iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.58842

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

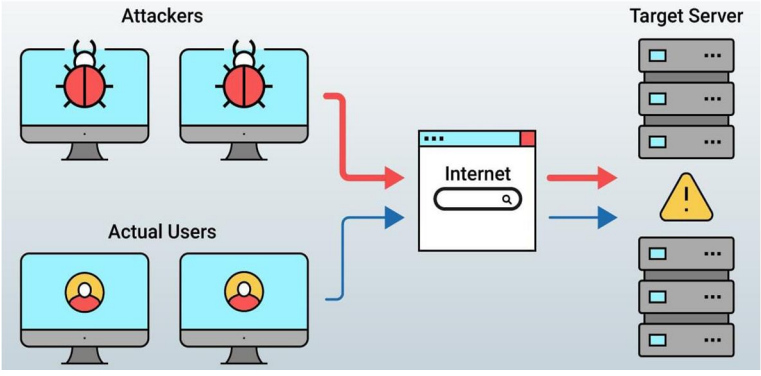
Detection and Characterization of DDoS Attacks using Time Based Features

Vandana M[1], Tejashwini V[2], Pankaja S K[3], Vandana M Koppal[4], Vedashree L V[5]
[1, 2, 3, 4]*Computer Science and Engineering, Dayananda Sagar University, Bengaluru, India*
[5]*Assistant Professor, Dayananda Sagar University, Bengaluru, India*

Abstract: ***In today's evolving cyber security environment, DDoS attacks are now one of the riskiest and most expensive attacks. DDoS detection and prevention has become critical as businesses and government agencies are affected by DDoS, which can disrupt network services and cause billions of dollars in damage. Our project offers a solution that detects different types of DDoS attacks using machine learning algorithms. The main aim of the project is to detect attacks of binary classification and multi class classification, this also reduces the time complexity.***
The proposed system studies the efficiency of time based features to detect and classify types of DDoS attacks using binary and multiclass classification. Using machine learning algorithms, the system analyzes this data to detect between legitimate and the attack network request. The addition of a time based features subset increases the accuracy of the system, reduces training time without compromising test accuracy.
The general purpose of the project is not only detection research. It can be seen that training a subset of time-based features can reduce training time without affecting test accuracy; thus, the small subset of time-based features is itself useful for near-real-time applications with continuous learning.
This demonstration aims to investigate the effectiveness of DDoS attacks based on time based features, providing a better path to network safety. This innovation, which meets the need to be more efficient in network and crime investigations, is not only based on modern technology, but also has a social and environmental purpose, being an important step towards safety.
The Data will be reduced before training our dealers. Deep learning models in particular require a lot of data; therefore, training the included data may influence the results, and achieve a higher standard.
Keywords: DDoS Attack, XGBOOST, Binary classification, Multi class classification, Time Based Features.

I. INTRODUCTION

Today, it is entirely on the internet as the world's source of information for all users of the age. Distributed Denial of Service is one of the most significant attacks in today's online world. It can attack any computer at any time without being detected by the user's computer. It can attack every customer in the country, even the highest level of government. Their sole purpose is to make money from their victims.



This project explores the detection and characterization of DDoS attacks using machine learning algorithms. This presentation introduces a time based features subset to detect and classify attacks. The system addresses the need for better road safety and contributes to societal and environmental benefits.

The system uses IP addresses and methods to complete the process of locating events on the network. They do this according to the feature selection principle, thus reducing the feature making time. As a result, risks can be intervened immediately.
Binary classification is an important task in machine learning, where the goal is to classify data into one of two classes.This detects whether the request is legitimate or a DDoS attack. On further process of multiclass classification it detects various DDoS types.
Multi Classification is the process of assigning entities to more than two groups. All fields are assigned to the class without overlap. In our paper we will be working on 12 different attacks namely MS SQL, SSDP, NTP, Port Map, DNS, SYN Flood, UDP Flood, UDP Lag, LDAP, Net Bios, SNMP, TFTP. This project detects and classifies these attacks.

