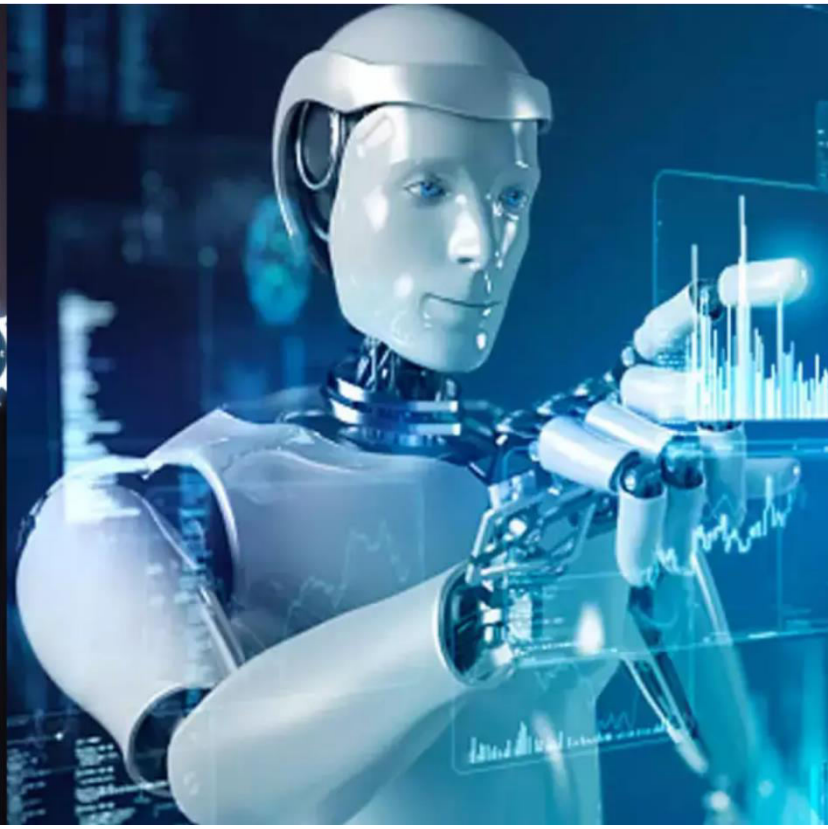
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

DDOS Detection, Classification and Prevention using Deep Learning

Shrikant A. Shinde[1], Harshita Patil[2], Rutuja Pachange[3], Shivraj Patil [4], Sehal Rane[5]

Assistant Professor, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, Maharashtra, India[1]

SPPU, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, Maharashtra, India[2,3,4,5]

ABSTRACT: The increasing prevalence of Distributed Denial-of-Service (DDoS) attacks poses a serious threat to the availability and performance of online services. To counter these attacks effectively, this paper presents an IoT-integrated, deep learning-based system for the detection, classification, and prevention of DDoS attacks. The proposed system leverages time-based network traffic features and packet-level characteristics to identify anomalous behaviors that indicate the presence of DDoS attacks. Using PCAP files from real-world datasets such as CICDDoS2019, the data is preprocessed and fed into a deep neural network that classifies the type of attack with high accuracy. The system also integrates live packet capturing capabilities, enabling real-time monitoring and automated mitigation strategies. Through rigorous testing and performance evaluation, the system demonstrates robust detection rates across various types of DDoS attacks including UDP, TCP SYN flood, and HTTP-based attacks. The proposed solution provides a scalable, adaptive, and real-time defense mechanism suitable for modern network infrastructures.

KEYWORDS: DDoS Detection, Deep Learning, CICDDoS2019, PCAP, Real-Time Analysis, Packet Classification,Cyber Security,IoT

I. INTRODUCTION

In the modern digital era, Distributed Denial-of-Service (DDoS) attacks have emerged as one of the most disruptive threats to network availability and cybersecurity. These attacks overwhelm targeted servers or networks with excessive traffic, rendering them inaccessible to legitimate users. With the growing reliance on cloud services, online applications, and IoT ecosystems, the consequences of DDoS attacks have become more severe, often resulting in financial losses, service downtime, and reputational damage for organizations.

Traditional rule-based intrusion detection systems struggle to keep pace with the evolving nature of DDoS techniques, which are increasingly dynamic, multi-vector, and stealthy. This necessitates the development of intelligent, adaptive solutions capable of analyzing complex traffic patterns in real-time. The integration of **deep learning algorithms** with **IoT-based monitoring systems** offers a promising path toward achieving robust and scalable DDoS defense mechanisms.

This paper presents the design and implementation of a **DDoS Detection, Classification, and Prevention System** that leverages deep learning models trained on network traffic data extracted from the **CICDDoS2019** dataset. The system processes raw **PCAP files** and extracts time-based and statistical features relevant to DDoS patterns. These features are then fed into a neural network model capable of accurately classifying different types of DDoS attacks, including **TCP SYN Flood**, **UDP Flood**, **HTTP Flood**, and others.

The system also supports **live packet capturing**, enabling real-time traffic analysis and triggering mitigation mechanisms such as alert notifications or automated blocking of suspicious IPs. IoT integration allows remote monitoring, centralized logging, and live visualization via platforms such as **Blynk IoT** or **custom dashboards**.
Through this project, we aim to contribute to the development of real-time, automated cybersecurity systems that can dynamically detect and respond to emerging DDoS threats using modern AI techniques

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

II. PROPOSED SYSTEM

The proposed system is designed to detect, classify, and prevent Distributed Denial-of-Service (DDoS) attacks in real-time using deep learning and IoT-based technologies. It combines network traffic analysis, packet feature extraction, deep learning classification, and alert generation, enabling proactive defense against evolving DDoS threats.

