 2022.
16. Das and S. Misra, "Blockchain- enabled defense against DDoS attacks in cloud computing," IEEE Transactions on Cloud Computing, 2022.
17. R. Mahmoud et al., "Lightweight machine learning models for DDoS detection in IoT networks," IEEE Access, vol. 10, pp. 43212– 43225, 2022.
18. T. Zhang and H. Chen, "Attention- based deep learning for DDoS detection in cloud and IoT systems," Computers & Security, vol. 126, p. 103040, 2023.
19. F. Ullah et al., "Explainable AI for DDoS attack detection in IoT and cloud systems," IEEE Access, vol. 11, pp. 44312– 44328, 2023.
20. Ghosh and S. Banerjee, "Hybrid ML approach for high-speed DDoS detection in cloud data centers," Future Generation Computer Systems, vol. 138, pp. 112–125, 2023.
21. H. Javed et al., "A federated learning framework for DDoS detection in cloud computing," IEEE Internet of Things Journal, 2023.
22. P. Kaur and A. Singh, "Cloud security against DDoS: A deep learning perspective," Journal of Cloud Computing, vol. 12, no. 1, pp. 1–15, 2023.
23. J. Luo et al., "Real-time detection of DDoS attacks using graph neural networks," IEEE Transactions on Dependable and Secure Computing, 2023.
24. H. Patel and S. Shah, "Lightweight deep learning for DDoS detection in IoT- cloud systems," Future Internet, vol. 16, no. 2, p. 45, 2024.
25. J. Wang et al., "Self-learning DDoS detection using reinforcement learning in cloud networks," IEEE Access, vol. 12, pp. 204112–204128, 2024.

Cite as:

Roopali Pattankude, Supriya Munavalli, Ranjita Chougale, Nayan Hullikuppi, Vijaylaxmi Nagnur. (2026). DDoS Attack Detection. Journal of Research in Computer Science and Engineering, 11(1), 18-32.

https://doi.org/10.5281/zenodo.19204722