II.LITERATURE SURVEY

Some Conclusions we got from the necessary references:

1) DDoS Attacks Detection in the Application Layer Using Three Level Machine Learning Classification Architecture(2021)
This paper introduces a three-layer framework designed to detect application layer DDoS attacks. The first layer is responsible for selecting the best features of the model and classifying traffic as bad or bad, and the second layer has a complex voting process that identifies the type of DDoS source (UDP, TCP or hybrid). Finally, we move on to the final stage with the attack with the appropriate DDoS type. The method is validated using the CIC-DDoS2019 dataset and time, accuracy score, and accuracy are used to model the performance. It provides improvements in both binary and multiclass classification of application-layer DDoS attacks. It needs improvement in time efficiency

2) Feature Selection Approach To Detect DDoS Attack Using Machine Learning Algorithm(2021):
This study was conducted to detect the presence of DDoS attacks using machine learning techniques on the UNSW-NB 15 dataset. The features in the dataset will be selected by using a filter method which is Information Gain and Data Reduction to get the best subset of features to detect the DDoS attack. After selecting the highest ranked features from Information Gain, machine learning techniques will be used to test datasets to get the output. The output will be in the classes of attack and normal. The algorithms that will be used in this research are ANN, Naïve Bayes and Decision Table. The experiments were run on the WEKA Machine Learning tool to generate the parameter evaluation like Accuracy, Precision, True Positive and False Positive metric. The result obtained from this study has been compared with the previous research conducted on DDoS attack detection.

3) A Machine Learning Approach for DDoS Detection on IOT Devices(2021):
This research work on new types of DDoS attacks are highly advanced and complicated, and it is almost impossible to detect or mitigate by the existing intrusion detection systems and traditional methods. Fortunately, Big Data, Data mining, and Machine Learning technologies make it possible to detect DDoS traffic effectively. This paper suggests a DDoS detection model based on data mining and machine learning techniques. For writing this paper, the latest available Dataset, CICDDoS2019, experimented with the most popular machine learning algorithms and specified the most correlated features with predicted classes being used. It is discovered that AdaBoost and XGBoost were extraordinarily accurate and correctly.It provides high performance. It needs to be extended by enhancing the model for multi classification of different DDoS attack types and testing hybrid algorithms and newer datasets on this model.

4) Development And Evaluation of Ensemble Learning Models for Detection of DDoS Attack in IOT (2020):
In this work, the new Distributed Denial-of-Service (DDoS) detection models using feature selection and learning algorithms jointly are proposed to detect DDoS attacks, which are the most common type encountered by Internet of Things networks. Additionally, this study evaluates the memory consumption of single-based, bagging, and boosting algorithms on the client-side which has scarce resources.
Not only the evaluation of memory consumption but also development of ensemble learning models refer to the novel part of this study demonstrating the feasibility of the base models, for the Internet of Things DDoS detection task, due to their application performance. It needs to detect more cyber threads in an IoT environment by performing future Selection for any cyber-attack in a comprehensive dataset including DOS detection, BOT detection, brute-force detection, and intrusion detection.

III. MATERIAL REQUIREMENTS

General equipment is very important to comply with the best recommendations on detection and characterization. Key components include data collection, data preprocessing, feature extraction, machine learning models development, evaluation and testing, deployment and integration, privacy and ethics, resource requirements, reporting and communication. Additionally, it requires libraries namely Matplotlib, Numpy, Pandas, Sckit-learn, Seaborn, Joblib, Tensorflow, Keras, dash to get the output.

User-friendly interface depends on appropriate software and graphical user interface (GUI) development tools. Cost considerations require the selection of system scalability to be compatible with network systems. The project works on anaconda application with jupyter notebook platform.

IV. METHODOLOGY

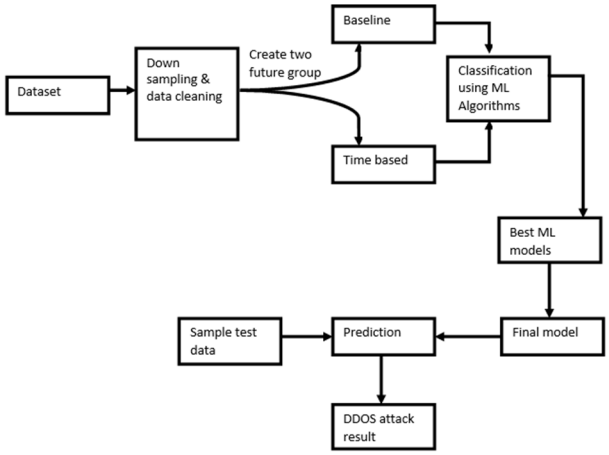
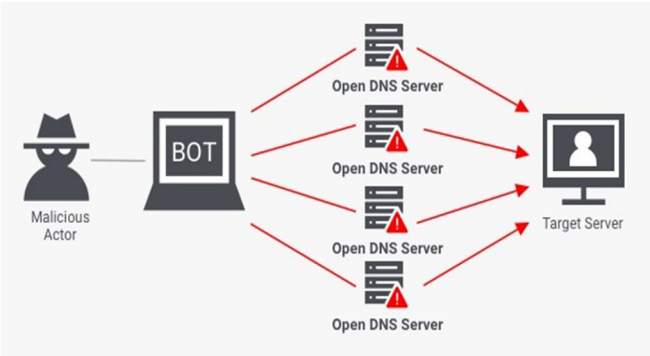


