IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Network Security Monitoring System

Mr. Prajwal Ajay Chitwar, Dr. Abhishek Gulhane, Ms. Pournima Hemraj Bhuyar, Mr. Om Nandkishor Talokar, Mr. Amar Rajendra Dhore

Final year student, Professor, Final year student

PRMITR Badnera,Amravati

ABSTRACT:

The publication proposes a machine learning-based Network Security Monitoring System to combat network attacks like DoS and DDoS. Leveraging the NSL KDD Dataset, the system integrates Software Defined Networking (SDN) principles for dynamic control and flexibility. Machine learning algorithms including Support Vector Machine, K Nearest Neighbor, Decision Tree Classifier, and ADABoost Classifier are employed. Additional features such as prevention strategies for attacks and BOTNET detection are being developed to enhance security for both large companies and individual device owners. Keywords: Network Security, DDoS, Machine Learning, Cybersecurity.

INTRODUCTION

In today's digital landscape, the threat of Network attacks looms large, posing significant challenges to the uninterrupted operation of computer networks. These attacks, orchestrated by malicious entities, aim to disrupt the normal flow of traffic to targeted servers, services, or entire networks by inundating them with an overwhelming volume of Internet traffic. The result is a denial of service to legitimate users, rendering the targeted resources inaccessible.

Traditionally, distinguishing between legitimate and malicious traffic in the midst of a DDoS onslaught has been a daunting task. Attackers leverage botnets armies of malware-infected computers under their control—to orchestrate these assaults, making it difficult to discern between genuine user activity and malicious traffic.

In response to this escalating threat landscape, the need for robust network security monitoring systems has become paramount. These systems play a crucial role in identifying, analyzing, and mitigating Network attacks, thereby safeguarding the continuity of essential services and protecting organizational assets.

Our endeavor focuses on developing an advanced Network Security Monitoring (NSM) system tailored to the specific needs of large organizations vulnerable to Network attacks. Through the integration of cutting-edge technologies and innovative methodologies, our NSM solution empowers cybersecurity and IT departments to proactively detect and respond to evolving threats.

Central to our approach is the implementation of a hybrid heterogeneous multi-classifier ensemble learning framework, which harnesses the collective intelligence of diverse detection algorithms. By leveraging techniques such as Bagging, Random Forest, Artificial Neural Networks (ANN), and k-Nearest Neighbor (k-NN), our system enhances detection accuracy and resilience to adversarial evasion tactics.

Furthermore, our NSM solution incorporates a novel detection algorithm based on Singular Value Decomposition (SVD) within the heterogeneous classification ensemble model. This algorithm exhibits exceptional stability and performance metrics, including True Negative Rate (TNR), accuracy, and precision, thereby fortifying the defense against Network attacks.

Looking ahead, our roadmap includes the integration of additional features such as Botnet prevention, aimed at thwarting the creation and proliferation of botnets. By scanning URLs for malware and preemptively blocking malicious activities, this feature empowers both cybersecurity professionals and end-users to mitigate the risk of becoming unwitting participants in Network attacks.

In essence, our NSM system represents a proactive and adaptive approach to combating the ever-evolving threat landscape posed by Network attacks. By combining state-of-the-art technologies with a strategic focus on prevention and detection, we strive to fortify the resilience of organizations against cyber threats, ensuring the uninterrupted delivery of critical services in an increasingly interconnected world.

OBJECTIVES OF STUDY

a) A network using Mininet and Ryu controller is to be implemented.

b) The dataset is to be generated.

c) The Random Forest Machine learning algorithm is to be applied to detect DDoS attacks.

HYPOTHESIS

1 Network Attack Detection: Implementing machine learning algorithms for analyzing network traffic patterns will lead to the identification of anomalies indicative of potential network attacks with enhanced accuracy, thereby enabling swift recognition and classification of various types of network attacks.

2 Network Attack Prevention: The development of proactive measures for automatic mitigation of identified network attacks, coupled with the exploration of adaptive strategies, will result in minimal impact on targeted networks, allowing for dynamic adjustment of prevention mechanisms based on evolving attack vectors.

3 Network Attack Prevention: The implementation of a real-time monitoring system will enable continuous surveillance of network traffic, facilitating swift responses to emerging threats by providing timely insights into network health.

4 Real-Time Monitoring: Employing machine learning models for dynamic adaptation and learning from past attack data will enhance future detection and prevention capabilities, thereby improving overall network security.

