Distributed Denial of Service (DDOS) Detection Using Artificial Neural Network

Dr.P.Vijaya Bharati[1], Petakamsetty Swathi[2], Pasupureddy Tejaswi[3], Polamarasetty Sangeetha Rani[4], Vegi Swetha Sri[5]

[1,2,3,4,5] Department of Computer Science and Engineering, Vignan's Institute of Engineeringfor Women, Visakhapatnam, Andhra Pradesh, India.

ABSTRACT

The "DDoS Detection using ANN" paper presents a robust cybersecurity solution employing Artificial Neural Networks (ANN) to detect and mitigate Distributed Denial of Service(DDoS) attacks in real-time. By consolidating data from various network protocols and preprocessing it for uniformity, the system ensures comprehensive coverage and reliability. The ANN model, trained with optimized parameters, accurately distinguishes between normal and malicious network traffic, facilitating rapid detection and triggering of mitigation measures. A user-friendly web interface enables easy analysis and provides recommendations for enhancing network security. Overall, this solution offers an effective and scalable approach for organizations to proactively protect their resources and maintain service continuity against DDoS attacks.

Keywords: DDoS Detection, Mitigation System, Network Security, Real-time Monitoring, Anomaly Detection, Traffic Analysis, Dashboard Interface, Cyber Threats.

INTRODUCTION

In moment's connected digital geography, cybersecurity remains a consummate concern for associations and individualities likewise. One of the most current and disruptive cyberpitfalls is Distributed Denial of Service(DDoS) attacks, where vicious actors submerge a network with inviting business to disrupt its normal functioning. These attacks can lead to significant fiscal losses, reputational damage, and service dislocations for targeted realities. The" DDoS Attack Discovery using ANN" design aims to attack this critical cybersecurity challenge by using the power of Artificial Neural Networks(ANN). ANNs are computational models inspired by the mortal brain's neural networks, able of literacy andfeting complex patterns in data. By training an ANN model on a different andcomprehensive dataset comprising colorful network protocols, the design seeks to developan intelligent system able of detecting and mollifying DDoS attacks in real time.

This design's significance lies in its eventuality to give associations with a visionary defensemedium against DDoS attacks, enabling them to guard their network structure, insure

service durability, and cover their precious means. With its stoner friendly interface and robust discovery capabilities, the" DDoS Attack Discovery using ANN" design offers a promising result to enhance cybersecurity measures and alleviate the pitfalls associated withDDoS attacks effectively.

LITERATURE SURVEY

[1] Dong and Sarem (2020) present a DDoS attack detection method based on an improved KNN algorithm with the degree of DDoS attack in software-defined networks, offering insights into leveraging machine learning for DDoS detection while considering the dynamic nature of attacks.

[2] Chen et al. (2018) propose an XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud environments, offering a specific machine learning-based solution tailored for detecting DDoS attacks in software-defined networks.

[3] Girma and Wang (2018) introduce an efficient hybrid model for detecting DDoS attacks in cloud computing using multivariate correlation and data mining clustering techniques, offering a comprehensive approach to address the challenges of accurate detection and mitigation.

[4] Alsirhani et al. (2018) propose a DDoS attack detection system leveraging classification algorithms with Apache Spark, providing a methodology for enhancing the accuracy of DDoS detection while mitigating false positives and negatives.

[5] Sahi et al. (2017) present an efficient DDoS TCP flood attack detection and prevention system tailored for cloud environments, offering a specific solution to address the real-time detection challenges posed by DDoS attacks.

EXISTING SYSTEM

Traditionally, DDoS (Distributed Denial of Service) detection and mitigation have relied on rule based systems and signature based approaches. These systems typically employ predefined rules or signatures to identify known attack patterns and block malicious traffic. While these methods can be effective against known attacks, they often struggle to detect new or sophisticated attacks that don't match existing signatures.

In recent years, machine learning and artificial intelligence (AI) techniques have been

increasingly adopted for DDoS detection due to their ability to analyze large volumes of network traffic data and identify subtle patterns indicative of malicious activity. However, most existing machine learning based DDoS detection systems use simple models and features, limiting their detection capabilities and accuracy.

Some existing systems also utilize anomaly detection techniques to identify abnormal patterns in network traffic. While these methods can be effective in detecting unknown attacks, they often suffer from high false positive rates and require extensive tuning and maintenance.