Figure 1. Design of the System

The approach adopted to enhance maximum planning with various technologies to ensure good crime-by-crime solving has been taken. The foundation is based on the use of technology, including data collection, detection and characterization of attacks. Machine learning algorithms form an important part of the process, enabling the system to analyze and interpret incoming data with high accuracy. This system helps intelligently identify DDoS attacks that differ from regular habits and situations that require immediate intervention. Detecting using time-based features increases the accuracy of the system, ensuring that identified events are not only accurately detected. The importance of this approach, highlighting the importance of rapid coordination to minimize the impact of an incident. In summary, the approach takes a similar approach, combining machine learning algorithms and user-friendly interfaces with the ability to intervene immediately to create new collisions and prevent crime effectively and efficiently.

A. A DDoS attack Hierarchy Consisting of bots Controlled by Master Machines under an attacker's Control



DDoS detection in network systems improves safety. The operation of a detection system usually involves the following steps:

1) *Data Collection:* The detection system acquires diverse datasets containing information about different types of DDoS attacks.
2) *Data Preprocessing:*Preprocess the datasets by cleaning, normalizing, and handling missing data to ensure consistency and reliability.
3) *Feature Extraction:*Implement algorithms to extract relevant time- based features from the preprocessed datasets. dExplore statistical methods to analyze temporal patterns and characteristics in network traffic.
4) *Model Development:*Design the machine learning model architecture, incorporating the extracted time-based features. Consider the use of appropriate algorithms, including traditional classifiers and potentially deep learning models.
5) *Training:* Split the dataset into training and testing sets for model evaluation. Train the model using the training dataset, fine-tuning parameters for optimal performance.
6) *Testing:* Evaluate the model on the testing dataset to measure its accuracy, precision, recall, and other relevant metrics.
7) *Classifier Optimization:* Apply optimization techniques to enhance the efficiency of the classifiers. Explore methods to reduce training time without sacrificing the model's accuracy during testing.
8) *Validation and Robustness Testing:* Validate the model's performance using additional datasets or real-world scenarios. Conduct robustness testing to ensure the model's effectiveness in diverse and dynamic network environments.
9) *Documentation and Reporting:* Document the entire methodology, including data preprocessing, feature extraction, model development, and optimization. Prepare comprehensive reports detailing the methodology, findings, challenges encountered, and proposed solutions.
10) *Ethical Considerations:* Address ethical considerations related to data privacy, informed consent, and responsible use of machine learning in cybersecurity research.

Defines the problem of DDoS attack detection and classification. Identify the specific challenges associated with the existing methods and the potential benefits of incorporating time-based features

The design of this project is centered on a holistic and innovative approach to elevate the efficacy of detecting and classifying Distributed Denial of Service (DDoS) attacks. At its core, the design emphasizes the integration of time-based features, recognizing their potential in providing a nuanced understanding of network traffic patterns.

The initial phase involves meticulous data preprocessing, encompassing the acquisition, cleaning, and normalization of datasets containing diverse DDoS attack information. Subsequently, algorithms will be implemented to extract pertinent time-based features, enabling a detailed temporal analysis of network traffic. The model architecture, a key component, will be developed with sophistication, incorporating state-of-the-art machine learning algorithms and potentially integrating deep learning techniques to ensure robust classification accuracy. The design accommodates both binary and multiclass classification approaches, recognizing the necessity of discerning various DDoS attack types. Furthermore, a crucial aspect of the design involves the optimization of classifiers through machine learning techniques, aiming to reduce training time while maintaining the model's accuracy during testing. The integration of machine learning libraries ensures a seamless and efficient implementation of the proposed design. Prototyping and testing phases will iteratively refine the design, and comprehensive documentation will capture the entire process, contributing valuable insights for future advancements in cybersecurity measures.

We train nine classifiers on a time-based feature subset to detect and classify DDoS attacks by analyzing temporally related features in traffic flows. To our knowledge, the time-based feature set has not been investigated in the domain of DDoS attacks.