5 Machine Learning Integration: Creating profiles of DDoS incidents will lead to a better understanding of attack patterns, facilitating the refinement of detection and prevention algorithms for more effective defense against network attacks.

6 Incident Profiling: The development of a comprehensive data logging system to record and analyze DDoS attack incidents will enable post-incident analysis and continuous improvement in network security measures.

7 Data Logging and Analysis: Designing a user-friendly interface for system administrators and implementing an alerting mechanism will result in prompt notification of stakeholders about detected DDoS incidents and mitigation outcomes, thereby enhancing the overall management of network security incidents.

8 User Interface and Alerts:

LITERATURE SURVEY

Several research studies have delved into the realm of leveraging machine learning (ML) techniques to detect Distributed Denial of Service (DDoS) attacks, showcasing impressive accuracy rates ranging from 93.71% to 99.88%. Jin Kim et al. (2017) introduced a pioneering exploration into intrusion detection systems using deep neural networks (DNN), achieving a remarkable accuracy rate of 99.01% by employing the KDD Cup 99 dataset. To address challenges posed by time series data, Pei et al. (2019) focused on understanding DDoS attack modes, developing an ML-based method that effectively detects these attacks. Their approach, incorporating feature extraction and model detection techniques, fine-tuned model detection through training on the Random Forest algorithm and validation with Support Vector Machines (SVM). Similarly, Kaur et al. (2019) centered their research on DDoS attack detection, employing ML techniques such as K-Nearest Neighbors (KNN), Support Vector Machines (SVM), and Artificial Neural Networks (ANN). Their hybrid model demonstrated superior accuracy ranging from 95.2% to 97.4%, emphasizing the integration of diverse ML techniques for enhanced detection.

Moreover, Sahingoz et al. proposed phishing URL detection using ML, achieving 97.08% accuracy with support vector classifiers and 98.33% with deep learning algorithms. These studies collectively underscore the efficacy of ML in bolstering cybersecurity measures against DDoS attacks and phishing threats. Additionally, the heightened vulnerability of privacy and security in organizations due to rapid technological advancements emphasizes the pressing need for robust defense mechanisms.

DDoS attacks pose a significant security threat, aiming to decrease service availability by overwhelming network or computational resources, thereby preventing legitimate users from accessing services. Existing solutions encompass a spectrum of approaches, including ML-based solutions, distributed system solutions, and hybrid approaches that combine both. The emergence of ML-focused solutions highlights a promising trend in combating DDoS attacks, indicative of ongoing efforts to bolster network security in an evolving cyber landscape.

PROBLEM STATEMENT AND PROPOSED METHODLOGY

The publication utilizes the NSL-KDD dataset, a refined version of KDD-99, for network security monitoring. The dataset comprises 125,973 training rows and 22,544 test rows, categorized into five classes: Normal, Denial of Service (DoS), Probing, User to Root (U2R), and Remote to User (R2L). Data preprocessing involves null value removal and One-Hot-Encoding for categorical conversion. Machine learning algorithms including Logistic Regression, Support Vector Machine (SVM), K Nearest Neighbor, Random Forest, and Decision Tree classifiers are employed, with Logistic Regression demonstrating superior accuracy. Feature selection is performed using SelectKBest to optimize model performance. Additionally, a Botnet Prevention System is proposed, leveraging a malicious URL scanner. The system tokenizes and vectorizes text data for analysis. Experimental setup includes a Windows 10 64-bit OS laptop with an AMD Ryzen 3 CPU, 8GB RAM, and a 1TB hard drive.

In the proposed system:
1. Users input data via a local Flask application.
2. Data undergoes classification using SVM and Logistic Regression.
3. Detection determines if a DDoS attack occurred.
4. If positive, the user is alerted; if negative, the system remains normal.

5. The process concludes, ensuring timely response to potential threats.

In the Network Attack DDoS Prevention System:
1. Users input a URL via a Flask web application.
2. A URL classification model predicts the URL's nature.
3. If potentially malicious, preventive measures are activated to thwart DDoS attacks.
4. The process concludes, ensuring proactive protection against potential threats.

