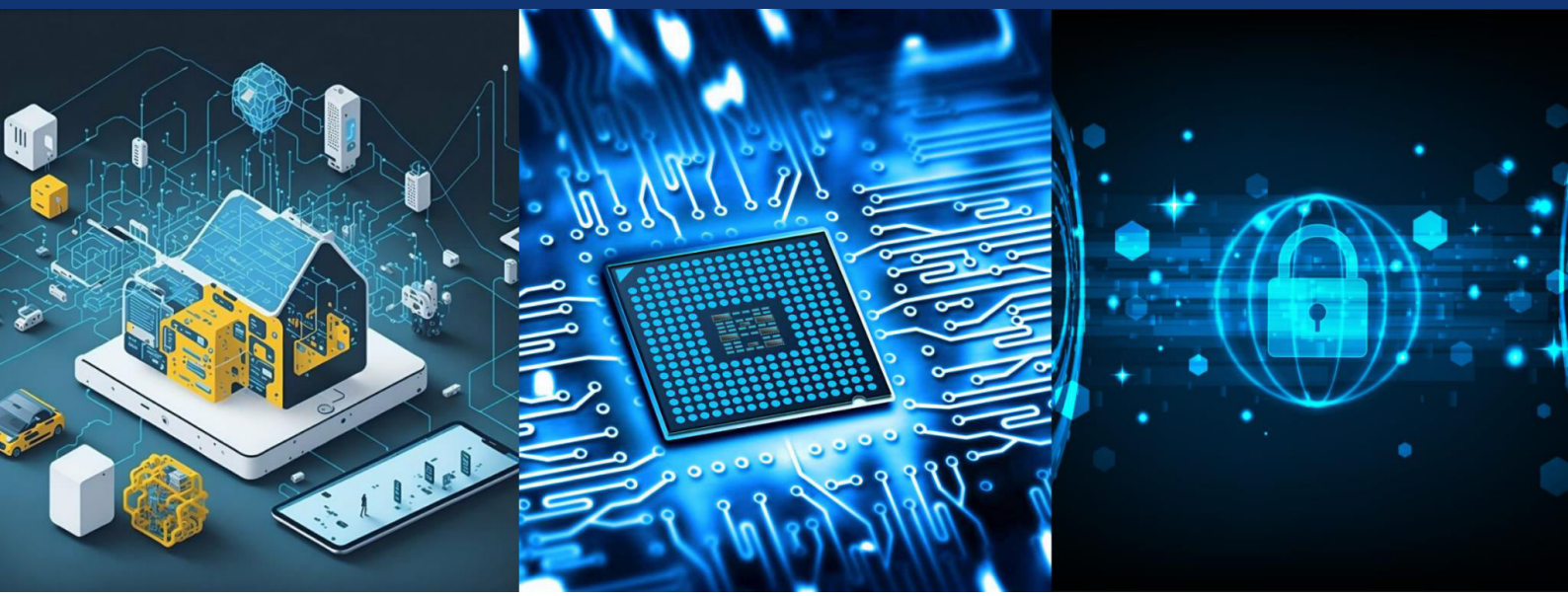
IJIRCCE

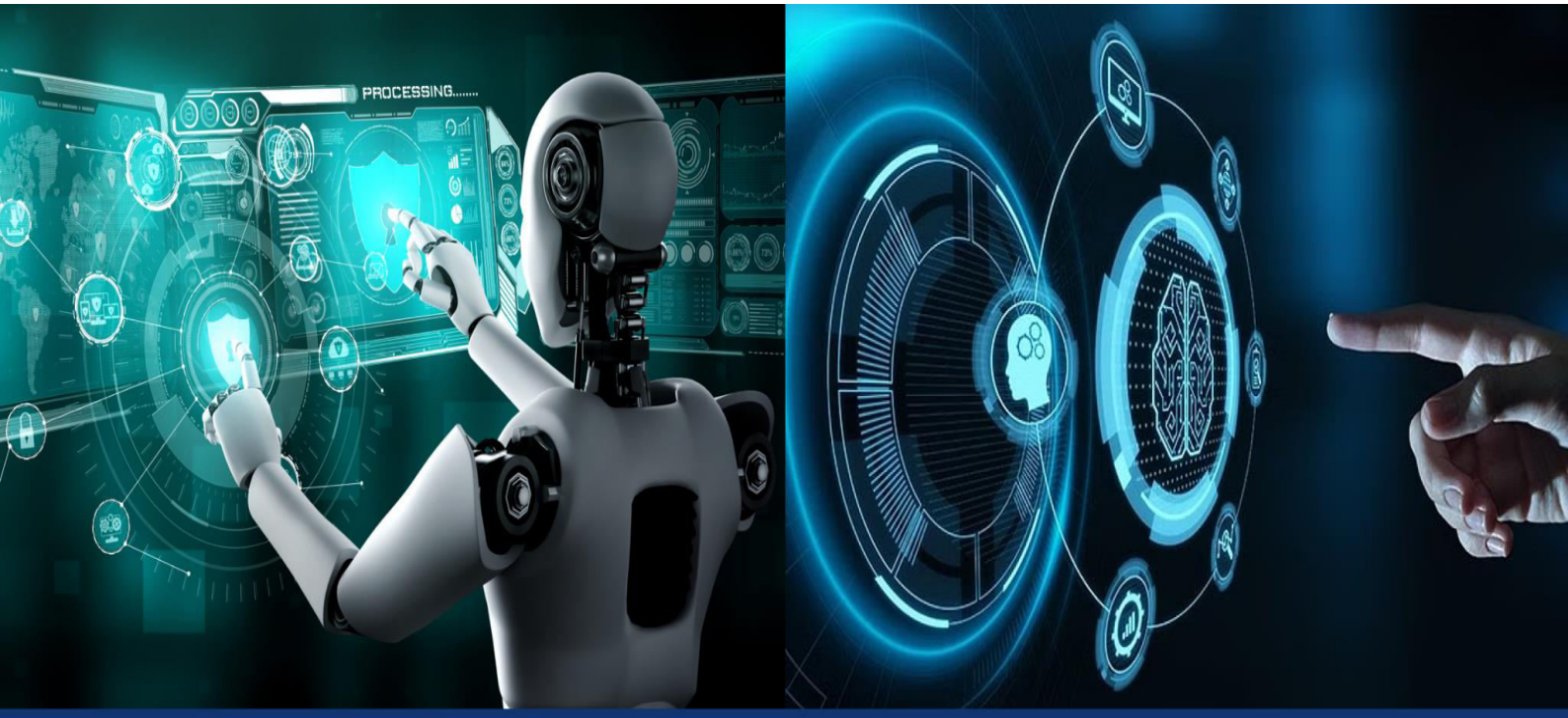
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407028

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Machine Learning-Based DDoS Detection for Network Slicing in Next-Generation Networks

Deshapathi Sathwik Sharma, Dr. M. Dhanalakshmi

Post Graduate Student, Department of Computer Science and Engineering, Computer Networks and Information Security, Jawaharlal Nehru Technological University, Hyderabad, India

Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, India

ABSTRACT: A key feature of 5G and upcoming 6G networks is network slicing, which allows several services with various performance needs to run on shared infrastructure. Nevertheless, it is susceptible to Distributed Denial of Service assaults, which can impair network availability and performance. The CIC-DDoS2019 dataset, which includes both normal and attack traffic records, is used in this investigation. A Random Forest classifier is used to precisely identify fraudulent traffic following data preparation, feature selection, and traffic analysis. A slice-aware Moving Target Defense mechanism finds impacted slices and uses mitigation techniques such traffic rerouting, slice isolation, IP shuffling, port modification, and dynamic resource allocation to improve network resilience and guarantee availability and service continuity.

KEYWORDS: Network Slicing, Moving Target Defense, Network resilience.

I. INTRODUCTION

The rapid evolution of fifth-generation (5G) and emerging sixth-generation (6G) communication networks has transformed the way data is transmitted, processed, and accessed. Numerous applications, including the Internet of Things (IoT), smart cities, industrial automation, driverless cars, and real-time multimedia services, are supported by these sophisticated networks. Network slicing has become a crucial technology that allows several virtual network instances to function independently on a common physical infrastructure in order to effectively handle a variety of service requirements. In order to ensure effective resource use and service delivery, each network slice is built to satisfy particular performance, latency, and bandwidth requirements.

