DDOS ATTACK DETECTION AND MITIGATION

SHAIK AREEF
Shaik.areef2002@gmail.com
24NH1D5814
G. VIJAYASRI
nirmalaganji666@gmail.com
ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
V.K.R, V.N.B & A.G.K College of Engineering

ABSTRACT
(DDoS) attacks are one of the major cybersecurity threats that disrupt network services by overwhelming servers, systems, or networks with massive amounts of malicious traffic. These attacks can cause service downtime, financial loss, and reduced system performance, affecting organizations and users worldwide. The proposed DDoS Attack Detection and Mitigation system uses Artificial Intelligence and Machine Learning techniques to identify abnormal traffic patterns and detect malicious activities in real time. The system continuously monitors network traffic, analyzes packet behavior, and classifies legitimate and attack traffic using intelligent algorithms. Once a DDoS attack is detected, mitigation techniques such as traffic filtering, rate limiting, IP blocking, and load balancing are applied to reduce the impact of the attack and maintain service availability. The proposed system improves network security, enhances detection accuracy, minimizes false positives, and provides fast response mechanisms for protecting critical network infrastructures from cyber threats.

INTRODUCTION

(DDoS) attacks have become one of the most serious threats in modern computer networks and internet-based services. A DDoS attack occurs when multiple compromised systems or devices flood a target server, website, or network with excessive traffic, making the service unavailable to legitimate users. With the rapid growth of cloud computing, online banking, e-commerce, and digital communication platforms, the impact of DDoS attacks has increased significantly, causing financial losses, service interruptions, and security breaches for organizations worldwide.

Traditional security systems often fail to detect sophisticated DDoS attacks because attackers continuously change attack patterns and use large botnets to generate malicious traffic. To overcome these challenges, advanced detection and mitigation techniques using Artificial Intelligence, Machine Learning, and real-time traffic analysis are being developed. These intelligent systems can monitor network behavior, identify abnormal traffic patterns, and distinguish between legitimate and malicious requests with higher accuracy.

The proposed DDoS Attack Detection and Mitigation system aims to provide an efficient security mechanism for protecting network infrastructures from cyberattacks. The system continuously analyzes incoming network traffic and applies detection algorithms to identify suspicious activities in real time. Once an attack is detected, mitigation strategies such as traffic filtering, IP blocking, rate limiting, and load balancing are implemented to minimize the impact of the attack and maintain network availability. This project enhances cybersecurity by improving attack detection speed, reducing false alarms, and ensuring reliable network performance in modern digital environments.

LITERATURE SURVEY

1. DDoS Attack Detection Using Machine Learning

Author: Tom Mitchell
This research focused on the use of Machine Learning algorithms for detecting abnormal network traffic patterns caused by DDoS attacks. The system analyzed traffic behavior and classified malicious and legitimate packets with improved accuracy.

2. Network Intrusion Detection System Using Artificial Intelligence
Author: Andrew Ng
This study proposed an AI-based intrusion detection system capable of identifying cyber threats in real time. The system used intelligent classification techniques to improve detection speed and reduce false positive rates in network security.

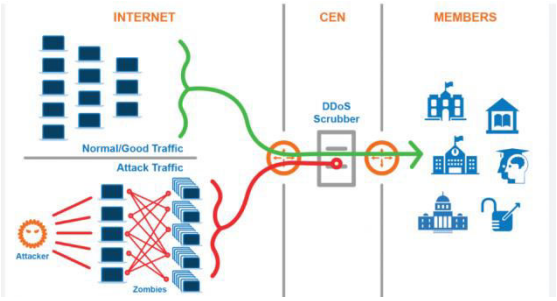
3. Deep Learning-Based DDoS Detection Framework
Author: Yoshua Bengio
This paper introduced the application of Deep Learning models for analyzing large-scale network traffic data. The framework improved the identification of complex DDoS attack patterns and enhanced mitigation performance.