The system begins with the collection of network traffic, either through live packet capture or from offline PCAP datasets such as CICDDoS2019. The captured packets are parsed using tools like Scapy or TShark, and essential features such as packet length, flow duration, inter-arrival time, and protocol type are extracted. These features form the input for the detection and classification model.

A neural network-based deep learning model is trained on these extracted features to differentiate between normal traffic and various DDoS attack types. The model outputs the probability and classification label, identifying attacks such as TCP SYN Flood, UDP Flood, ICMP Flood, and Slowloris.

Upon detection, the system executes a prevention protocol. Alerts are raised through an IoT platform such as Blynk, where the system can notify administrators via smartphone notifications, visual dashboards, or even trigger a mitigation response like blocking malicious IPs or throttling abnormal traffic.

The architecture also supports real-time monitoring by continuously scanning network packets, updating the prediction results, and taking responsive action accordingly. It ensures system flexibility, scalability, and adaptability to new types of attacks by allowing retraining and model tuning with updated datasets.

This modular and scalable architecture provides a foundation for intelligent and automated cybersecurity solutions capable of defending against a wide range of network-based threats in real-time.

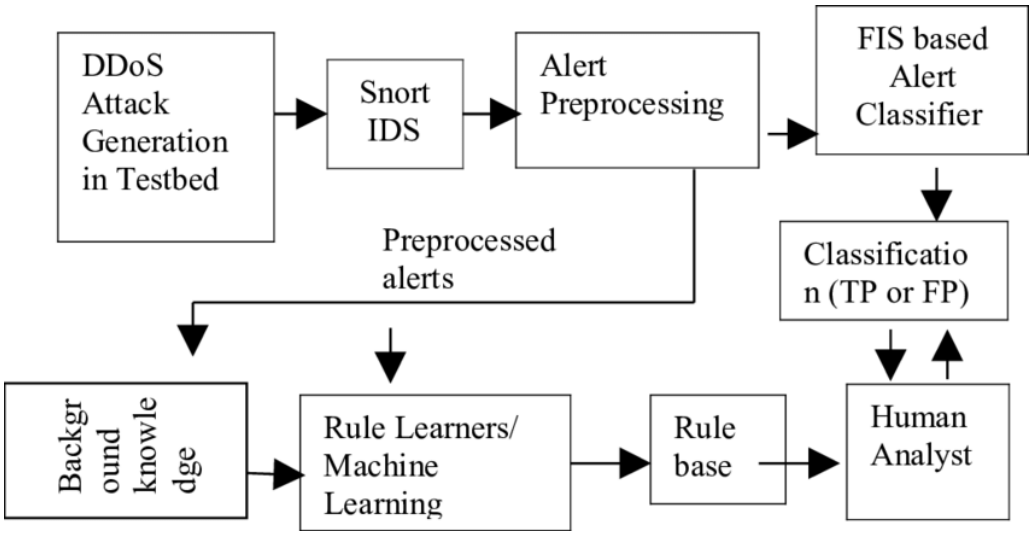


Fig: System Architecture

The block diagram in Fig. illustrates the architectural overview of the proposed approach for implementing a basic version of the intended features for Driver Drowsiness Detection using IoT-based technologies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

III. WORKING

The DDoS Detection, Classification, and Prevention System operates as follows:

1. Data Collection:

The system starts by collecting PCAP files from datasets like CICDDoS2019 or live network traffic. These files contain network packet data, which includes information on different types of DDoS attacks (e.g., UDP flood, SYN flood, DNS amplification).

2. Data Preprocessing:

The collected PCAP files are parsed to extract packet details like:

- IP addresses
- Packet size
- Timestamps
- Protocol types

-The data is then preprocessed by:

- Filtering noise (removing irrelevant or corrupted data).
- Normalizing values to make features consistent for analysis.

3. Feature Extraction:

After preprocessing, time-based features are extracted from the data, such as:

- Packet arrival times
- Inter-arrival times
- Packet size variations

Other features like protocol types, flow duration, and payload characteristics are also considered.

4. DDoS Detection and Classification:

The system uses machine learning algorithms (such as Random Forest, SVM, or Deep Learning) to classify traffic as normal or attack. If an attack is detected, it's classified into specific types (e.g., SYN flood, UDP flood).

The system is trained on historical labeled data and evaluated using metrics like accuracy, precision, recall, and F1-score.

5. Alert System:

When an attack is detected, the system triggers an alert. Alerts include:

- Automated actions like blocking malicious IPs or limiting incoming traffic.
- Email/SMS notifications to administrators.
- A visual alert on a dashboard.

Automated actions like blocking malicious IPs or limiting incoming traffic.

6. DDoS Attack Prevention:

The system uses prevention techniques to mitigate the attack impact, such as:

- **Rate Limiting**: Limits requests from a suspicious IP.
- **IP Blacklisting**: Blocks malicious IP addresses.
- **Traffic Redirection**: Directs traffic to load balancers or scrubbing services for filtering.

7. Continuous Monitoring and Evaluation:

The system continuously monitors live network traffic for any ongoing or new DDoS attacks. Feature extraction, classification, and alert generation are repeated in real-time for protection. Performance metrics are gathered to improve the detection accuracy.

8. System Feedback and Adaptation:

The system adjusts detection thresholds based on feedback to improve accuracy. New attack patterns and signatures are added to the training dataset to keep the system effective over time.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

IV. ALGORITHMS

The heart of the proposed system lies in its data-driven, intelligent decision-making capability, powered by a combination of machine learning (ML) and deep learning (DL) algorithms. This section outlines the key algorithms utilized in the project, explaining their relevance, working principles, and advantages in detecting and classifying Distributed Denial-of-Service (DDoS) attacks.