Existing DDoS detection systems face challenges in terms of accuracy, scalability, adaptability, and real time detection capabilities. There is a need for more advanced and robust detection systems that can effectively mitigate the growing threat of DDoS attacks while minimizing false positives and operational overhead.

Disadvantages

1. **Scalability:**
   - With the increasing size and complexity of networks, scalability becomes a major concern.Large data quantities are typically difficult for traditional approaches to handle effectively.
2. **False Positives/Negatives:**
   - Accurate detection without generating false alarms (false positives) or missing actualattacks (false negatives) remains a challenge.
3. **RealTime Detection:**
   - Real Time detection and response to DDoS attacks are essential but challenging dueto the rapid and dynamic nature of these attacks.
4. **Adaptive Attack Patterns:**
   - Attackers continually adapt and evolve their techniques, making it difficult fordetection systems to keep up with the changing attack patterns.
5. **Resource Constraints:**
   - Limited computational resources, especially in edge devices, pose constraints on deploying sophisticated detection algorithms.

PROPOSED SYSTEM

The proposed system aims to enhance the detection and mitigation of DDoS attacks using advanced machine learning techniques, specifically Artificial Neural Networks (ANNs).

Unlike traditional rule based and signature based systems, the proposed system utilizes ANNsto learn and identify complex patterns in network traffic data that are indicative of DDoS attacks.

Table1 :Comparison table between existing system and proposed system

Aspect	Existing System	Proposed System
Detection Approach	Rule-based and signature-based	Advanced machine learning (ANNs)
Effectiveness	Limited against new or sophisticated attacks	More accurate with complex attack pattern recognition
Real-Time Detection	Limited	Enabled
Scalability	Limited scalability	Scalable with increasing network traffic
Adaptability	Limited adaptability to evolving attack patterns	Adaptive to evolving attack patterns
False Positive Rate	Can be high due to reliance on predefined rules/signatures	Aimed to be lower through deep learning
User Interface	Varies, typically lacks user-friendly interface	Includes user-friendly web interface for network monitoring

Key Features of the Proposed System:

1. **Advanced Machine Learning Model**: The system employs a deep learning model, specifically an Artificial Neural Network (ANN), trained on a large dataset of network traffic to identify patterns associated with DDoS attacks.
2. **RealTime Detection**: The ANN model is designed to analyze network traffic data in realtime, allowing for timely detection and mitigation of DDoS attacks as they occur.
3. **Scalability:** The system is designed to scale with increasing network traffic and can adapt to evolving attack patterns, ensuring effective detection and mitigation of DDoS attacksacross various network environments.
4. **Low False Positives**: By leveraging the power of deep learning, the system aims to reduce false positives and improve the accuracy of DDoS attack detection, minimizing the impact on legitimate network traffic.

5. **UserFriendly Interface:** The system includes a user friendly web interface that allows network administrators to monitor network traffic, view detected attacks, and take appropriate actions, making it easier to manage and maintain the network security.

The proposed system offers a more advanced, accurate, and scalable solution for DDoS detection and mitigation, addressing the limitations of existing systems and providing better protection against DDoS attacks.

SYSTEM ARCHITECTURE

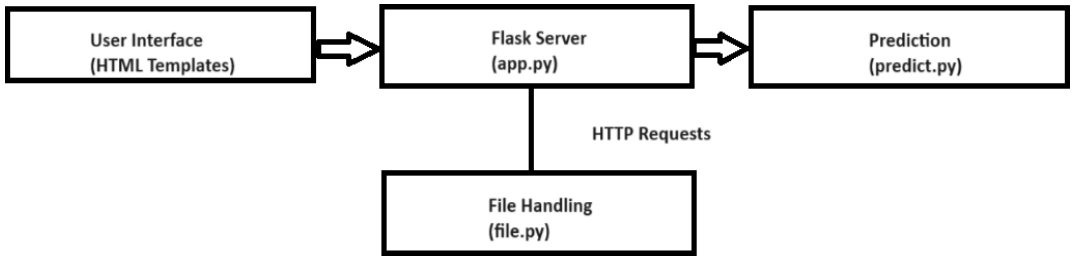


Figure 1: System Architecture

User Interface (HTML Templates): This is where users interact with the system, providing input data via a web interface.

Flask Server (app.py): Flask is used to handle incoming HTTP requests, process the uploaded data, and call the prediction module.

Prediction Module (predict.py): This module loads the trained machine learning model and performs predictions on the input data.

File Handling (file.py): This module manages the uploading and handling of text files containing the input data.