4. Intelligent Traffic Analysis for Cybersecurity
Author: Geoffrey Hinton
The research focused on intelligent traffic monitoring systems that continuously analyze packet flow and identify suspicious activities. The proposed method helped in early DDoS attack detection and network protection.

5. Real-Time DDoS Mitigation Techniques in Cloud Networks
Author: Whitfield Diffie
This work explained various mitigation techniques such as rate limiting, IP filtering, and load balancing to reduce the impact of DDoS attacks in cloud computing environments and distributed networks.

6. AI-Driven Cybersecurity and Threat Detection
Author: Fei-Fei Li
This study highlighted the role of Artificial Intelligence in modern cybersecurity systems. The research emphasized automated threat detection, traffic analysis, and intelligent decision-making for protecting network infrastructures from cyberattacks.

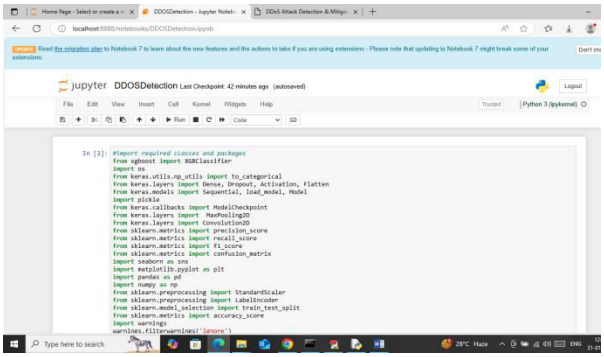
SYSTEM ARCHITECTURE



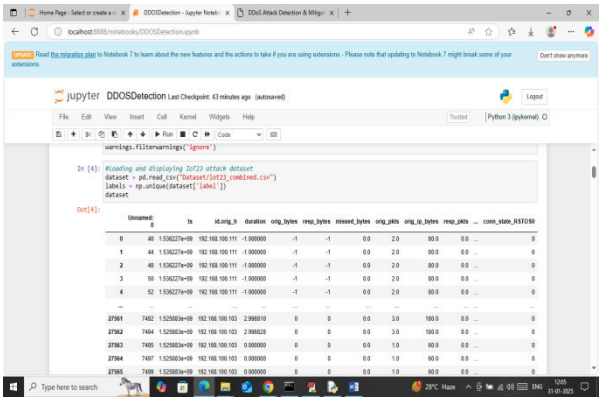
IMPLEMENTATION

DDoS Attack Detection & Mitigation
In propose work we are employing Machine & deep learning algorithms to detect IOT attacks. IOT are small devices which can be deployed anywhere to sense environment or its nearby data and then utilize internet connection to post sense data to centralized server for further processing or monitoring. Due to internet connectivity this small devices will be easily attack or hacked to inject false information or to steal data. To avoid such attacks heavy antivirus cannot be deployed as it consume heavy battery power and required heavy processing resources.
So rule based or ML based algorithms are cheap in processing but Rule based technique detection accuracy is very less so we are experimenting with ML and DL algorithms such as XGBOOST and CNN. This algorithms are able to detect attacks with an accuracy of more than 95%.
To train above algorithms we have utilize IOT23 DDOS attack dataset and then each algorithm performance is evaluated using different metrics like accuracy, precision, recall, Confusion Matrix and FCSORE.
Upon attack detection this application will add IP address to firewall which will prevent that IP from future IOT access.
SCREEN SHOTS
For training, testing, dataset processing we have utilize JUPYTER notebook and then employ web based flask framework to detect DDOD attack from test data. To run project double click on run.bat file to start JUPYTER