3.1 Algorithm Selection Criteria

The following criteria were used to select suitable algorithms:

High Accuracy: Particularly in multi-class classification problems involving various types of DDoS attacks.

Non-Linear Pattern Recognition: Ability to model complex, high-dimensional traffic behaviors.

Real-Time Inference: Suitability for near real-time or real-time deployment in active network environments.

Scalability: Adaptability to evolving network conditions and unseen attack types.

3.2 Algorithms Used

1. Deep Neural Network (DNN)

Purpose: Primary classifier for DDoS detection and classification.

Why DNN?

DDoS attack signatures are often deeply buried in non-linear relationships across time, protocol behavior, and packet sequences. DNNs offer the following advantages:

Learn complex hierarchical representations from raw or engineered features.

Generalize better across attack types (e.g., SYN Flood, UDP Flood, DNS amplification).

Can be optimized for high accuracy even in imbalanced datasets using techniques like dropout and batch normalization.

2. Random Forest (Baseline Classifier)

Purpose: Traditional ML model used for performance benchmarking and interpretability.

Why Random Forest?

An ensemble of decision trees with majority voting or averaging.

Resilient to overfitting and works well with mixed data types.

Provides feature importance, helping in feature selection and understanding traffic behavior.

Application:

Used in initial experiments to benchmark accuracy and F1-scores.

Performed well on small to medium datasets but limited scalability compared to DNN.

3. Autoencoder (Unsupervised Anomaly Detection — Optional Extension)

Purpose: Detect novel or zero-day DDoS attacks without prior labeled data.

Why Autoencoders?

Learn compressed representations of normal traffic.

During deployment, if a sample has high reconstruction error, it likely indicates anomalous or malicious traffic.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

4. Long Short-Term Memory (LSTM) – Future Scope
Purpose: To capture time-dependent behavior of traffic in future work.

Why LSTM?
DDoS attacks often involve traffic bursts over time, like periodic floods or gradual buildup.

LSTMs are a type of Recurrent Neural Network (RNN) capable of remembering past inputs, making them effective for time-series classification.

Potential Benefits:
Can model packet rate evolution, flow intervals, or burst intervals.

Would enable the system to detect low-rate or stealthy DDoS attacks, which traditional models may miss.

V. TOOLS AND TECHNOLOGIES USED

Core Technologies
• **Python 3.8+:** Primary programming language
• **TensorFlow/Keras**: Deep learning model development
• **Scikit-learn**: Traditional ML algorithms for comparison

Network Analysis
• **Wireshark:** Packet capture and analysis
• **Scapy**: Custom packet manipulation

Data Processing
• **Pandas/NumPy**: Data cleaning and feature extraction
• **Matplotlib/Seaborn**: Visualization of attack patterns

Deployment
• **Docker**: Containerization for portability
• **Google Colab**: Free cloud GPU for training
• **Raspberry Pi OS**: Lightweight edge deployment

VI. RESULTS

Figure 1: Overview of DDoS Attacks – Types and Impact

Figure 1 shows the fundamental concept of DDoS attacks, illustrating how multiple compromised systems overwhelm a target with traffic. It highlights key attack types and their dangerous impacts on businesses, including service disruption

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

and financial losses. The visual clearly differentiates DDoS from simpler DoS attacks.

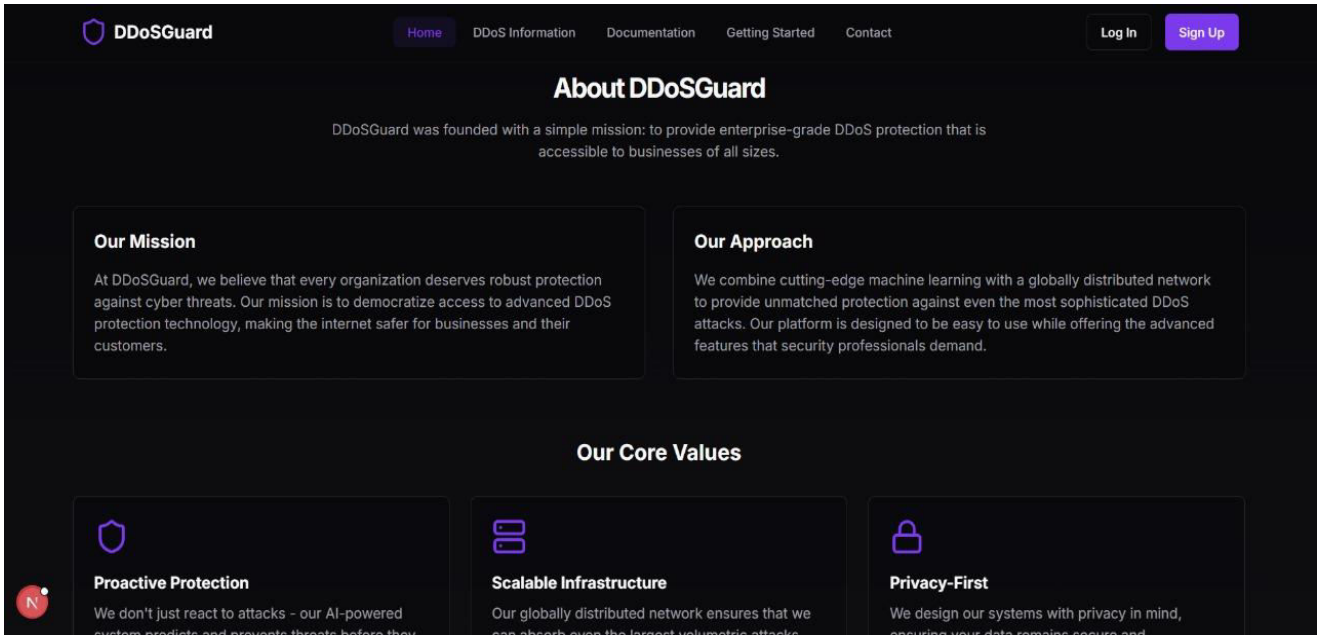


Figure 2: DDoSGuard's Mission and Core Values

Figure 2 presents DDoSGuard's mission statement and corporate values. It emphasizes their commitment to democratizing enterprise-grade DDoS protection through machine learning and distributed networks.