The smaller time-based feature set reduces overall training time, decreases dimensionality and noise, reduces the necessary computational resources, and promotes the viability of continuous learning. We've found few related works concerning multiclass classification in the domain of DDoS detection. Focused on differentiating five types of DDoS attacks whereas our classifiers differentiate 12 different attack types. Our binary classifiers produced comparable or higher accuracy results than the ones published in existing literature, and our multiclass classifiers' performances are in line with classifiers despite using seven more attack types. Found the time-based feature set to be effective in classifying Tor and VPN traffic. We have filled in the knowledge gap in the domain of DDoS attacks by finding the time-based feature subset alone to be comparably effective and providing much better training time.

V. CONCLUSION

This project endeavors to revolutionize the domain of DDoS attack detection and classification by introducing a pioneering methodology centered around the integration of time-based features. DDoS attacks persist as a formidable threat in the cybersecurity landscape, necessitating inventive strategies for the timely and precise identification of such threats to mitigate their disruptive impact.

The primary objectives of this project encompass the extraction of pertinent time-based features from datasets associated with DDoS attacks. Through a meticulous analysis of the temporal aspects of network traffic, the aim is to enrich the feature sets, thereby enhancing the overall efficacy of the detection process.

The subsequent phase involves the development of a sophisticated machine learning model employing cutting-edge algorithms. This model is designed to facilitate robust detection and classification, accommodating both binary and multiclass categorizations to discern diverse types of DDoS attacks.

Additionally, the project places a strong emphasis on the optimization of classifiers, leveraging machine learning techniques to streamline the training process while upholding the paramount importance of accuracy during testing. By addressing the inherent challenges and complexities of DDoS attack detection, this project aspires to contribute significantly to the evolution of cybersecurity measures in contemporary network environments.

We analyzed the performance of eight machine learning algorithms and one deep learning model on the CIC-D DoS2019 dataset in two events. Event A splits legitimate traffic and DDoS traffic, and event B splits DDoS attack types. To detect this we have used machine learning algorithms, boosting algorithms, and one deep learning algorithm.

We have worked on time based features to detect and characterize the DDoS attacks which improves accuracy to 99% and reduces training time. The accuracy is tested on every model and the accuracy is given as 99% which is better than other papers. Later we compared both base features and time - based features using a deep learning model namely Deep neural network to check which is better. As a result time - based features were better to detect and characterize the DDoS attacks.

The output is given in a GUI format where the data is passed and the result is given from both binary classification and multi class classification. Working over large data, this faster training time is desirable over accuracy as the models are trained continuously.

VI. ACKNOWLEDGMENT

We would like to thank the University that provided the necessary resources “Dayananda Sagar University” for the opportunities to make the study practical and accessible as desired.

We also thank professor “Vedashree L V” and friends for their collaboration, discussions, and helpful suggestions during a research conference and workshop where preliminary results of this study were presented. Their insights enrich our understanding and inspire us to renew our ways.

REFERENCES

[1] Kanber BM, Noaman NF, Saeed AM, Malas M. DDoS Attacks Detection in the Application Layer Using Three Level Machine Learning Classification Architecture. International Journal of Computer Network & Information Security. 2022 June 1;14(3).

[2] Azmi MA, Foozy CF, Sukri KA, Abdullah NA, Hamid IR, Amnur H. Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms. JOIV: International Journal on Informatics Visualization. 2021 Dec 28;5(4):395-401.

[3] Seifousadati A, Ghasemshirazi S, Fathian M. A Machine Learning approach for DDoS detection on IoT devices. arXiv preprint arXiv:2110.14911. 2021 Oct 28.

[4] YILMAZ Y, BUYRUKOĞLU S. Development and Evaluation of Ensemble Learning Models for Detection of DDOS Attacks in IoT. Hittite Journal of Science and Engineering. 2022 Jun 6;9(2):73-82.

[5] Sharafaldin, A. H. Lashkari, S. Hakak and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 2019, pp. 1-8, doi: 10.1109/CCST.2019.8888419.

[6] Shieh, C.-S.; Lin, W.-W.; Nguyen, T.-T.; Chen, C.-H.; Horng, M.-F.; Miu, D. Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model. Appl. Sci. 2021, 11, 5213. https://doi.org/ 10.3390/app11115213

[7] Abreu Maranhão JP, Carvalho Lustosa da Costa JP, Pignaton de Freitas E, Javidi E, Timóteo de Sousa Júnior R. Error-robust distributed denial of service attack detection based on an average common feature extraction technique Sensors. 2020 Oct 16;20(20):5845..