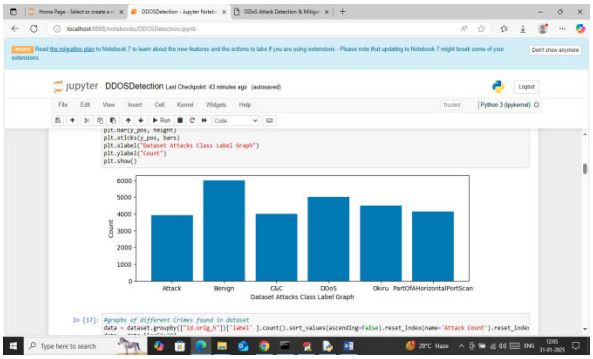
notebook. Below are the code and output screen with blue colour comments



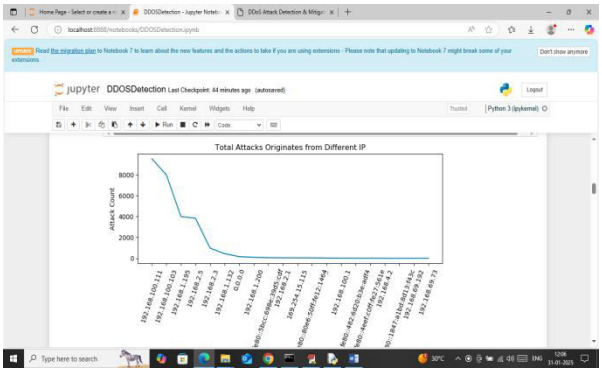
In above screen loading required python classes and packages



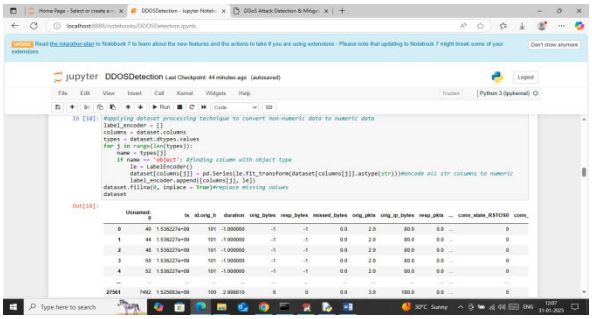
In above screen loading and displaying IOT23 dataset



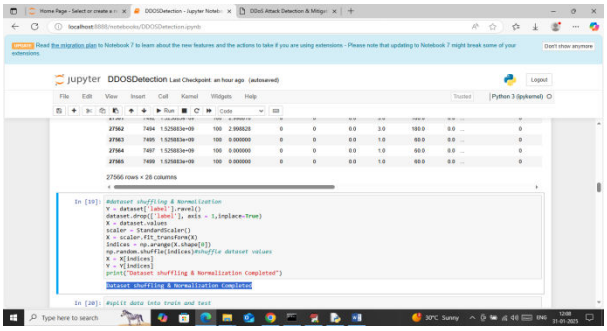
In above screen visualizing graph of different IOT attacks found in dataset where x-axis represents attack names and y-axis represents number of instances available in that attack category



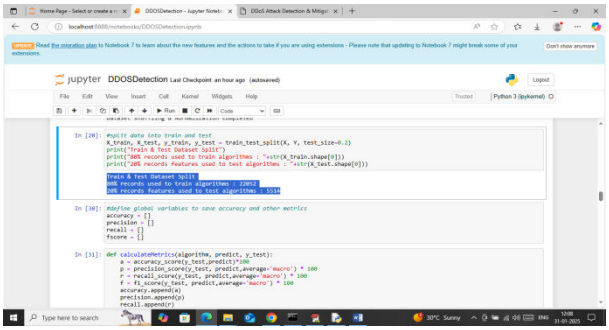
In above screen visualizing graph of most number of attacks originates from different IP. In above graph x-axis represents IP and y-axis represents number of attacks happen from that IP



