Balaji. L, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Evolving Malware and DDoS Attacks: Decadal Longitudinal Study

Balaji. L, Professor Dr.Prasanna.S
Department of Computer Application- PG
VISTAS Chennai

Abstract- With the emergence of network-based computing technologies like Cloud Computing, Fog Computing, and IoT (Internet of Things), the context of digitizing confidential data over the network is being adopted by various organizations where the security of that sensitive data is considered a major concern. Over a decade there has been a massive growth in the usage of the internet along with the technological advancements that demand the need for the development of efficient security algorithms that could withstand various patterns of security breaches These attacks take advantage of specific limitations that apply to any arrangement asset, such as the framework of the authorized organization's site. In the existing research study, the author worked on an old KDD dataset. It is necessary to work with the latest dataset to identify the current state of DDoS attacks. This paper used a machine learning approach for DDoS attack types classification and prediction For this purpose, used LSTM and CNN classification algorithms. To access the research proposed dataset UNWS-np-15 extracted a complete framework for DDoS attack prediction to get better accuracy.

Keywords: Network-based computing technologies, Cloud Computing, Fog Computing, Internet of Things (IoT)

I. INTRODUCTION

Now with the advent of 4G, 5G networks, and economic smart devices, there is a massive growth in the usage of the internet that has become a part of daily life. A vast range of services provided over the Internet in diverse application areas such as business, entertainment, education, etc. made it a vital component in framing various business models. This context made security over wireless networks the most important factor while using the internet from unsecured connections Different security algorithms and frameworks are developed to enable protection from Internet-based attacks while devising high-performance IDS (Intrusion detection systems) which act as a defensive wall while confronting the attacks over internet-based devices. Distributed architecture-based computing environments like cloud computing and IoT are more prone to DDoS attacks in which multiple devices are coordinated to launch attacks over distributed targets. DDOS attacks are primarily launched in the context of exhausting the connectivity and the processing of the target server resources. It enables the access constraints to the legitimate users to utilize the services provided by the target server which leads towards the partial unavailability or total unavailability of the services. The phenomenon of distributed computing is based on the one-to-many dimension in which these types of attacks may cause a possible amount of damage to the server resources.

II. OBJECTIVE

Therefore, this paper aims to show the process of detection of prototype DDoS attacks using a supervised learning model of the data based on the operational variables: rate of false positives, rate of false negatives, and rate of classification and then

© 2025 Balaji. L. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

sends the information to corresponding training and testing sets With the selected attributes, various machine learning models, like proposed methods based on lstm and CNN are developed for efficient detection of DDoS attacks.

This paper first studies how to launch such attacks and verifies the effectiveness of such attacks. Then, by extracting the four features related to the flow rules, the feature data set for detecting such attacks is established, and the FM-based detection method for low-rate DDoS attacks in SDN is proposed.

III. LITERATURE REVIEW

Machine Learning-Based Network Vulnerability Analysis Of Industrial Internet Of ThingsProposed a recurrent neural network model for classification intrusion detection. They compared other deep learning models with RNN. Finally, they found that RNN is the best model for intrusion detection by using the KDD dataset. Yijing Chen et al. [12] proposed a domain that generates an algorithm for botnet classification. It was a multiple-classification problem. They used advanced deep learning LSTM for multiple classification problems. They found good results with 89% average accuracy for the proposed work.

An Iot-Focused Intrusion Detection System Approach Based On Preprocessing Characterization For Cybersecurity Datasets proposed two benchmark datasets, especially UGR16 and UNSW-NB15, and the most used dataset KDD99 were used for evaluation. The pre-processing strategy is evaluated based on scalar and standardization capabilities. These pre-processing models are applied through various attribute arrangements. These attributes depend on the classification of the four sets of highlights: basic associated highlights, content quality, fact attributes, and finally the creation of highlights based on traffic and traffic quality based on associated titles Collection. The goal of this inspection is to evaluate this arrangement by using different information pre-processing methods to obtain the most accurate model. Our proposition shows that by applying the order of organizing traffic and some preprocessing strategies, the accuracy can be improved by up to 45%. The pre-processing of a specific quality set takes into account more prominent accuracy, allowing AI calculations to effectively group these boundaries identified as potential attacks.