The flow starts with the user uploading a text file via the web interface. The Flask server receives the file, and the File Handling module processes it. The processed data is then passed to the Prediction Module, which uses the trained model to make predictions and returns the results to the user via the Flask server and User Interface.

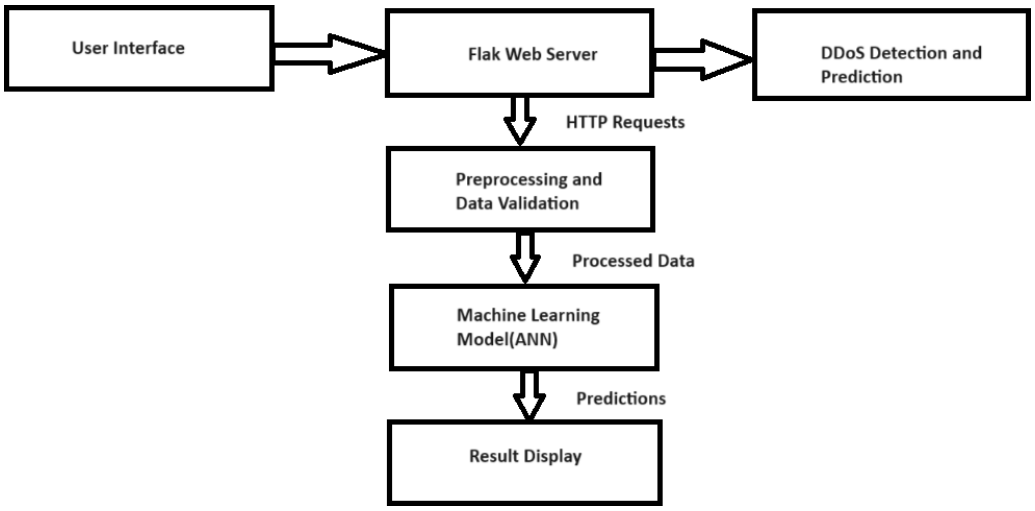
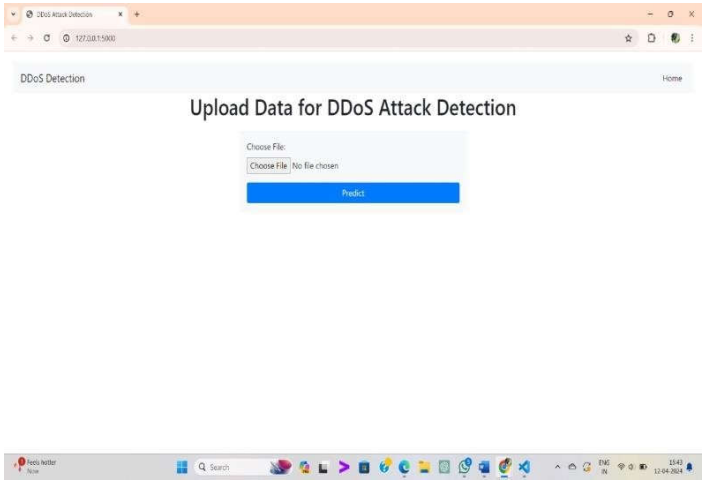
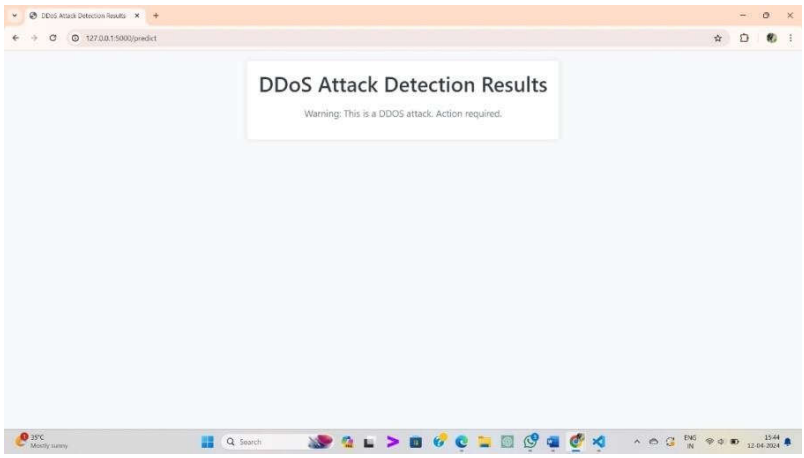