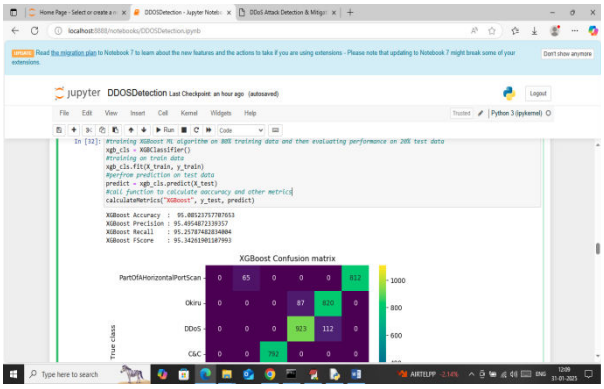
In above screen applying Label encoder class on dataset values to convert non-numeric data to numeric features and then replacing missing values with 0 and then can see cleaned dataset values



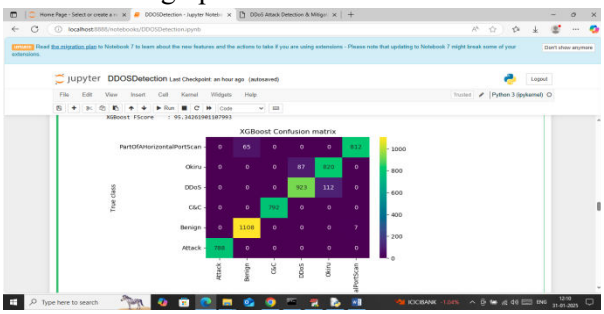
In above screen applying various dataset processing techniques such as shuffling and normalization



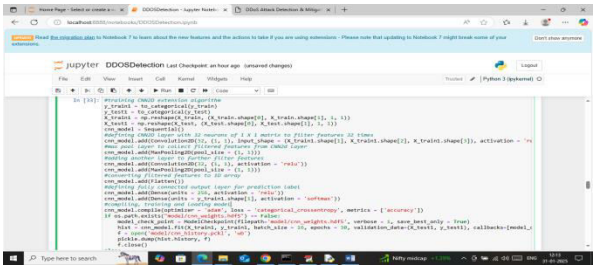
In above screen splitting dataset into train and test where application using 80% dataset for training and 20% for testing and then can see train and test size. In next blocks defining function to calculate accuracy and other metrics



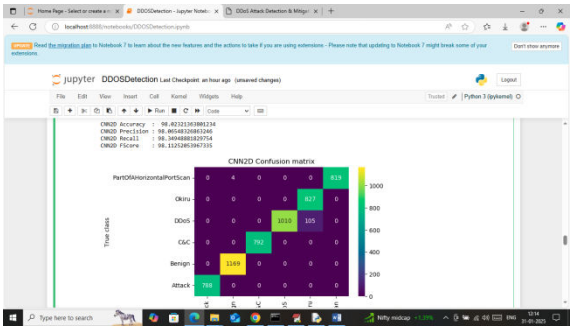
In above screen training XGBOOST algorithm on 80% training data and then performing prediction on 20% test data and then calculating prediction accuracy. In above screen XGBOOST got 95% accuracy on test and can see other metrics like precision, recall and FSCORE. Below is the confusion matrix classification graph



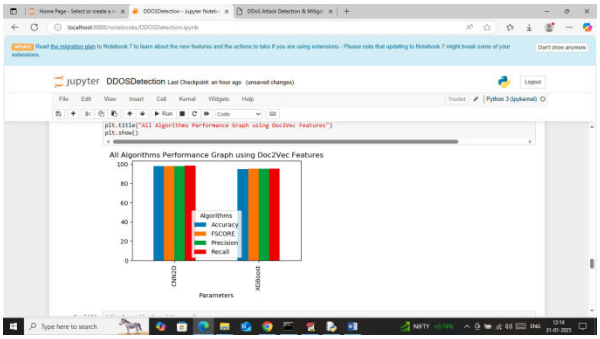
In above graph x-axis represents 'Predicted Labels' and y-axis represents True Labels and then all different colour boxes in diagonal represents correct prediction count and remaining blue boxes represents incorrect prediction count which are very few.



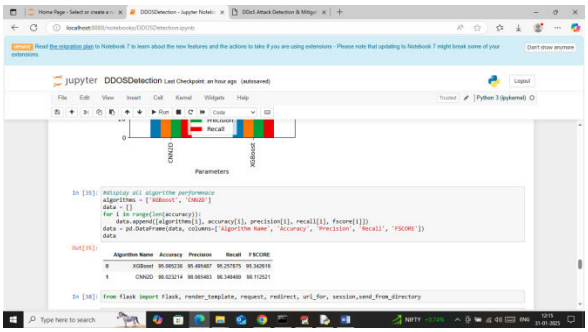
In above screen defining and training CNN2D algorithm and after executing this model will get below output



In above screen CNN got 98% accuracy and can see other metrics also

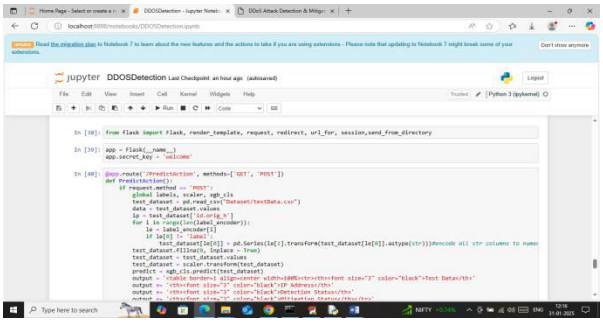


In above screen displaying comparison graph between both algorithms where x-axis represents algorithm names and y-axis represents accuracy and other metrics in different colour bars.

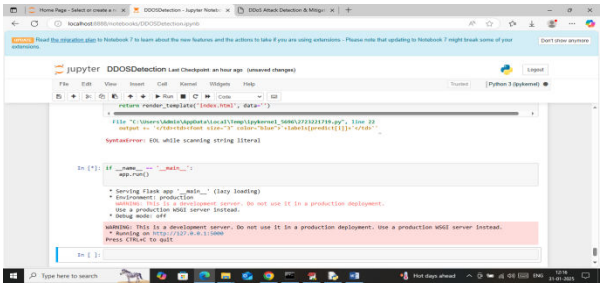


In above screen displaying both algorithm performance in tabular format. So in above screen we have done all data training and experiments execution.

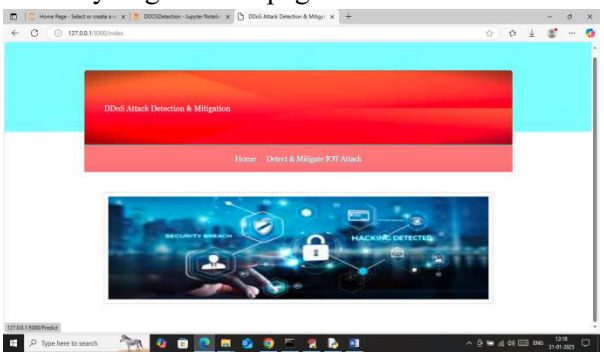
Now run all flask block code to mitigate attack from web page



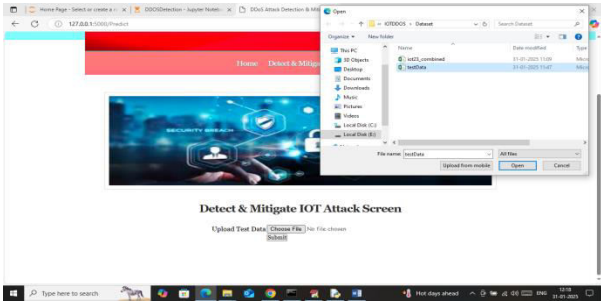
In above screen run all flask blocks to start flask server and then will get below page