Network slicing presents a number of security risks despite its benefits. The Distributed Denial of Service attack, which can overload network resources with malicious traffic and result in service disruption and decreased network availability, is one of the biggest dangers. The network's overall performance may be impacted by such attacks, which may target a single slice or spread to several slices.

By examining network traffic patterns and differentiating between benign and malevolent activity, machine learning techniques have emerged as useful instruments for detecting cyber threats. Compared to conventional security measures, these strategies allow for faster and more precise attack detection.

This paper proposes a machine learning-based method for DDoS detection in network slicing scenarios using the dataset. Traffic is categorized as either regular or attack traffic using a Random Forest classifier. A slice-aware Moving Target Defense mechanism is incorporated to detect impacted slices and implement adaptive mitigation techniques in order to improve network resilience. In next-generation communication networks, the suggested framework enhances security, service availability, and dependability.

II. RELATED WORK

With the ability to create multiple virtualized network slices over a shared physical infrastructure, network slicing has become a fundamental technology in next-generation 5G and emerging 6G communication networks. This approach

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407028

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

improves resource utilization, service customization, and operational flexibility by allowing different applications to operate with specific performance requirements. To enhance efficiency and adaptive resource management, Andreou and Mavromoustakis proposed an intelligent network slicing framework based on Multi-Agent Deep Deterministic Policy Gradient (MADDPG) techniques. The framework employs multiple reinforcement learning agents that continuously monitor network conditions and dynamically allocate resources among network slices.

In the proposed architecture, each learning agent independently determines optimal resource allocation strategies based on traffic patterns, service demands, and environmental conditions. By leveraging deep reinforcement learning, the system can adapt to changing network requirements without relying on predefined rules or manual intervention. Experimental results presented by the authors indicate improvements in service quality, resource utilization, and operational efficiency across heterogeneous network environments. These capabilities make the framework suitable for managing complex next-generation communication infrastructures.

Despite these advantages, the proposed architecture primarily focuses on resource optimization and network management rather than cybersecurity. The study does not provide a dedicated mechanism for detecting or mitigating Distributed Denial of Service (DDoS) attacks targeting specific network slices. Furthermore, it lacks slice-level threat identification and does not address the impact of malicious traffic on service availability. To overcome these limitations, the proposed work introduces a Machine Learning-based DDoS detection framework that combines Random Forest-based traffic classification with slice-aware monitoring and Moving Target Defense (MTD) techniques. This approach enables accurate attack detection, improves network security and resilience, and maintains service continuity across unaffected network slices.