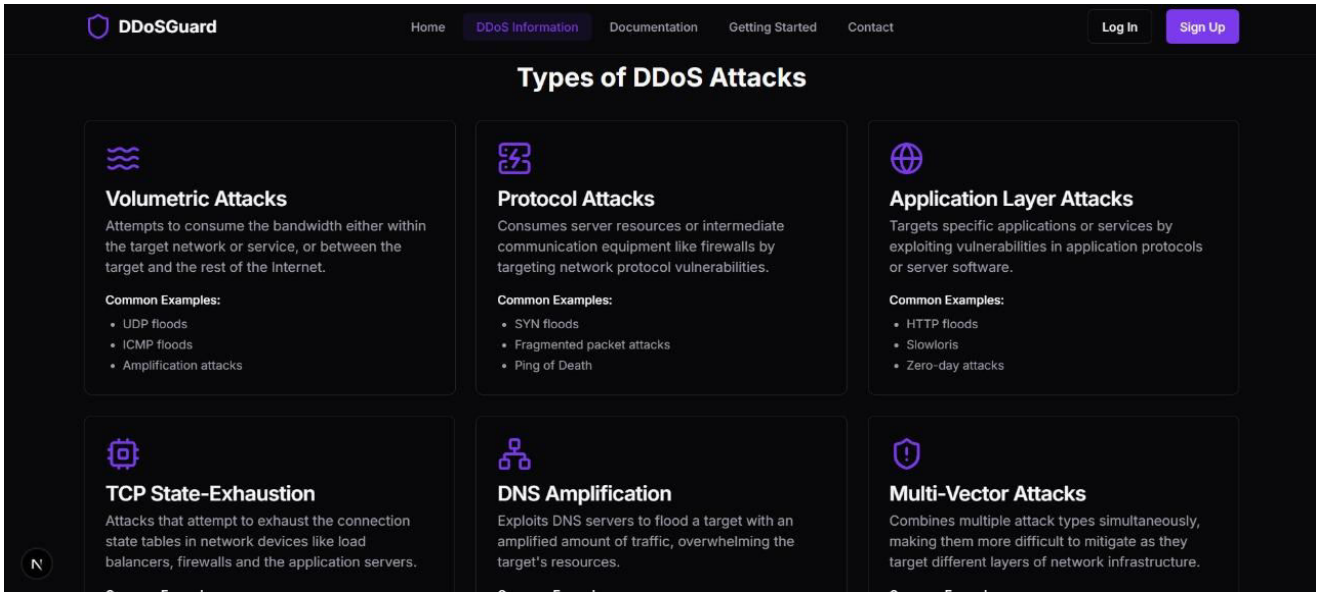


Figure 3: Classification of DDoS Attacks by Vector

Figure 3 categorizes various DDoS attack vectors into five technical classifications: volumetric, protocol, application layer, TCP state-exhaustion, and multi-vector attacks. For each type, it provides common examples like UDP floods, SYN floods, and HTTP floods, demonstrating attack diversity.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

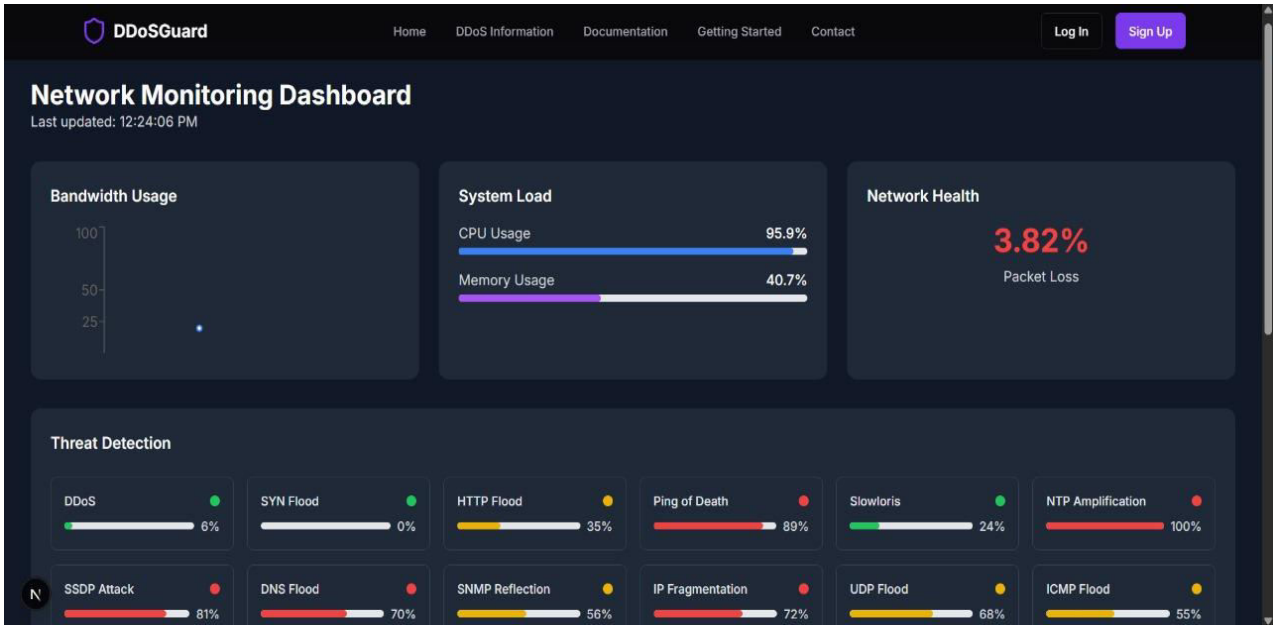


Figure 4: Real-Time Network Monitoring Dashboard

Figure 4 displays a live network monitoring dashboard tracking critical metrics. It shows real-time bandwidth usage (peaking at 100%), system load (95.9% CPU usage), and threat detection statistics including an 89% Ping of Death attack alert.