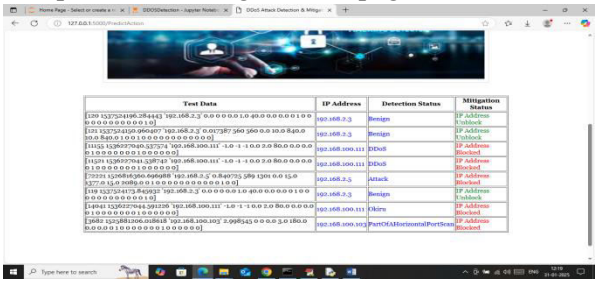
In above screen flask server started and now open browser and enter URL as http://127.0.0.1:5000/index and then press enter key to get below page



In above screen click on 'Detect & Mitigate IOT Attack' link to get below page



In above screen select and upload test data file which contains IOT network request data and then press button to get below page



In above screen in first column can see network request data and in second column can see SOURCE IP address which is sending request to IOT. In 3rd column can see predicted output as 'Benign (normal) or attack' and based on detected attack that IP will get blocked.

So by using above ML and DL algorithm you can detect and mitigate all possible IOT attacks.

CONCLUSION

The DDoS Attack Detection and Mitigation system provides an effective solution for protecting computer networks and online services from malicious cyberattacks. By using advanced technologies such as Artificial Intelligence, Machine Learning, and real-time traffic analysis, the system can accurately detect abnormal network behavior and identify DDoS attacks at an early stage. The proposed approach improves network security by continuously monitoring incoming traffic and distinguishing between legitimate and malicious requests.

The implementation of mitigation techniques such as traffic filtering, IP blocking, rate limiting, and load balancing helps reduce the impact of attacks and ensures uninterrupted network services. The system also minimizes false positives and enhances detection accuracy compared to traditional security methods. Overall, the project demonstrates the importance of intelligent cybersecurity solutions in safeguarding modern digital infrastructures and maintaining reliable network performance against increasing cyber threats.

FUTURE WORK

The future enhancement of the DDoS Attack Detection and Mitigation system can focus on improving detection accuracy, scalability, and response speed using advanced cybersecurity technologies. Integration of Deep Learning and real-time behavioral analysis can help the system identify complex and evolving DDoS attack patterns more effectively. Future systems may also incorporate adaptive learning models that continuously update themselves based on newly detected attack behaviors.

The proposed system can be extended to support cloud computing, Internet of Things (IoT) environments, and large-scale distributed networks for broader cybersecurity protection. Integration with blockchain technology can improve the security and integrity of network logs and attack records. Future versions may also include automated threat intelligence sharing between multiple networks to enable faster attack prevention and collaborative defense mechanisms.

Additionally, the system can be enhanced with predictive analytics to forecast potential cyberattacks before they occur. Advanced visualization dashboards and real-time monitoring tools can help network administrators analyze attack patterns and respond more efficiently. Overall, future developments will make the DDoS detection and mitigation system more intelligent, secure, scalable, and capable of protecting modern digital infrastructures from sophisticated cyber threats.

REFERENCE

1. – James F. Kurose and Keith W. Ross, Pearson Education.
2. Artificial Intelligence: A Modern Approach – Stuart Russell and Peter Norvig, Pearson Education, 4th Edition, 2020.
3. Machine Learning – Tom Mitchell, McGraw-Hill Education.
4. Deep Learning – Ian Goodfellow, Yoshua Bengio, and Aaron Courville, MIT Press, 2016.
5. “DDoS Attack Detection Using Machine Learning Techniques” – Andrew Ng, International Journal of Network Security.
6. “Deep Learning-Based Intrusion Detection System for Cybersecurity” – Geoffrey Hinton, Journal of Cyber Defense Research.
7. “Real-Time DDoS Mitigation in Cloud Computing Environments” – Whitfield Diffie, International Journal of Cloud Security.
8. TensorFlow Official Website
9. Scikit-learn Official Website
10. Kaspersky Cybersecurity Resources