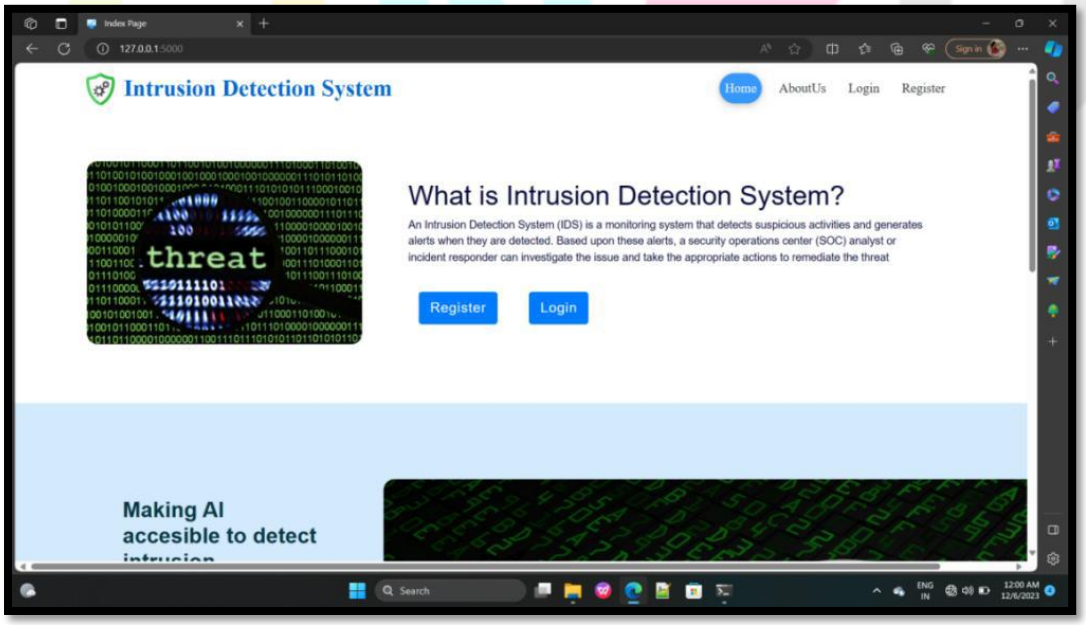
Parameter Evaluation:
Accuracy, detection rate, and false alarm rate are key metrics evaluated using a confusion matrix to assess the model's performance in identifying DDoS attacks accurately while minimizing false positives.

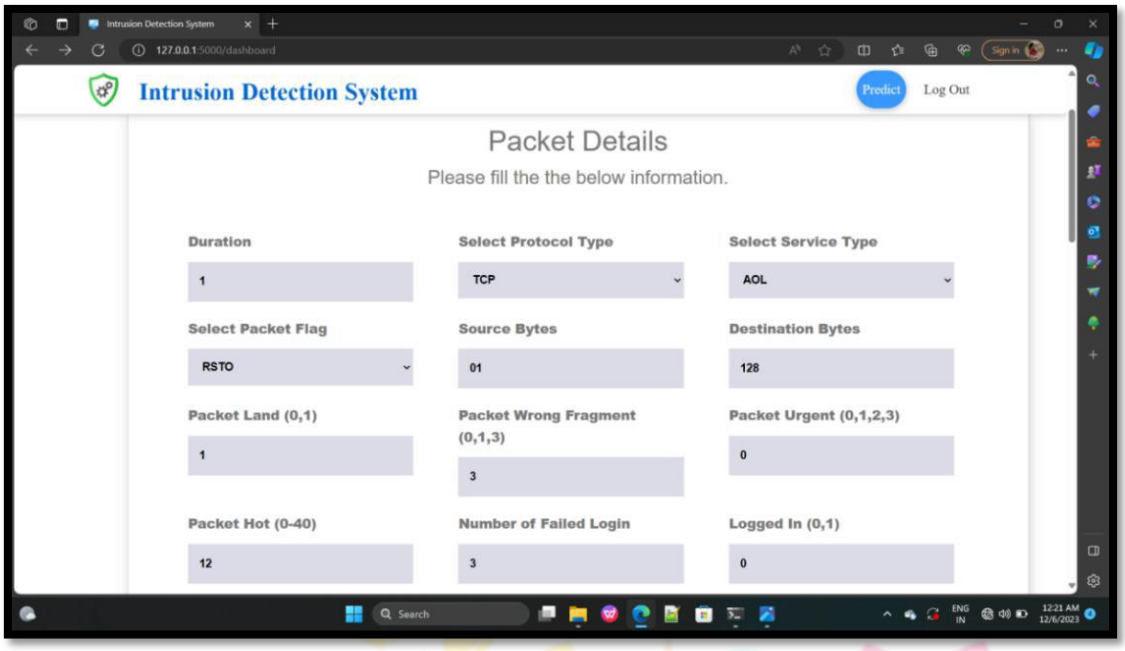
Evaluation of classification models reveals their efficacy in detecting DDoS attacks. Support Vector Machine (SVM) achieves 90.36% accuracy, demonstrating its capability in linear and non-linear classification. K Nearest Neighbors (KNN) reaches 89.15%, leveraging simplicity and proximity-based decision-making. ADA Boost attains 84.57%, harnessing boosting to improve the performance of decision stumps. Decision Tree Classifier scores 82.28%, benefiting from attribute selection measures for optimal tree construction. Confusion matrices illustrate true positives, true negatives, false positives, and false negatives, elucidating each model's predictive accuracy. SVM's versatility, KNN's ease of implementation, ADA Boost's enhancing effect, and Decision Tree's informative attribute selection contribute to their performance in detecting DDoS threats. These findings underscore the importance of selecting appropriate classification algorithms for network security applications, considering factors such as accuracy, computational efficiency, and interpretability. By comprehensively evaluating these models, network administrators can make informed decisions to enhance their defense mechanisms against DDoS attacks, ensuring the resilience and reliability of their networks in the face of evolving cyber threats.