Machine Learning Classification Of Port Scanning And DDoS Attacks: A Comparative Analysis proposed AI calculations were prepared and tried on the latest distributed benchmark dataset (CICIDS2017) to distinguish the best performance calculations on information, which contains the latest vectors of port checks and DDoS attacks. The permutation results show that every variation of isolation check and support vector machine (SVM) can provide high test accuracy, for example, more than 90%. According to the abstract scoring criteria cited in this article, 9 calculations from a bunch of AI tests received the most noteworthy score (highest) because they gave more than 85% representation (test) accuracy in 22 absolute calculations. In addition, this related investigation was also conducted to note that through the k-fold cross approval, the area under the curve (AUC) check of the receiver operating characteristic (ROC) curve, and the use of principal component analysis (PCA) for size reduction in preparation for AI execution model. When considering such late attacks, it was found that many checks on different AI calculations of the CICIDS2017 datasets were not sufficient for port checks and DDoS attacks.

A Novel Video Steganography-Based Botnet Communication Model In Telegram Sns Messenger proposed a video steganography botnet model. In addition, they plan to use another video steganography technology based on the payload method (DECM: Frequency Division Embedded Component Method), which can use two open devices VirtualDub and Stegano to implant significantly more privileges than existing tools information. They show that the proposed model

can be performed in the Telegram SNS courier, and compared the proposed model and DECM with the current image steganography-based botnets and methods in terms of effectiveness and imperceptibility.

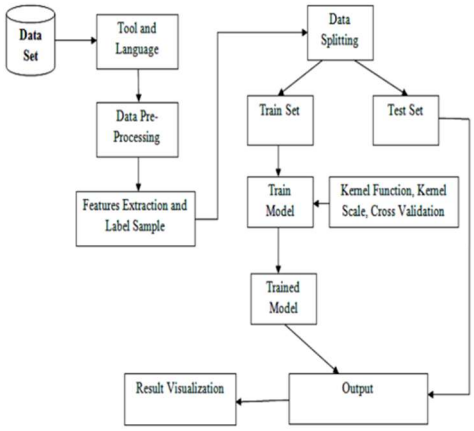
Detection Of Distributed Denial Of Service Attacks Using Automatic Feature Selection With Enhancement For Imbalance Dataset I became familiar with a model that can identify and arrange distributed denial of service attacks that rely on the use of the proposed program including selected segments of neural tissue. The experimental results of the CIC-DDoS 2019 dataset show that our proposed model beats other AI-based models to a large extent. We also studied the selection of weighted misfortune and the choice of pivotal misfortune in taking care of class embarrassment.

Advantage Of Ddos Attack:

Machine learning is an extensive way to detect DDoS attacks with no chance of overfitting or collinearity.

- Monitors unknown behaviors.
- Detects unknown attacks.
- Decrease limitations problem
- Low alarm measure, low false positive rate.
- Signature-based NIDs are very precise.
- Fast detection period.
- Based on well-known DoS attack patterns

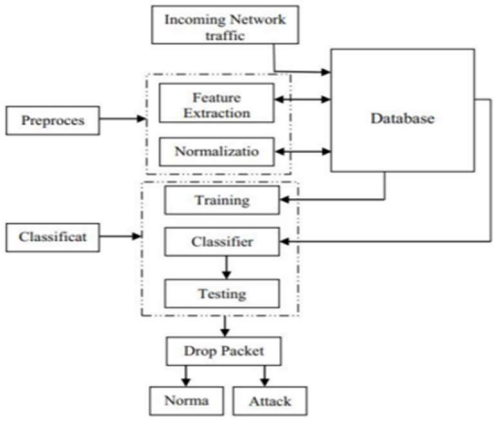
IV. ARCHITECTURE DIAGRAM



Module Data and Methods

- Data Preparation
- Data Normalization
- Feature Engineering
- Machine Learning
- DDoS Attack
- Training
- Testing

Modules Design



Input Design & Output Design

Input Design

The input design is the link between the information system and the user. It comprises the developing specifications and procedures for data preparation and those steps are necessary to put transaction data into a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps, and keeping the process simple. The input is designed in such a way that it provides security and ease of use while retaining privacy.

Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog guides the operating personnel in providing input.

- Methods for preparing input validations and steps to follow when errors occur.

Objectives

Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

It is achieved by creating user-friendly screens for the data entry to handle large volumes of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulations can be performed. It also provides record viewing facilities.

When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to another system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source of information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

Designing computer output should proceed in an organized, well-thought-out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can be used easily and effectively. When analyzing design computer output, they should Identify the specific output that is needed to meet the requirements.

Select methods for presenting information.