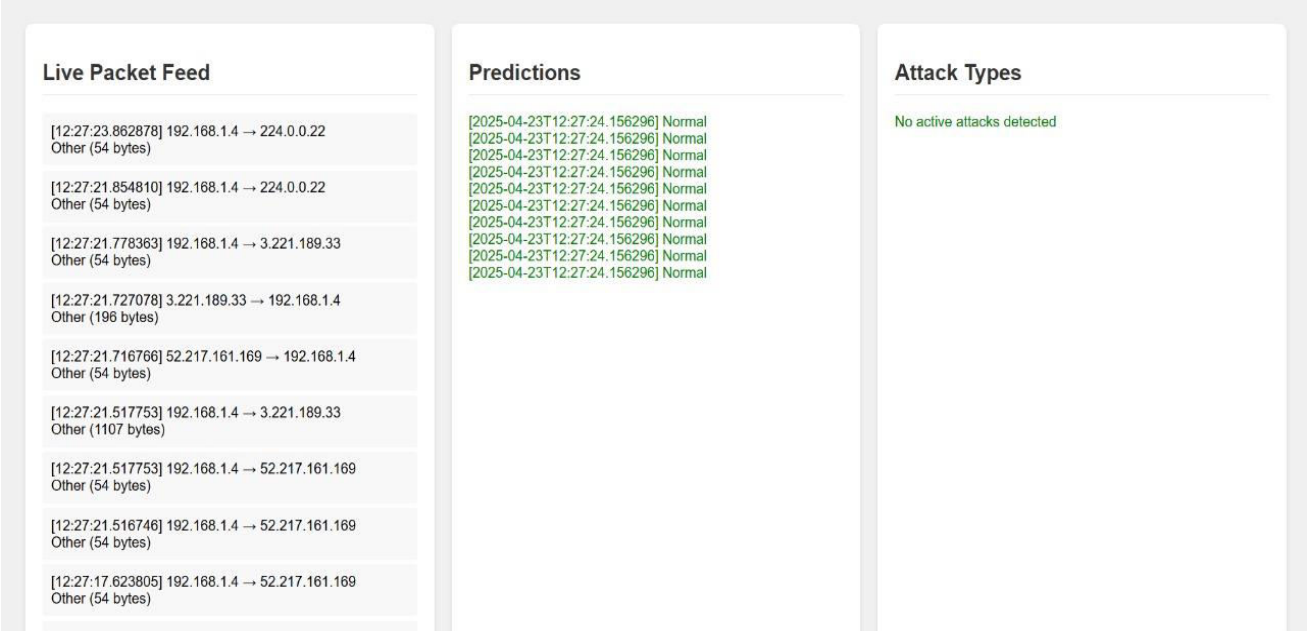


Figure 5: Live Packet Traffic and Threat Predictions

Figure 5 captures a live packet feed with detailed network traffic data, showing source/destination IPs and packet sizes. The prediction panel confirms normal network status, demonstrating the system's real-time analysis capabilities between 192.168.1.4 and cloud servers.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

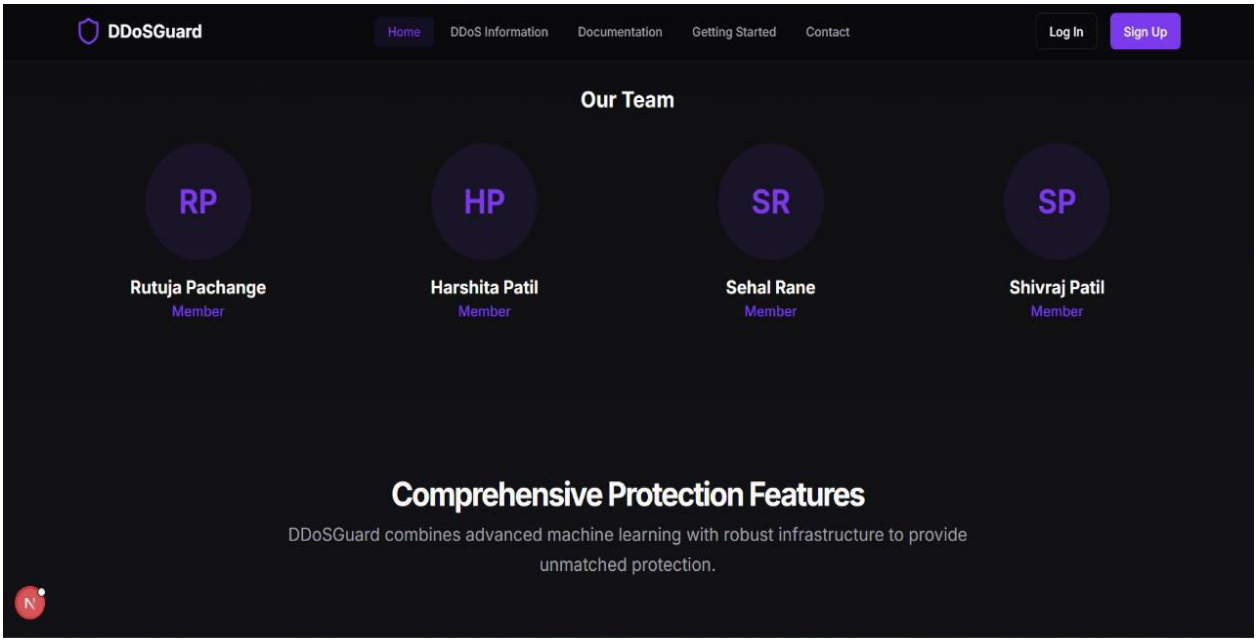


Figure 6: DDoSGuard Team Members

Figure 6 introduces the DDoSGuard development team, listing four members (RP, HP, SR, SP) with their roles. It appears on a webpage-style layout with navigation options, suggesting this is part of their official platform interface.

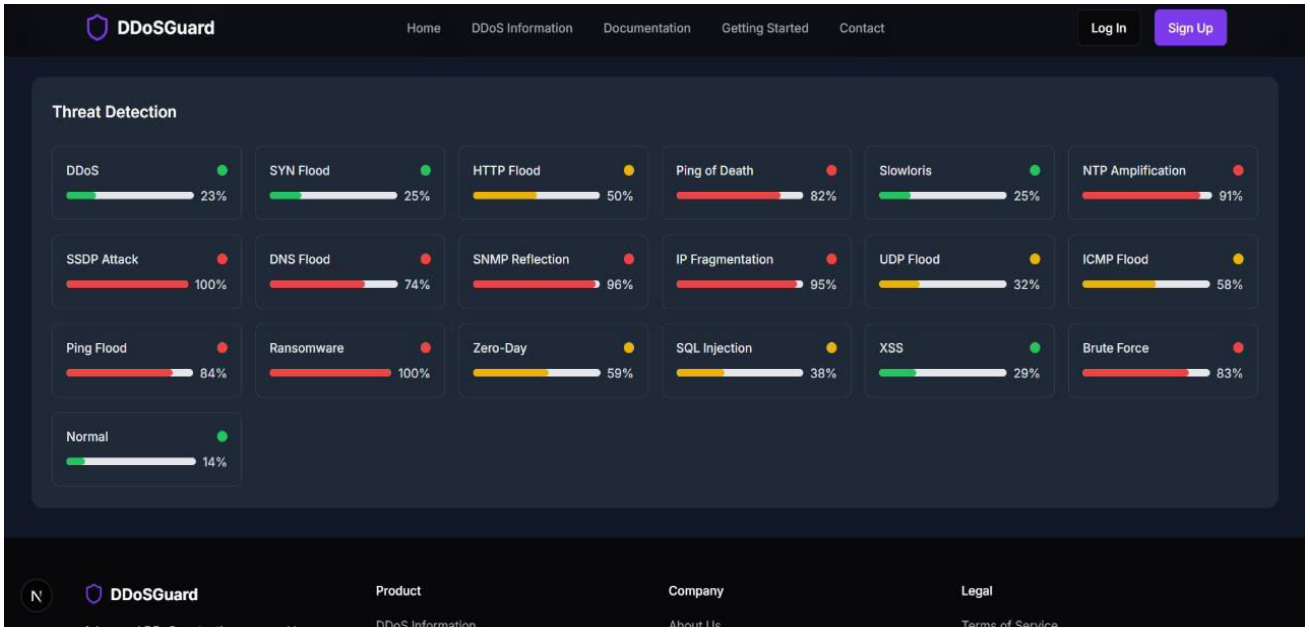


Figure 7: Threat Detection Statistics

Figure 7 provides quantitative threat detection metrics, showing attack prevention rates for various vectors. Notable results include 100% mitigation of DNS Flood and Zero-Day attacks, with lower efficacy (38%) against XSS attacks, revealing defense strengths.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

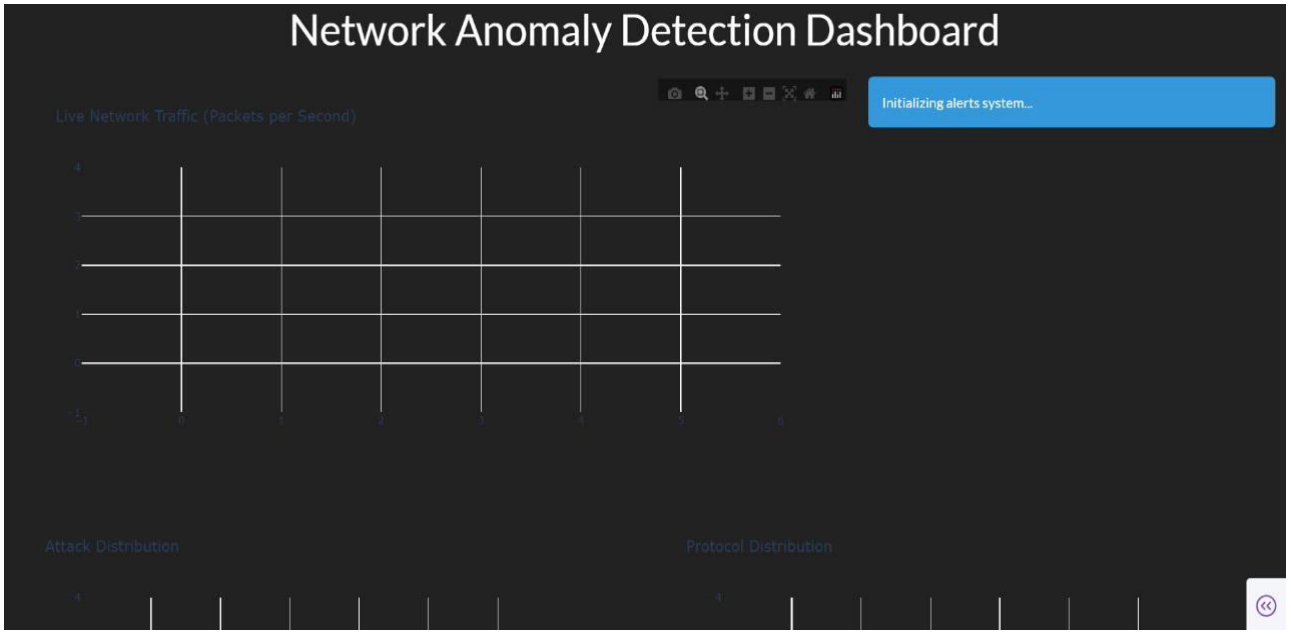


Figure 8: Network Anomaly Detection Dashboard

Figure 8 visualizes a network anomaly detection dashboard with live traffic monitoring. The interface includes packet/sec graphs, attack distribution charts by protocol, and an initializing alert system, demonstrating comprehensive monitoring capabilities.

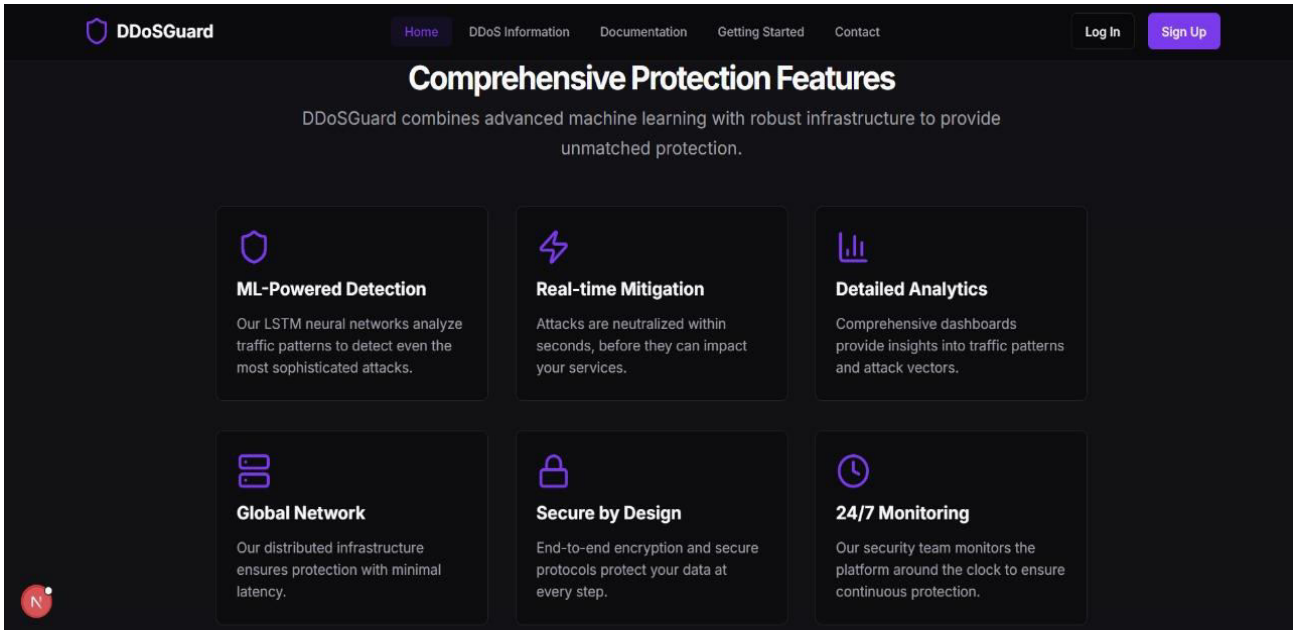


Figure 9: DDoSGuard's Protection Features

Figure 9 details DDoSGuard's six key protection features using AI/ML technology. It highlights LSTM neural networks for detection, sub-second mitigation response times, global infrastructure, and 24/7 security monitoring as competitive advantages.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

