Archives available at journals.mriindia.com

**International Journal of Electrical, Electronics and Computer Systems**

ISSN: 2347-2820
Volume 14 Issue 01, 2025

# Detection of DDoS Attack in Cloud Computing using Machine Learning Algorithm

Saroj Shambharkar[1], Ketki Thakare[2], Sambhav Takkamore[3], Rahul Padole[4], Kashish Chaure[5]

[1]*Head of Department of Information Technology, Kavikulguru Institute of Technology & Science, Ramtek,*
*Nagpur, Maharashtra, India*
[2],[3],[4],[5] *Department of Information Technology, Kavikulguru Institute of Technology & Science, Ramtek, Nagpur, Maharashtra, India*

**Peer Review Information**

*Submission: 07 Feb 2025*
*Revision: 16 Mar 2025*
*Acceptance: 18 April 2025*

**Keywords**

*Cloud Computing*
*DDoS Attack*
*Machine Learning*
*Cyber security*

**Abstract**

Cloud Computing is highly susceptible to Distributed Denial of Service (DDoS) attacks, which can disrupt services and compromise security. Traditional methods struggle to detect evolving attack patterns effectively. This study explores machine learning algorithms like SVM, Random Forest, and Neural Networks for identifying DDoS attacks in real time. These models enhance accuracy and response time by distinguishing malicious traffic from legitimate users. The results highlight the effectiveness of intelligent threat detection in securing cloud environments.

## INTRODUCTION

In the rapidly evolving landscape of cloud computing, ensuring the security and availability of services is paramount. Distributed Denial of Service (DDoS) attacks pose a significant threat to cloud environments, disrupting services by overwhelming servers, networks, or applications with a flood of malicious traffic. As the scale and sophistication of DDoS attacks continue to grow, traditional detection and mitigation techniques often struggle to keep pace. This has led to the adoption of advanced approaches, including machine learning (ML) algorithms, to enhance the detection and prevention of such attacks.

Machine Learning offers the ability to analyze large volumes of network traffic data, identify patterns, and detect anomalies in real-time. By leveraging these capabilities, ML- based systems can distinguish between legitimate traffic and malicious activity with greater accuracy. Unlike rule-based systems, which rely on predefined signatures and thresholds, machine learning models can adapt to evolving attack patterns and novel threats, making them particularly well-suited for dynamic cloud environments.

## PROPOSED SYSTEM

The methodology involves collecting and preprocessing data from datasets like CICDDoS2019, selecting relevant features, and training ML models such as Decision Trees, Random Forest, SVM,ANN, and Gradient Boosting techniques. The trained model is deployed in a cloud-based intrusion detection system with real-time monitoring.

Expected outcomes include an efficient and accurate DDoS detection system, improved response time, and a comparative analysis of ML algorithms. Future work will explore deep learning models, adversarial attack counter measures, and AI- driven mitigation strategies using SDN.

**Block Diagram**

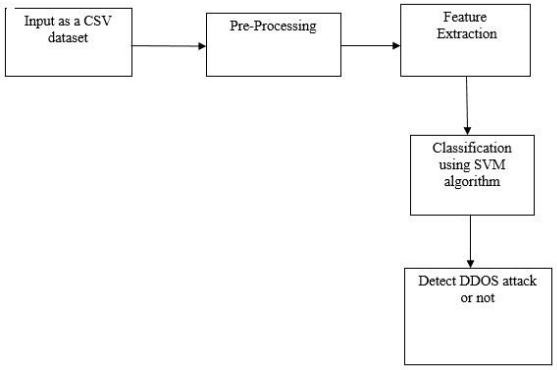


*Fig 1: Block diagram of Detection of DDoS attack in cloud computing using machine learning algorithm*

**Architecture Diagram**

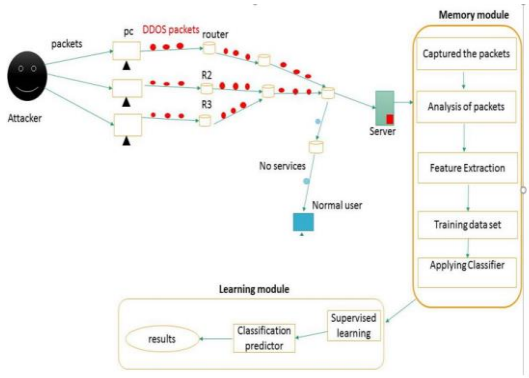


*Fig 2: Architecture of Detection of DDoS attack in cloud computing using machine learning algorithm*

**Working**

DDoS attacks pose a serious challenge to cloud computing environments, leading to service disruptions, resource exhaustion, and security breaches. This study proposes a machine learning-based detection system to effectively identify and mitigate such attacks. The key objective of this research includes developing a robust detection model, analyzing various machine learning algorithms to determine their effectiveness, improving detection accuracy while minimizing false positives, and implementing a real-time monitoring and alerting system to enhance cloud security.The detection system follows a structured workflow consisting of several stages. The process begins with data collection, where network traffic data is obtained from publicly available datasets such as CICDDoS2019, CAIDA, or through controlled network simulations. This data consists of both normal and attack traffic patterns, which are essential for training the model. Following data collection, preprocessing is conducted to clean the data by handling missing values, normalizing numerical features, and encoding categorical variables.