Figure 2 :Block diagram

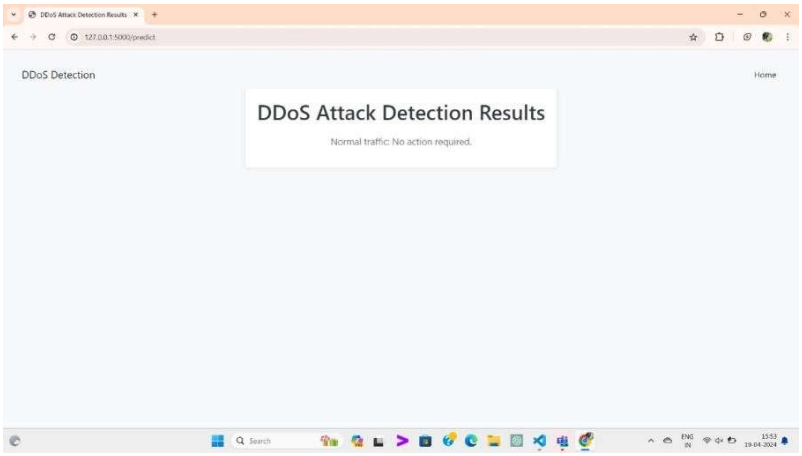
Output Screens



Output screen 1:User Interface



Output screen 2:Output for DDoS attack



Output screen 3: Output for Normal traffic

REFERENCES

1) R.B. Bohn,J. Messina,F. Liu,J. Tong, andJ. Mao, " NIST pall computing reference armature, " Proc. - 2011 IEEE World Congr. Serv. Serv. 2011,pp. 594 – 596, 2011, doi10.1109/SERVICES.2011.105.

2) GhsuoonB. Roomi and KhaldunI. Arif, " A cold-blooded approach for cargo balancing in pall computing Ghsuoon, "Adv. Intell. Syst.Comput.,vol. 554,no. 2,pp. 197 – 206, 2020, doi10.1007/ 978-981-10-3773-3, 19.

3) V. Varsha,A. Wadhwa, andS. Gupta, " Framework using Multitenancy Architecture in Cloud Computing, " Int.J. Comput.Appl.,vol. 121,no. 15,pp. 12 – 17, 2015, doi10.5120/ 21615- 4883.

4) A. Sahi,D. Lai,Y.A.N. Li, andM. Diykh, " An Effective DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment, " IEEE Access,vol. 5,pp. 6036 –

6048, 2017, doi10.1109/ACCESS.2017.2688460.

5) A. Alsirhani,S. Sampalli, andP. Bodorik, " DDoS attack discovery system exercising bracket algorithms with apache spark, " 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018- Proceedings,vol. 2018- Janua.pp. 1 – 7,
2018, doi10.1109/NTMS.2018.8328686.

6) He, Zecheng, Zhang, Tianwei, and Lee, RubyB.," Machine literacy Grounded DDoS Attack Detection From Source Side in Cloud" Proceedings- 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart pall, SSC 2017.

7) A. Girma andP. Wang, " Issues in Information Systems AN Effective mongrel MODEL FOR DETECTING DISTRIBUTED DENIAL OF SERVICE(DDOS) ATTACKS IN CLOUD COMPUTING USING. MULTIVARIATE CORRELATION AND DATA MINING CLUSTERING ways, "vol. 19,no. 2,pp. 1 – 12, 2018, doi10.48009/2_iis_2018_1-

12.(8)T. Mahjabin,Y. Xiao,G. Sun, andW. Jiang, " A check of distributed denial- of- service attack, forestallment, and mitigation ways, " Int.J. Distrib.Sens. Networks,vol. 13,no. 12, 2017, doi10.1177/ 1550147717741463.

9) Z. Chen,F. Jiang,Y. Cheng,X. Gu,W. Liu, andJ. Peng, " XGBoost Classifier for DDoS Attack Detection and Analysis in SDN- Grounded pall, " Proceedings- 2018 IEEE International Conference on Big Data and Smart Computing, BigComp 2018.pp. 251 – 256, 2018, doi10.1109/ BigComp.2018.00044.

10) S. Dong andM. Sarem, " DDoS Attack Discovery system Grounded on bettered KNN with the Degree of DDoS Attack in Software- Defined Networks, " IEEE Access,vol. 8,pp. 5039 – 5048, 2020, doi10.1109/ACCESS.2019.2963077.