The system architecture for Network Attack Detection using Machine Learning (ML) encompasses supervised, unsupervised, and hybrid approaches. Supervised learning involves training models on labeled data, distinguishing normal from attack traffic using algorithms like Regression and Classification. Unsupervised learning identifies patterns in unlabeled data through techniques such as Partitioning and Density-based algorithms. Hybrid methods combine supervised and unsupervised approaches to classify traffic and detect anomalies. System requirements include functional aspects like DDoS detection and communication with controllers, along with non-functional criteria such as detection and mitigation timeframes. Software requirements encompass operating systems like Windows, Linux, or macOS, along with tools like Ryu controller and Mininet software. The system design adheres to the principles of Software-Defined Networking (SDN), with layers including Application, Control, and Infrastructure. Activity diagrams detail dataset features and system implementation steps, from traffic categorization to machine learning model training and mitigation actions. The implemented system involves flow collection, feature extraction, anomaly detection, and mitigation modules, leveraging ML for flow-based detection and classification. Data gathering is facilitated through the OpenFlow protocol, with flow information parsed and processed to identify abnormal traffic for potential mitigation actions.

RESULT

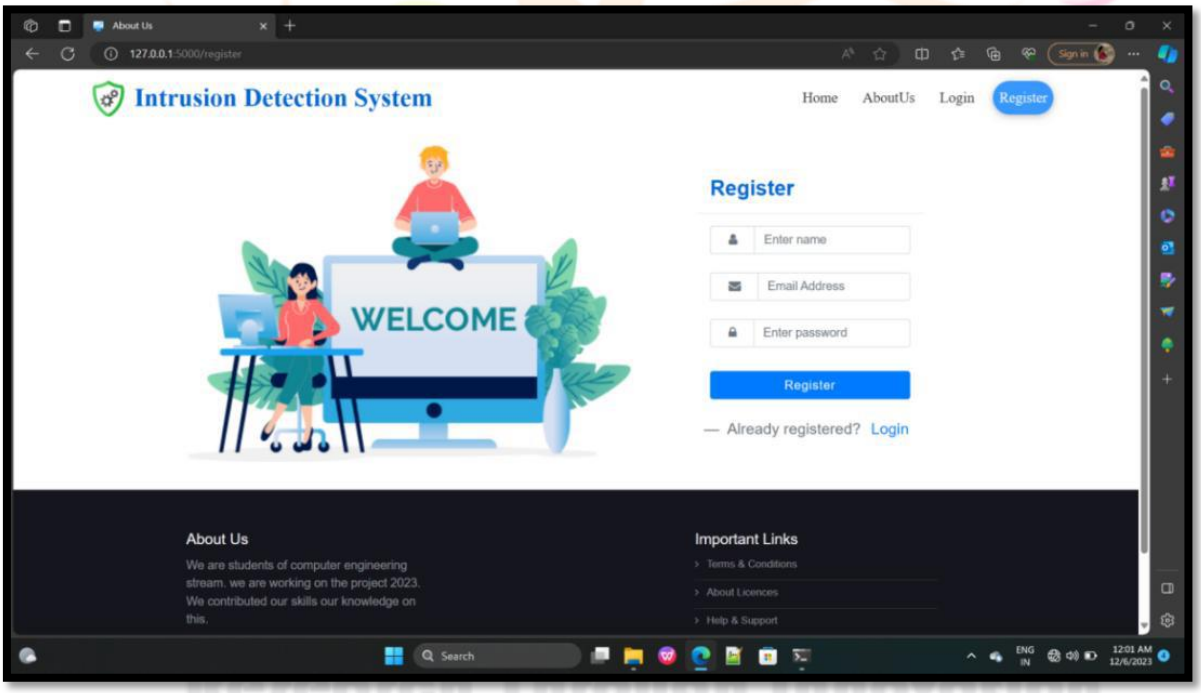
After designing the network attack detection and mitigation method, the results are tested and evaluated. The evaluation of the framework includes the evaluation of the different ML algorithms, and a comparison of the different models used.
In order to evaluate the performance of the model, a test is performed by process of online traffic classification and attack mitigation. For mitigating attacks, firewall rules were set to block attacks that were detected. Thus, for every flow detected as malicious, a firewall rule is installed to block the Ethernet address from which the attack is launched. The Python code of the generated prototype is implemented, and then normal traffic is generated as background traffic, and DDoS attack is detected.
Results from that after the traffic is launched it is collected and detected and firewall rules were installed to block the source attack. After this point all the attacks generated from the source were blocked without affecting normal traffic.





Screenshot No. 1 Intrusion Detection System site

As shown in screenshot no 1, it appears that, after exploring the system, you obtained a result related to a Network Security Monitoring by performing DDoS (Distributed Denial of Service) attack. The output includes various parameters, and the first part of this result describes aspects of the attack. Additionally, the output presents different options, such as "about," "home," "register," and others. This suggests that the system provides information or actions related to the DDoS attack, and users have the option to navigate or access specific functionalities through the mentioned options. To gain a more detailed understanding, further exploration of the output and its subsequent parts may be necessary.

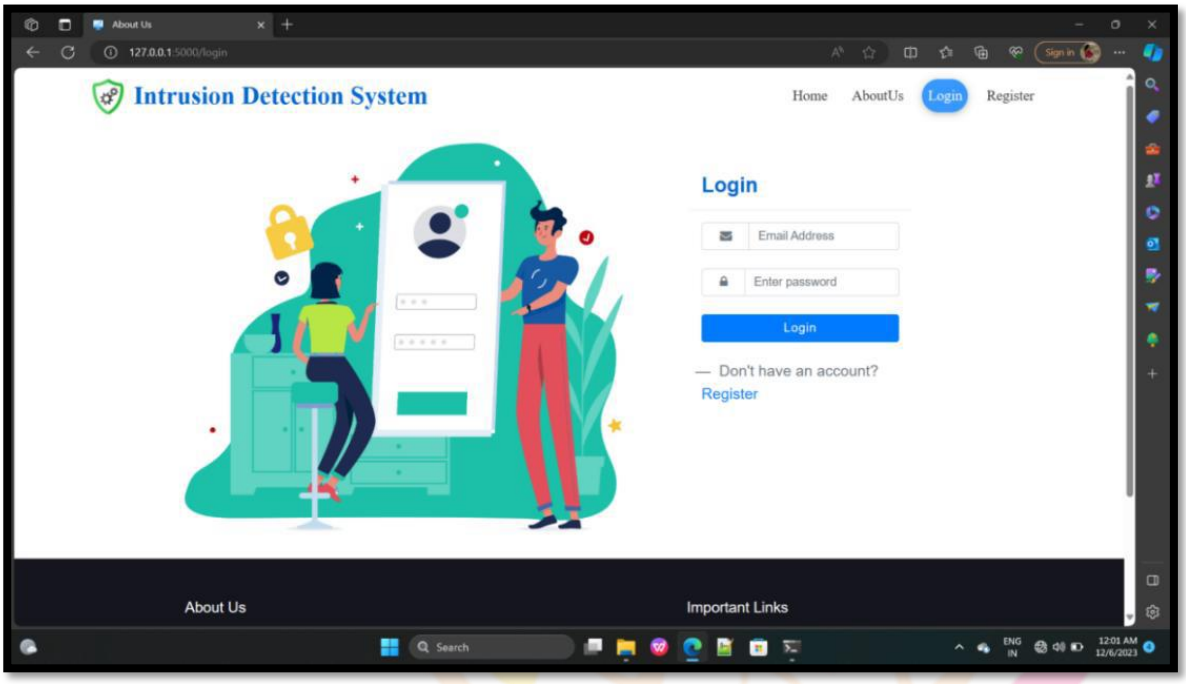


Screenshot No. 2 Register Page

As shown in screenshot no. 2, upon clicking on the "register" option, you are redirected to another page where you encounter a registration form. This form is designed for users to input necessary information and create a new account within the system. Registering an account typically involves providing details such as a username, email address, password, and possibly additional information depending on the system's requirements.
The registration process is fundamental for users to access specific features, personalize their experience, and potentially contribute or interact with the system in various ways. If you encounter any challenges or uncertainties
during the registration process, the system may provide guidance or instructions to facilitate the creation of a new account.
Screenshot No. 3 Login Page