Relevant features such as packet arrival rate, flow duration, protocol type source- destination IP statistics, and traffic behavior patterns are extracted. Once feature selection is complete, the data is used to train multiple machines learning models, including Decision Trees, Random Forests, Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Gradient Boosting techniques like XGBoost and Light GBM. Each model is evaluated based on accuracy, precision, recall, F1-Score, and ROC-AUC to determine the best performing algorithm.

**SOFTWARE SETUP**

The implementation of DDoS attack detection system requires a structured software setup: -

- Operating Systems: Ubuntu 20.04 or a compatible Linux distribution for deployment.
- Programming Language: Python (with libraries such as Scikit-learn, Tensor Flow, PyTorch, Pandas, NumPy, and Matplotlib for data analysis and model deployment).
- Machine Learning Frameworks: Scikitlearn, TensorFlow, PyTorch, and light BGM for training and evaluating models.
- Database: MongoDB or Postgre for storing network traffic logs and attack records.

**RESULT AND DISCUSSION**

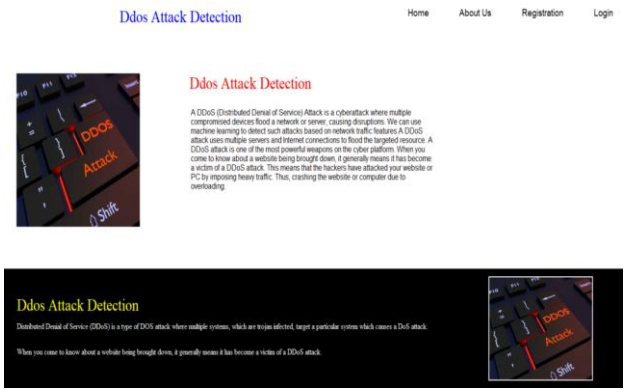


*Fig 2.1: Home page of registration*

In this home page there are options like registration, login and firstly the registration process takes place then account is created successfully after that go to login page where all credentials are entered.


*Fig 2.2: Registration page*


*Fig 2.3: Login Page*

Username and password must be entered and then click on login button and then the DDoS detection page will appear click on detect the DDoS attack. Dataset contain the all port address, protocol, and destination address, Packet Length, Traffic Type, Alerts Warnings, Security Level and log source.


*Fig 2.4: DDoS attack detection using ML*


*Fig 2.5: DDoS attack Detected Value*

The results of the DDoS detection system demonstrate its effectiveness in identifying and mitigating attacks in cloud computing environments. The machine learning models achieved high accuracy in classifying network traffic, with Random Forest and XGBoost showing superior performance in terms of precision, recall and F1- score.

## CONCLUSIONS

This study highlights the effectiveness of using machine learning algorithms for detecting and mitigating DDoS attacks in cloud computing environments. By leveraging feature selection techniques and training multiple ML models, the proposed detection system demonstrated high accuracy and reliability in identifying various types of DDoS attacks. The real-time deployment using streaming frameworks like Apache Kafka and Spark Streaming further enhances cloud security by enabling swift detection and response mechanisms.

## FUTURE SCOPE

The future scope of DDoS attack detection in cloud computing using machine learning involves several promising directions. First, the integration of deep learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), can further enhance the accuracy and adaptability of detection models. Additionally, reinforcement learning and AI-driven self-learning models can improve the system's ability to detect new and evolving attack patterns

## References

1. N. Tabassum, M. S. Khan, S. Abbas, T. Alyas, A. Athar, and M. A. Khan, "EAI Endorsed Transactions Intelligent reliability management in hyperconvergence cloud infrastructure using fuzzy inference system," pp. 1–12.

2. A. S. Boroujerdi and S. Ayat, "A robust ensemble of neuro-fuzzy classifiers for DDoS attack detection," Proc. 2013 3rd Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2013, pp. 484–487, (2014).

3. L. Kwiat, C. A. Kamhoua, K. A. Kwiat, and J. Tang, "Risks and Benefits: Game-Theoretical Analysis and Algorithm for Virtual Machine Security Management in the Cloud," Assur. Cloud Comput., pp. 49–80, (2018).

4. A. K. Soliman, C. Salama, and H. K. Mohamed, "Detecting DNS Reflection Amplification DDoS Attack Originating from the Cloud," Proc. - 2018 13th Int. Conf. Comput. Eng. Syst. ICCES 2018, pp. 145–150, (2019).

5. X. Jing, Z. Yan, and W. Pedrycz, "Security data collection and data analytics in the internet: A survey," IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 586–618, (2019).

6. Rudol, "Implementasi Keamanan Jaringan Komputer Pada Virtual Private Network ( Vpn ) Menggungakan," Implementasi Keamanan Jar. Komput. Pada Virtual Priv. Netw. Menggungakan Ipsec, vol. 2, no. 1, pp. 65–68, (2017).

W. Alosaimi, M. Alshamrani, and K. Al-Begain, "Simulation-Based Study of Distributed Denial of Service Attacks Prevention in the Cloud," Proc. - NGMAST 2015 9th Int. Conf. Next Gener. Mob. Appl. Serv. Technol., pp. 60–65, (2016).

N. C. S. N. Iyengar and G. Ganapathy, "Chaotic theory based defensive mechanism against distributed Denial of Service Attack in cloud computing environment," Int. J. Secure. its Appl., vol. 9, no. 9, pp. 197–212, (2015).