Create documents, reports, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status, or projections of the Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

V. RESULT

DDoS attack analysis and detection were performed using machine learning methods. In this work, a subset of the CICIDS2017 dataset was utilized, which included 10K samples of DDoS and Benign classes. The data contained 84 categorical and numerical features in total, where one feature was dropped, so feature engineering and machine learning model development was completed with 83 features. A correlation analysis and feature importance exploration using a decision tree was employed in feature engineering. Also, the results of machine learning models, which included decision trees and linear support vector machine models, demonstrated that DDoS and Benign attacks were classified where accuracy rates of around 100% were achieved. The replication of the original paper was completed, and other machine-learning models can be considered for future work.

System design

VI. CONCULSION

DDoS attacks become increasingly complicated and reach massive sizes. Even though it is not inevitable for organizations to sustain DDoS attacks, they are not unavoidable. No matter how large and complicated such attacks are, it is possible to be affected the least by such attacks if necessary and

sufficient preparations are in place. Case studies described under the heading 'True Events' are the best examples of this. Planned defense actions on the axis of Technology will be important in corroborating the resilience of organizations against DDoS attacks. To summarize the main topics about DDoS protection and defense:

- To ensure, consistent monitoring and to improve the security service and components necessary at external, edge, and middle layers;
- To create and keep up-to-date processes, procedures, and directives for DDoS protection;
- To make sure that the personnel responsible for DDoS protection is technically and administratively trained;
- To test the systems and applications for DDoS and load testing after any major changes or before commissioning any new applications or periodically; and
- To test the components of people-process-technology through drills and to apply any necessary improvements.

Future Enhancement

Future enhancements of this project include integrating real-time threat monitoring to detect and mitigate DDoS attacks dynamically. Expanding the model with advanced deep-learning techniques can further improve classification accuracy and adaptability. Incorporating automated incident response mechanisms will enhance cybersecurity resilience. Additionally, updating the dataset with emerging attack patterns will ensure the system remains effective against evolving threats.

REFERENCE

1. Henze, M.; Matzutt, R.; Hiller, J.; Erik, M.; Ziegeldorf, J.H.; van der Giet, J.; Wehrle, K. Complying with Data Handling Requirements in Cloud Storage Systems. IEEE Trans. Cloud Comput. 2020,
2. González-Martínez, J.A.; Bote-Lorenzo, M.L.; Gómez-Sánchez, E.; Cano-Parra, R. Cloud computing and education: A state-of-theart survey. Comput. Educ. 2015, 80, 132–151.
3. Huttunen, J.; Jauhiainen, J.; Lehti, L.; Nylund, A.; Martikainen, M.; Lehner, O. Big data, cloud computing and data science applications in finance and accounting. ACRN Oxf. J. Financ. Risk Perspect. 2019, 8, 16–30.
4. Heck, M.; Edinger, J.; Schaefer, D.; Becker, C. IoT Applications in Fog and Edge Computing: Where Are We and Where Are We Going? In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICN), Hangzhou, China, 30 July–2 August 2018; pp. 1–6.
5. Kaur, J.; Agrawal, A.; Khan, R.A. Security Issues in Fog Environment: A Systematic Literature Review. Int. J. Wirel. Inf. Netw. 2020, 27, 467–483.
6. Khan, S.; Parkinson, S.; Qin, Y. Fog computing security: A review of current applications and security solutions. J. Cloud Comput. 2017, 6, 1–22.
7. Sha, K.; Yang, T.A.; Wei, W.; Davari, S. A survey of edge computing-based designs for IoT security. Digit. Commun. Netw. 2020, 6, 195–202.
8. Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A Survey on Security and Privacy Issues in EdgeComputing-Assisted Internet of Things. IEEE Internet Things J. 2020, 8, 4004–4022.
9. Badidi, E.; Ragmani, A. An Architecture for QoS-Aware Fog Service Provisioning. Procedia Comput. Sci. 2020, 170, 411–418.
10. Mebrek, A.; Merghem-Boulahia, L.; Esseghir, M. Efficient green solution for balanced energy consumption and delay in the IoT-Fog-Cloud computing. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–4.
11. Marbukh, V. Towards Fog Network Utility Maximization (FoNUM) for Managing Fog Computing Resources. In Proceedings of the 2019 IEEE International Conference on Fog

Computing (ICFC), Prague, Czech Republic, 24–26 June 2019; pp. 195–200.

12. Naha, R.K.; Garg, S.; Georgakopoulos, D.; Jayaraman, P.P.; Gao, L.; Xiang, Y.; Ranjan, R. Fog computing: Survey of trends, architectures, requirements, and research directions. IEEE Access 2018, 6, 47980–48009.