III. PROPOSED ALGORITHM

A. *System Architecture:*

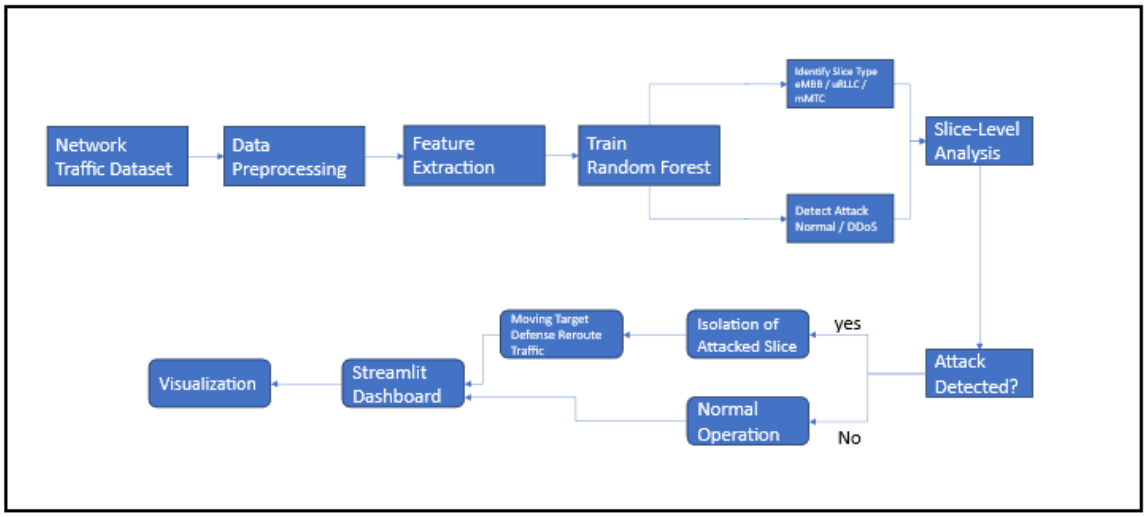


Fig. 1. Proposed System Architecture

B. *Design Considerations:*

- The DDoS detection model is trained and tested using the CIC-DDoS2019 dataset.
- Both benign and malicious traffic examples can be found in network traffic records.
- Missing values, superfluous attributes, and inconsistent records are eliminated by data preprocessing.
- To enhance categorization performance, significant network traffic characteristics are used.
- Random Forest was selected because of its excellent accuracy, resilience, and capacity to manage massive amounts of network traffic data.
- There are three types of network slices: URLLC (Ultra-Reliable Low Latency Communication), mMTC (Massive Machine Type Communication), and eMBB (Enhanced Mobile Broadband).

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Only when malicious traffic is identified are Slice-Aware Moving Target Defense (MTD) methods triggered.
- Through a Streamlit dashboard, the technology is intended to offer real-time attack detection and visualization.

C. *Description of the Proposed Algorithm:*

In order to preserve network availability and security, the suggested technique aims to precisely identify Distributed Denial of Service (DDoS) threats in network slicing scenarios and produce adaptive defense measures. There are five main steps in the suggested algorithm.

Step 1: Data Preprocessing:

The CIC-DDoS2019 dataset is loaded and preprocessed. Missing values, duplicate records, and irrelevant features are removed. The dataset is then normalized and transformed into a format suitable for machine learning analysis.

Let,

D = {x1, x2, x3, ..., xn}

where D represents the preprocessed network traffic dataset consisting of n traffic records.

Step 2: Feature Selection and Model Training:

Relevant traffic features are selected and used to train the Random Forest classifier. Multiple decision trees are constructed using random subsets of training samples and features.

The final prediction is determined using majority voting:

Prediction = Mode(T1, T2, T3, ... , Tn) eq. (1)

where T1, T2, ... , Tn represent the predictions generated by individual decision trees.

Step 3: DDoS Attack Detection:

The trained Random Forest model analyzes incoming traffic records and classifies them as either Benign or Attack.

Attack Status = RF(X) eq. (2)

where RF represents the Random Forest classifier and X represents the input traffic feature vector.

If Attack Status = 0 → Benign Traffic

If Attack Status = 1 → DDoS Attack

Step 4: Slice Identification:

When malicious traffic is detected, the system identifies the affected network slice based on traffic characteristics and service requirements.

Slice = {eMBB, mMTC, URLLC} eq. (3)

The slice with the highest concentration of attack traffic is marked as the affected slice.

Step5: Moving Target Defense Response:

After identifying the affected slice, the Slice-Aware Moving Target Defense (MTD) engine generates suitable defense actions.

Defense Response = {Slice Isolation, Traffic Rerouting, IP Shuffling, Port Modification, Resource Reallocation} eq. (4)

These adaptive mitigation strategies reduce attack impact, improve resilience, and maintain service continuity across the network.

IV. PSEUDO CODE

Step 1: Load the CIC-DDoS2019 dataset containing both benign and DDoS attack traffic records.

Step 2: Perform data preprocessing by:

- Removing missing and duplicate values.
- Eliminating irrelevant features.
- Converting categorical attributes into numerical format.
- Normalizing selected features for better model performance.

Step 3: Separate the dataset into input features (X) and target labels (Y).

Step 4: Split the dataset into training and testing datasets.

Step 5: Perform feature selection to identify the most significant traffic attributes contributing to DDoS detection.

Step 6: Initialize the Random Forest classifier with suitable hyperparameters.

Step 7: Train the Random Forest model using the training dataset.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Step 8: Test the trained model using the testing dataset.
Step 9: Calculate performance metrics such as Accuracy, Precision, Recall, F1-Score, ROC-AUC Score, and Confusion Matrix.
Step 10: Upload or receive new network traffic data for analysis.
Step 11: Apply the same preprocessing and feature transformation steps to the incoming traffic data.
Step 12: Pass the processed traffic data to the trained Random Forest classifier.
Step 13: Predict the traffic class.
IF Prediction = Benign
    Display "Normal Network Traffic"
    Continue Monitoring
ELSE
    Display "DDoS Attack Detected"
    Proceed to Slice Analysis
Step 14: Analyze attack traffic characteristics and identify the affected network slice.
IF Traffic Pattern corresponds to eMBB
    Affected Slice ← eMBB
ELSE IF Traffic Pattern corresponds to mMTC
    Affected Slice ← mMTC
ELSE
    Affected Slice ← URLLC
Step 15: Activate Slice-Aware Moving Target Defense (MTD) mechanism.
Step 16: Generate appropriate defense actions such as:

- Slice Isolation
- Traffic Rerouting
- IP Address Shuffling
- Port Modification
- Dynamic Resource Reallocation

Step 17: Display attack statistics, affected slice information, model performance metrics, and defense responses on the Streamlit dashboard.
Step 18: Store analysis results for future monitoring and model improvement.
Step 19: Continue monitoring incoming traffic for new attack events.
Step 20: End.
.

V. SIMULATION RESULTS

The proposed Machine Learning-Based DDoS Detection Framework was implemented using Python and evaluated using the CIC-DDoS2019 dataset. The dataset contains both benign and malicious network traffic records, which were preprocessed and analyzed using the Random Forest classifier. The model was trained and tested to accurately classify network traffic as either normal or attack traffic. Performance evaluation was carried out using standard metrics such as Accuracy, Precision, Recall, and F1-Score. The experimental results indicate that the Random Forest model achieved high detection accuracy while maintaining low false positive and false negative rates, demonstrating its effectiveness in identifying DDoS attacks within network slicing environments.

In addition to attack detection, the proposed framework incorporates a Slice-Aware Moving Target Defense (MTD) mechanism to improve network security and resilience. Once malicious traffic is detected, the system identifies the affected network slice and generates suitable mitigation actions such as slice isolation, traffic rerouting, IP address shuffling, port modification, and dynamic resource allocation. The Streamlit-based dashboard provides interactive visualization of traffic analysis, attack statistics, model performance metrics, and defense responses. The overall results demonstrate that the proposed framework effectively enhances service availability, network reliability, and cybersecurity protection in next-generation 5G and 6G network slicing architectures.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407028

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A. Evaluation and Interpretation of System Interfaces:

Fig.2. Home Page

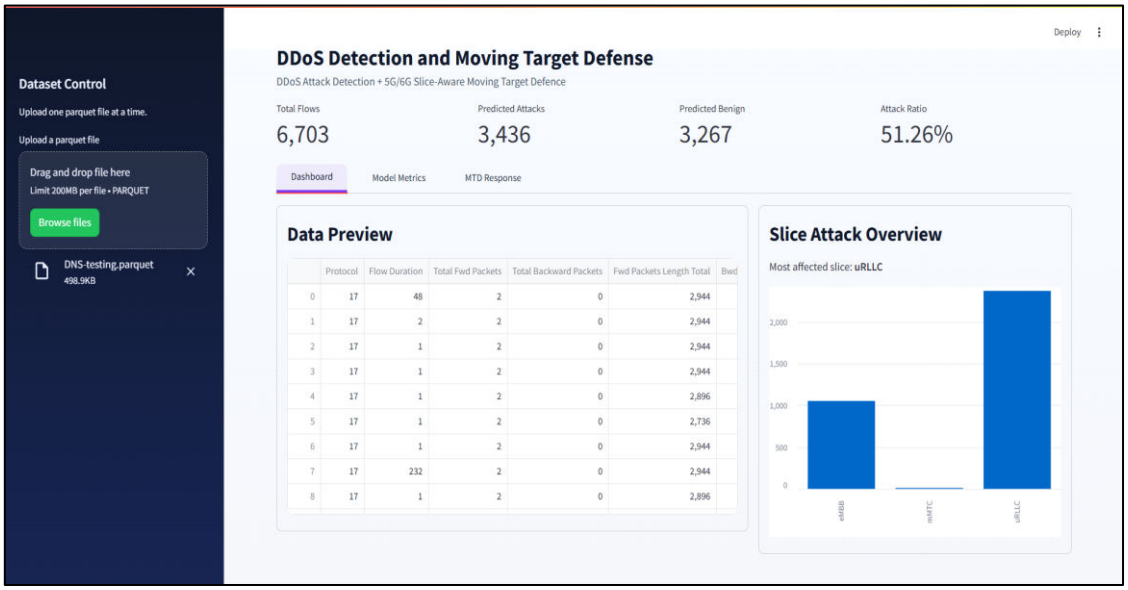


Fig.3. Dashboard After Dataset Upload

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407028

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

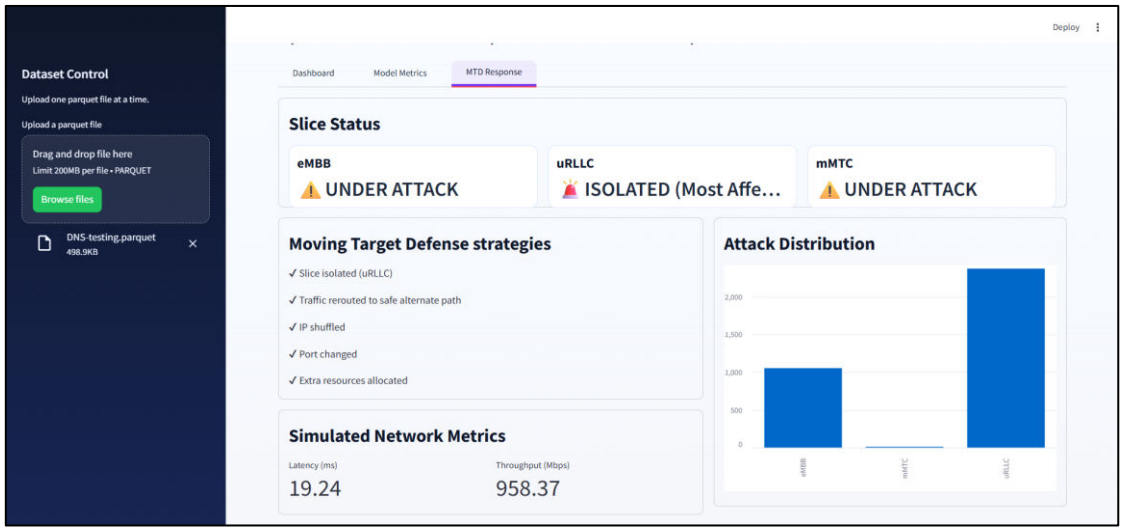


Fig.4. Moving Target Defence (MTD) Response and Slice Status

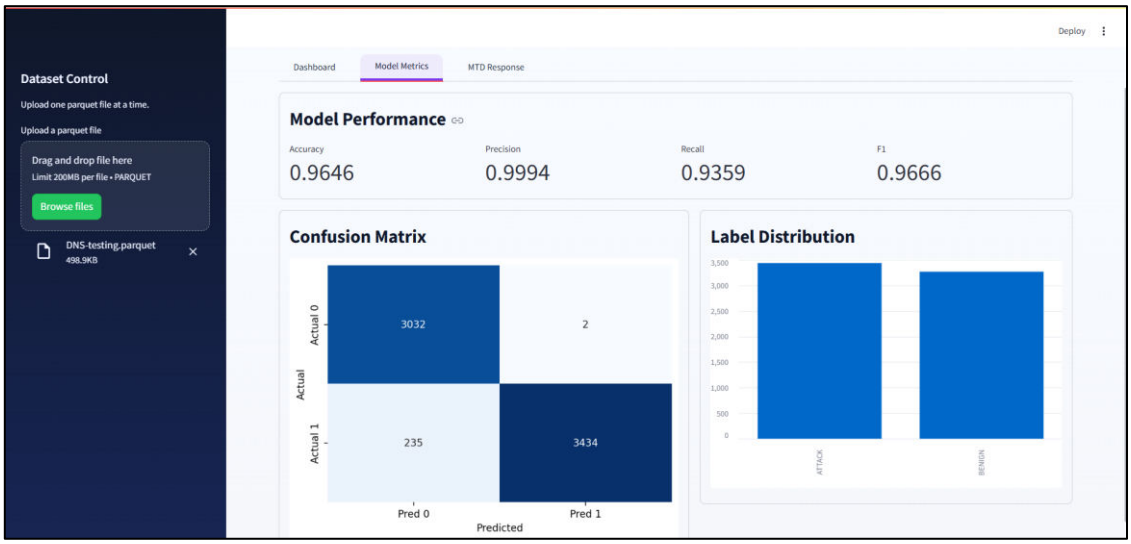


Fig.5. Model Performance Metrics

B. Metrics for Evaluation:

The performance of the proposed Machine Learning-Based DDoS Detection Framework is evaluated using standard classification metrics including Accuracy, Precision, Recall, F1-Score, and ROC-AUC. These metrics help assess the effectiveness of the Random Forest classifier in distinguishing between benign network traffic and DDoS attack traffic.

Let:
TP = True Positives (correctly identified DDoS attacks)
TN = True Negatives (correctly identified benign traffic)
FP = False Positives (benign traffic incorrectly classified as DDoS attacks)
FN = False Negatives (DDoS attacks incorrectly classified as benign traffic)

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Accuracy:

Accuracy represents the proportion of correctly classified traffic instances to the total number of traffic instances analyzed. It measures the overall effectiveness of the model in identifying both benign and malicious traffic.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad \text{eq. (5)}$$

Precision:

Precision is the ratio of correctly predicted attack instances to the total number of instances predicted as attacks.

$$\text{Precision} = \frac{TP}{TP + FP} \quad \text{eq. (6)}$$

Recall :

Recall measures the proportion of actual attack instances that are correctly detected by the model.

$$\text{Recall} = \frac{TP}{TP + FN} \quad \text{eq. (7)}$$

F1-Score:

The F1-Score is the harmonic mean of Precision and Recall and provides a balanced evaluation of the classifier's performance.

$$\text{F1Score} = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad \text{eq. (8)}$$

VI. CONCLUSION AND FUTURE WORK