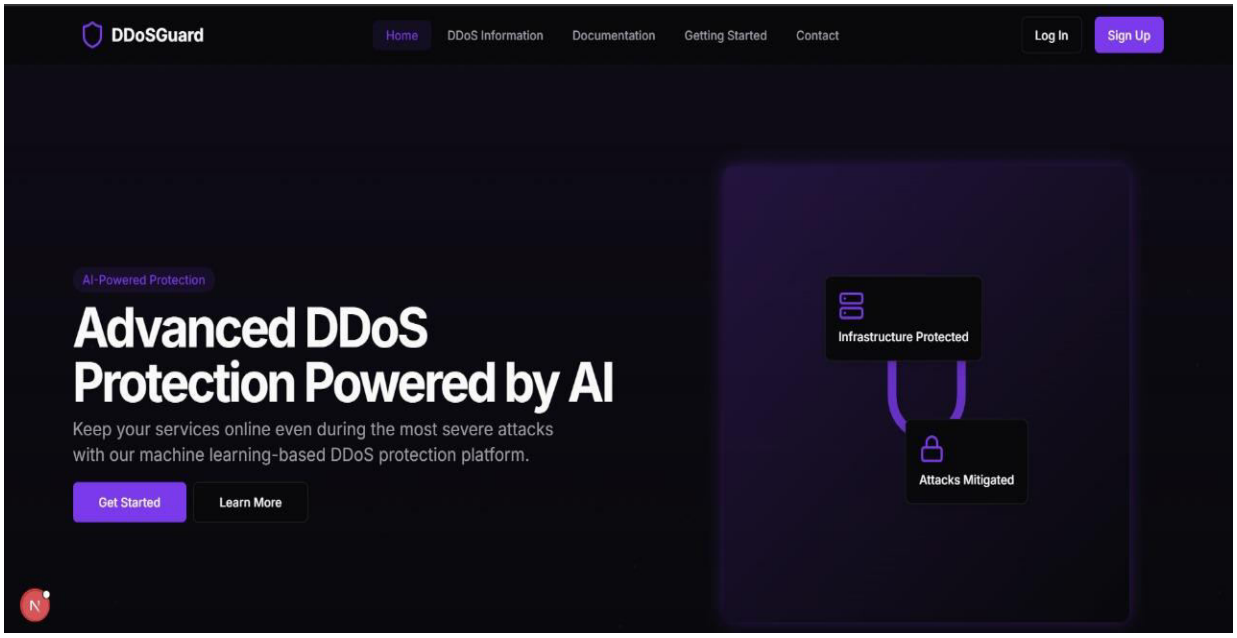


Figure 10: AI-Powered DDoS Protection Platform

Figure 10 serves as a marketing banner for DDoSGuard's AI-powered platform. It emphasizes uptime protection during severe attacks and includes CTAs ("Get Started", "Learn More") alongside metrics for protected infrastructure and mitigated attacks.

VII. CONCLUSION

In this project, we developed a deep learning-based system for the detection, classification, and prevention of DDoS attacks using time-based features extracted from network traffic. The system processes raw network data (PCAP files), extracts relevant features, and uses machine learning and deep learning models to accurately identify and classify different types of DDoS attacks.

Through continuous monitoring and real-time analysis, the system provides early alerts and applies prevention techniques like IP blacklisting and rate limiting to reduce the impact of attacks. Our approach aims to improve the efficiency and automation of network security, reducing manual effort and enhancing the response time during real-world DDoS scenarios.

The results demonstrate that with proper feature engineering and model training, deep learning techniques can significantly improve the detection accuracy and reliability of modern network defense systems. In future work, the system can be further extended with advanced models, real-time deployment, and integration with cloud-based security platforms.

VIII. FUTURE SCOPE

The current DDoS detection, classification, and prevention system provides a solid base for further development. Future enhancements may include real-time deployment for live network monitoring, improved model accuracy using advanced features like protocol analysis, and the adoption of deep learning models such as LSTM or Transformers. Integration with SIEM tools and adaptation for cloud platforms can enhance scalability and incident response. Additionally, incorporating self-learning mechanisms can help the system adapt to evolving attack patterns.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405021|

REFERENCES

[1] J. Halladay, M. D. Hall and M. J. Stojanovic, "Detection and Characterization of DDoS Attacks Using Time-Based Features," in Proc. IEEE Int. Conf. Commun. (ICC)*, 2022.
[2] M. Elsayed, M. Ibrahim and E. A. Elsayed, "DDoSNet: A DDoS Detection System Using Deep Learning," IEEE Access, vol. 9, pp. 95022–95031, 2021.
[3] M. Cil, M. A. G. Awais and A. J. Ahmed, "Detection of DDoS Attacks with Feedforward Neural Network," Computers, vol. 10, no. 1, pp. 8–23, 2021.
[4] G. Mirsky, A. Yerukhimovich and D. S. Kiv, "Chronos: Time-based Autoencoder for DDoS Detection," in Proc. IEEE Int. Conf. Cyber Security, 2021.
[5] X. Chen, M. L. Chen and Z. Yu, "DAD-MCNN: Multi-Channel CNN for DDoS Detection," J. Netw. Comput. Appl., vol. 142, pp. 91–101, 2020.
[6] M. Salahuddin, A. R. S. Noor and F. Shahid, "Anomaly Detection Using Autoencoder with Time-Based Features," Future Gener. Comput. Syst., vol. 106, pp. 623–633, 2020.
[7] R. Villalobos, A. L. Alvarez and E. A. Garcia, "Distributed DDoS Detection via K-Means," Int. J. Comput. Appl., vol. 175, no. 4, pp. 1–7, 2020.
[8] Z. Jia, Z. Dong and Y. Liu, "DDoS Attack Detection Using LSTM and CNN in IoT," IEEE Internet Things J., vol. 6, no. 4, pp. 7313–7321, 2019.
[9] M. Elejla, O. Alhazmi and A. Alharthi, "Comparison of Algorithms for IPv6 DDoS Detection," Int. J. Comput. Sci., vol. 45, pp. 43–52, 2019.
[10] G. Mirsky, R. C. Andrade and M. D. Nazari, "Kitsune: Lightweight Network Anomaly Detection," in Proc. IEEE Int. Conf. Netw. Syst. Secur. (NSS), 2018.
[11] H. Lashkari, S. S. Mehr and S. Z. Nia, "Characterization of Tor Traffic Using Time-Based Features," Int. J. Netw. Secur., vol. 19, no. 5, pp. 694–701, 2017.
[12] C. Huang, M. Y. Li and W. Zhang, "DDoS Detection in SDN Networks Using RNN," in Proc. IEEE Int. Conf. Cloud Comput. (CLOUD), 2017.
[13] A. Ioannidis, M. D. Manousakis and I. Roussos, "Autoencoder-Based Detection of DDoS Attacks in IoT," J. Cloud Comput. Adv. Syst. Appl., vol. 5, no. 1, pp. 49–56, 2016.
[14] X. Chen, W. Li and J. Lin, "Detection of Low-Rate DDoS Attacks with SVM," Int. J. Comput. Sci. Inf. Secur., vol. 13, no. 4, pp. 169–177, 2015.
[15] J. Yoon, A. Kumar and J. J. Berrill, "Anomaly Detection Using Packet-Rate Analysis," Comput. Secur., vol. 42, pp. 193–202, 2014.
[16] D. Callado, A. Ziviani and A. M. V. Freitas, "Survey on Machine Learning for Network Security," ACM Comput. Surv., vol. 45, no. 3, pp. 1–33, 2013.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details