As shown in screenshot no. 3, it seems that the system offers two distinct options. Upon clicking on one option, it directs users to a login page where they need to input their email address and password if they already have an account. On the other hand, if users haven't created an account yet, they are prompted to register first before accessing the login page.

This dual-option approach ensures flexibility for both existing users and new users. If individuals are returning users, they can swiftly log in with their existing credentials. On the other hand, new users are guided through the registration process to set up an account before gaining access to the login functionality. This system design promotes a user-friendly experience, catering to the needs of both those familiar with the system and those new to it.



Screenshot No. 4 Set data in System

As shown in screenshot no 4, it appears that, after a successful login, users gain access to a section involving the initialization of parameters. In this context, parameters refer to specific inputs or variables that the system uses for the detection of DDoS (Distributed Denial of Service) attacks. Users are prompted to input various parameters such as duration, service type, protocol type, packet flag, destination byte, source byte, and other relevant details.

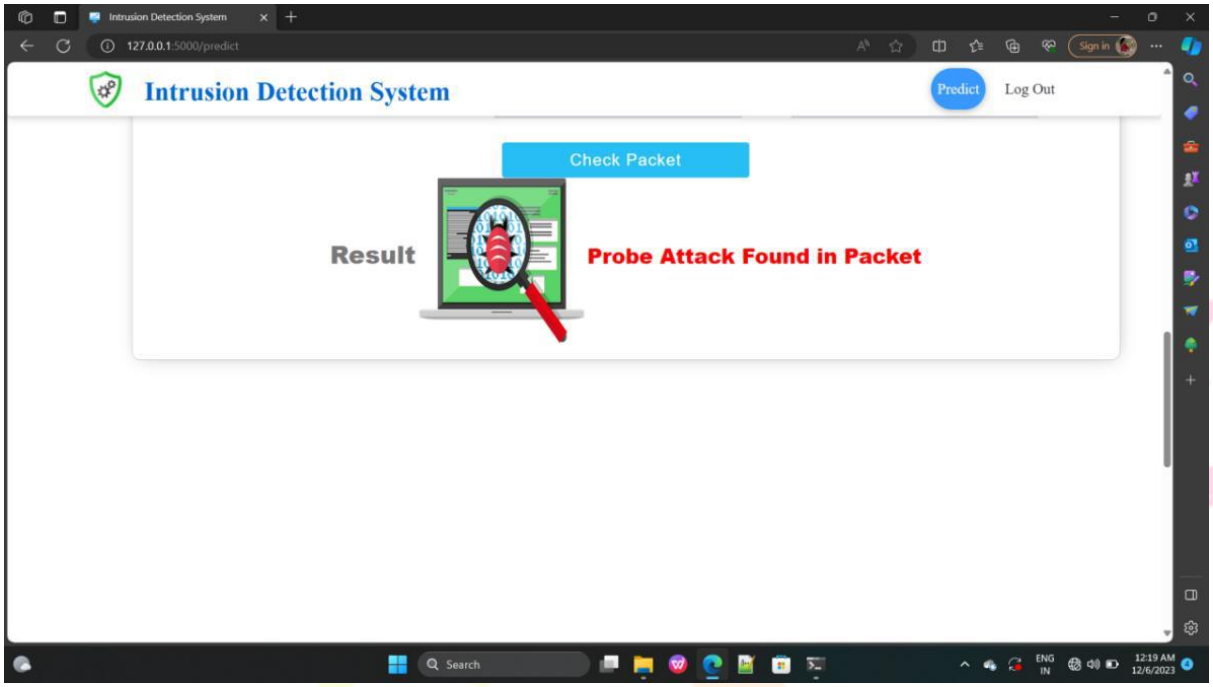
These parameters likely play a crucial role in configuring and customizing the DDoS detection process. By allowing users to specify these input values, the system tailors its analysis to the characteristics and requirements of the user's network or system. This level of customization enhances the system's ability to effectively identify and respond to DDoS attacks, providing a more robust and adaptable

security solution. Users can leverage this feature to fine-tune the DDoS detection mechanism according to the specific attributes of their network traffic

Screenshot No. 5 Result Attack found in packet

As shown in Screenshot no. 5, like after the initialization of input parameters, the system analyses various parameters to distinguish between DDoS attacks and normal packets. This analysis likely involves sophisticated algorithms and methods to identify patterns or anomalies in the network traffic. The preventive measures taken by the system are designed to mitigate the impact of DDoS attacks, ensuring the stability and security of the network.

Importantly, access to this analysis and prevention mechanism is restricted to developers or authorized personnel. This restriction ensures that only individuals with the appropriate permissions can interact with and configure the system's DDoS prevention features. This security measure is crucial for preventing unauthorized access and potential misuse of the system's powerful capabilities. It emphasizes the importance of maintaining a secure and controlled environment for Network Monitoring using DDoS detection and prevention.



CONCLUSION

The publication focuses on leveraging machine learning for detecting and analyzing network attacks, particularly Distributed Denial of Service (DDoS) attacks. It employs feature selection methods to identify significant features for prediction and evaluates multiple machine learning models. Results indicate that the Random Forest (RF) model with a 20-feature set demonstrates superior performance in terms of precision, accuracy, recall, and false negative rate. Future work aims to integrate these findings into real-time Network Security Monitoring systems for prompt DDoS attack detection. Additionally, the paper proposes using linear regression for Network Security Monitoring, specifically targeting DDoS attacks. It involves extracting protocol attack packets, performing feature extraction and format conversion, and utilizing logistic regression for model training. For botnet prevention, URL tokenization and classification into legitimate and malicious tokens are proposed, with logistic regression used for overall model training. This research contributes to enhancing the detection of network attacks, particularly DDoS attacks, utilizing the CICDDoS2019 dataset.

REFERENCE

[1] Jin Kim, Nara Shin, S. Y. Jo and Sang Hyun Kim, "Method of intrusion detection using deep neural network," 2017 IEEE International Conference on Big Data and Smart Computing (Big Comp), 2017, pp. 313316, doi: 10.1109/BIGCOMP.2017.7881684.

[2] Idhammad M, Afdel K, Belouch M. “Semi-supervised machine learning approach for DDoS detection.”Applied Intelligence. 2018 Oct;48(10):3193-208.

[3] Pei J, Chen Y, Ji W. “A DDoS Attack Detection Method Based on Machine Learning.” InJournal of Physics: Conference Series 2019 Jun 1 (Vol. 1237, No. 3, p. 032040). IOP.

[4] Kaur G, Gupta P. “Hybrid approach for detecting DDOS attacks in software defined networks.”In2019 Twelfth International Conference on Contemporary Computing (IC3) 2019 Aug 8 (pp. 1-6). IEEE.

[5] Sahingoz, O.K., Buber, E., Demir, O. and Diri, B., 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, pp.345-357.

[6] Zekri, M., El Kafhali, S., Aboutabit, N. and Saadi, Y., 2017, October. DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd international conference of cloud computing technologies and applications (CloudTech) (pp. 1-7). IEEE.

[7] Pervez, M.S. and Farid, D.M., 2014, December. Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs. In The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014) (pp. 1-6). IEEE.

[8] Faujdar, N., Sinha, A., Sharma, H., & Verma, E. (2020, October). Network Security in Software defined Networks (SDN). In 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE) (pp. 377380). IEEE.
[9] Iqbal, M., Iqbal, F., Mohsin, F., Rizwan, M., & Ahmad, F. (2019). Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions. International Journal of Advanced Computer Science and Applications.