The proposed Machine Learning-Based DDoS Detection Framework effectively identifies malicious network traffic in network slicing environments using the Random Forest algorithm and the CIC-DDoS2019 dataset. The system accurately classifies traffic as benign or attack traffic and enhances network security through a Slice-Aware Moving Target Defense (MTD) mechanism. The generated defense actions help maintain service availability and network resilience in 5G and future 6G networks. Experimental results demonstrate high detection performance and reliable attack mitigation. Future work includes integrating deep learning models, real-time traffic monitoring, SDN-based deployment, and larger datasets to further improve scalability and detection accuracy.

REFERENCES

1. Andreou, A., and C. X. Mavromoustakis, "6G+ Networks Through Enhanced Efficiency and Sustainability with MADDPG-Driven Network Slicing in SOS Environments," IEEE Transactions on Green Communications and Networking, vol. 8, pp. 1752–1761, 2024.
2. De Alwis, C., P. Porambage, P. Dev, T. R. Gadekallu, and M. Liyanage, "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions," IEEE Communications Surveys & Tutorials, vol. 26, no. 1, pp. 534–570, 2024.
3. Alajlan, R., M. M. Hafizur Rahman, M. Al-Naeem, and M. A. Almaiah, "A Literature Review on Cybersecurity Risks and Challenges Assessments in Virtual Power Plants: Current Landscape and Future Research Directions," IEEE Access, vol. 12, pp. 188813–188827, 2024.
4. Li, C., P. Zheng, Y. Yin, B. Wang, and L. Wang, "Deep Reinforcement Learning in Smart Manufacturing: A Review and Prospects," CIRP Journal of Manufacturing Science and Technology, vol. 40, pp. 75–101, 2023.
5. Tan, J., H. Jin, H. Zhang, Y. Zhang, D. Chang, X. Liu, and H. Zhang, "A Survey: When Moving Target Defense Meets Game Theory," Computer Science Review, vol. 48, p. 100544, 2023.
6. Bauerle, N., "Mean Field Markov Decision Processes," Applied Mathematics and Optimization, 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details