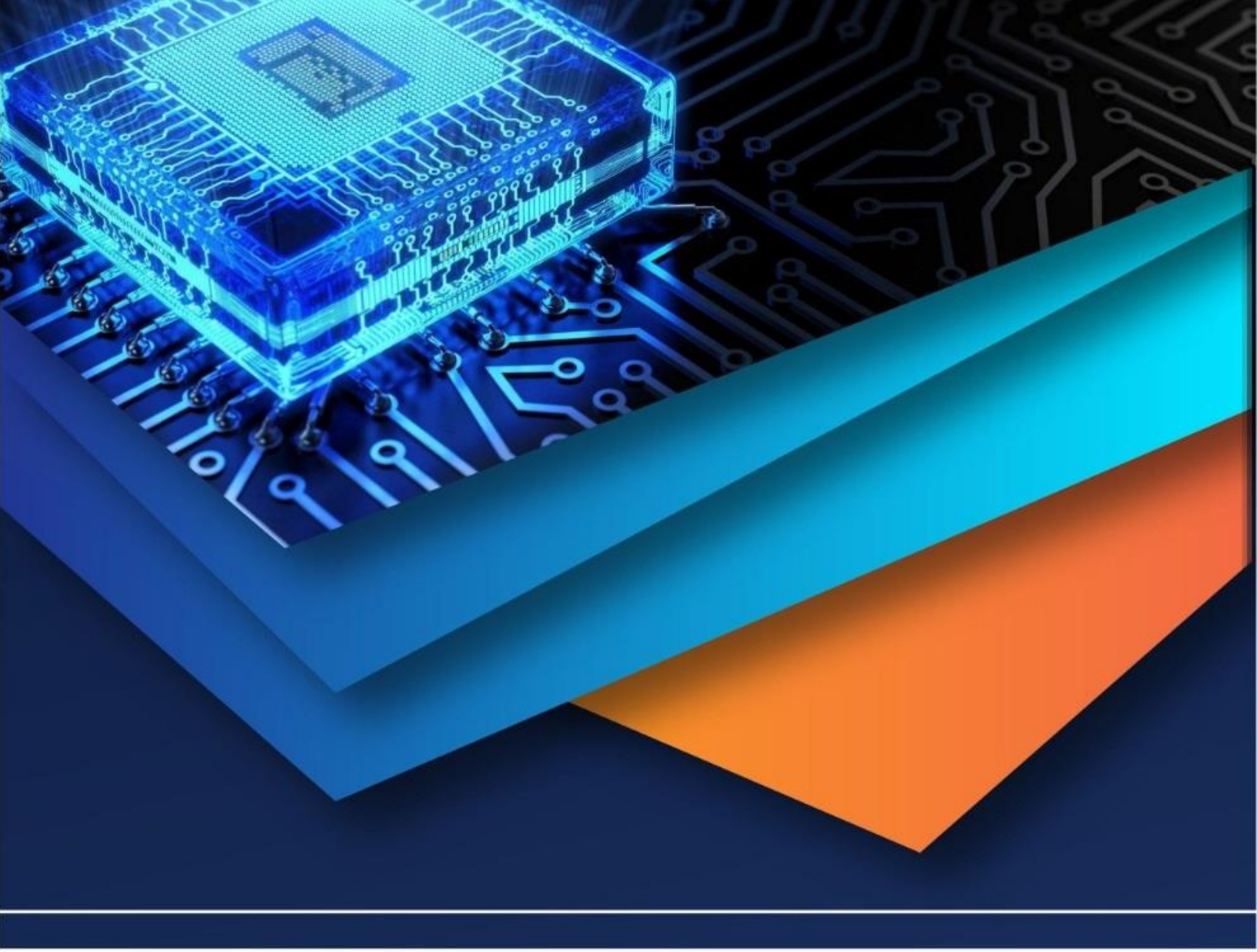
[8] Kumari, K., Mrunalini, M. Detecting Denial of Service attacks using machine learning algorithms. J Big Data 9, 56 (2022). https://doi.org/10.1186/s40537-022-00616-0

[9] Salahuddin MA, Pourahmadi V, Alameddine HA, Bari MF, Boutaba R. Chronos: Ddos attack detection using time-based autoencoder. IEEE Transactions on Network and Service Management. 2021 Jun 10;19(1):627-41.

[10] Fouladi RF, Kayatas CE, Anarim E. Statistical measures: Promising features for time series based DDoS attack detection. InProceedings 2018 Jan 10 (Vol. 2, No. 2, p. 96). MDPI.

[11] Lee SM, Kim DS, Lee JH, Park JS. Detection of DDoS attacks using optimized traffic matrix. Computers & Mathematics with Applications. 2012 Jan 1;63(2):501-10.

[12] Zhou L, Zhu Y, Zong T, Xiang Y. A feature selection-based method for DDoS attack flow classification. Future Generation Computer Systems. 2022 Jul 1;132:67-79.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY