International Journal of Research and Development in Engineering Science
ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/
Regular Issue, Vol. 6, Issue. 2 (March – April), 2024 , Pages: 4 - 7
Received: 20 April 2024 ; *Accepted* : 24 April 2024 ; *Published*: 25 April 2024
https://doi.org/10.63328/IJRDES-V6RI2P2
Original Paper : Applied Research - Experimental Research Paper

Intrusion Detection System Using Machine Learning Techniques

N Sathish Kumar [1*], A Sirisha [2]

[1*] Department of MCA ,Vignan's Institute of Information and Technology, JNTUK, Duvvada, Andhra Pradesh, India; satish.nallamilli54@gmail.com
[2] Department of Information Technology, Vignan's Institute of Information and Technology, JNTUK, Duvvada, India; aswadhati.sirisha@gmail.com

** Corresponding Author: A Sirisha ; aswadhati.sirisha@gmail.com*

Abstract: Network intrusion detection technology plays a vital role in guaranteeing network security. The primary goal is to continually monitor the current state of the network, identify abnormal behaviour in the network state, and notify network administrators in time. The speed and accuracy of an intrusion detection system (IDS) are important to the availability and dependability of today's network. In response to the difficulties of high false alarm rates, poor detection efficiency, and restricted functionality prevalent in IDS, this study first studies the application of machine learning approaches to network intrusion detection. Since machine learning algorithms can automatically extract characteristics from intrusion data and prevent human feature extraction, an intrusion detection approach based on a decision tree classifier is presented. The approach has been enhanced by integrating the Inception module for optimum separation of intrusion functions. The initialization module employs a classification structure with distinct filters, utilizing varying size classification kernels in each row to operate in several layers, and the diverse features of network incursions in the dataset are identified and categorized by stacking.

Keywords: : IDS, Feature extraction, Decision Tree Classifier, Network Intrusions.

1. Introduction

As computer networks emerged, multiple flaws were promulgated that assailants might take advantage of. An essential element of a secure network is an intrusion detection system (IDS), which maintains a watch on network traffic in order to identify and stop undesirable activity. Network traffic is examined by intrusion detection systems (IDS), which are hardware or software systems that search for any security vulnerabilities or unlawful access. In this text, we will speak about the kinds, operation, and importance of intrusion detection systems in network security. Intrusion Detection System (IDS) types: There are two varieties of IDS: network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS)[1]. Host-Based Intrusion Detection System (HIDS): This type of intrusion detection system keeps track of activity on a single host. Installed on the host itself, HIDS is capable of identifying any dubious behavior taking place there. Files, directories, system queries, and other host activity may all be seen by HIDS. It has the ability to identify any unlawful file deletion, alteration, or access on the host [2-5]. HIDS can also detect any unlawful system call that results in a security violation. Intrusion Detection System (NIDS): This system keeps an eye on network traffic to search for any anomalous activity. NIDS analyzes network traffic to discover any security violations. Any illicit access, denial-of-service attack, port scanning, and other potentially detrimental network intrusions may be detected by NIDS. To efficiently monitor network traffic, NIDS may be strategically positioned across the network.

How IDS operates:

Three phases constitute the operation of an intrusion detection system (IDS): data collection, analysis, and alerting.

Data Collection: The system accumulates information on network traffic, system contacts, and file activity during the initial phase of systems for intrusion detection (IDS). The knowledge is gathered from a number of outlets, such as system records, packet captures, and framework logs.

Analysis: During the examination phase, the IDS searches for any anomalous behavior in the information it gathers. In the analysis phase, the collected information is compared to a database of recognized assault patterns or signatures. The IDS analyzes the data and searches for any irregularities that can point to an attack using machine learning methods.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 6, Issue 2 , 2024 , https://doi.org/10.63328/IJRDES-V6RI2P2

Depending on the kind of IDS, the analysis phase might be rule-based, anomaly-based, or hybrid-based [6-8].

Alerting: If there is any unusual performance, the IDS sends an alert to the security personnel. An email, text message, or any additional means may be employed to distribute the alert. After that, the security personnel may respond adequately to diminish the threat and prevent the network [9].

2. Literature Survey

Numerous studies have been conducted to monitor infiltration throughout the previous 10 years. One of the earliest trends in intrusion detection and vulnerability inspection was given by Bishop [10]. The infrastructure-based rules and processes required for the creation and development of intrusion detection systems are known as intrusion detection trends. Another notably-known study by Kabiri and Ghorbani [11] explored some intrusion detection-related difficulties as well as improvements in IDS. Time consumption, log-file updating, statistical and rule-based analysis, accuracy, and other concerns beset classical IDS.

In their review study, Zamani and Movahedi [12] examined a variety of notable machine learning-based intrusion detection algorithms. Zamani researched the application of machine learning in intrusion detection, which can swiftly adapt to changing intrusive activity and give a high detection rate with a low false-positive rate.

A review of numerous data mining strategies for intrusion detection was undertaken by Agrawal and Agrawal [13]. In addition to being widely deployed in the disciplines of clustering and classification, machine learning approaches in their individual or hybrid forms have also been extensively used for feature selection and dimensionality reduction in intrusion detection systems. The concerns with the datasets being exploited for IDS were explored by Ahmed et al. [14]. The IDS model and its categorization, statistical, information-theoretic, and clustering categories were also examined.

New strategies based on bioinspired approaches are introduced to the statistical method in modern IDS approaches. These strategies mainly rely on the swarm intelligence approach or evolutionary theory [15]. Many criteria, such as convergence, intensification, diversification, CPU time, etc., need to be analyzed in order to establish the most suitable and best-fit selection of bio-inspired algorithms. An evaluation of intrusion detection systems (IDS) leading to an end-to-end secure Internet of Things (IoT) was undertaken by Gendreau and Moorman [16]. The IDS survey makes use of the newest ideas and approaches to advise the present IoT.

The current study trend toward a universal, cross-platform dispersed method has been taken into consideration in order to appreciate and illustrate the contrasts throughout IDS platforms. An overview of the benchmark datasets that are available to intrusion detection researchers for the purpose of training and evaluating their models was presented by Hamid et al. [17].

The details of classes, features, and instances were given by the analysis of several datasets, including ADFA-WD (Australian Defense Force Academy Window Dataset), Caida DDoS (Caida Distributed Denial of Service) Dataset, UNM-Dataset, UNSW-NW15, KDD'99, DARPA 98, and ADFA-Dataset. The most recent suggestion for a detailed assessment and evaluation of machine learning algorithms for intrusion detection comes from Mishra et al. [18].

3. Related Works

3.1. Design

Login: This is the starting phase where you will enter your login credentials and tries to login.

Verify Details: The second phase where the verification of the login details will be done to check whether the user is an authorized one or not.

Invalid: If the login credentials are not accurate then it will not logged in.

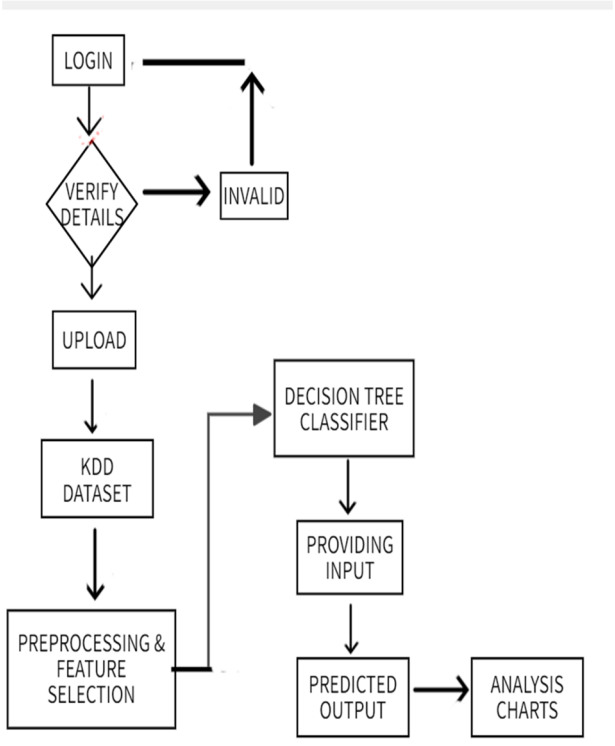


Fig.1 System Architecture

Upload: The KDD dataset need to be uploaded in the upload page to train the data.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 6, Issue 2 , 2024 , https://doi.org/10.63328/IJRDES-V6RI2P2

Preprocessing & Feature Selection: To get raw data ready for the machine learning model, preprocessing and feature selection are essential procedures. Their combined efforts boost the IDS's performance and efficiency.

Decision Tree Classifier: A classification-focused machine learning algorithm. In order to make a final call or forecast, it constructs a model like a tree that divides the data according to characteristics (attributes).

Providing Input: The various network attributes for a particular network will be given as an input so that the it the algorithm will predict the output.

Output: The result based on the input whether it is a normal or an intrusion based on the types of intrusions it will be classified in to various types.

Charts Analysis: Based on the outputs and our datasets the chart analysis will give a brief introduction about the intrusions.

4. Result and Discussion

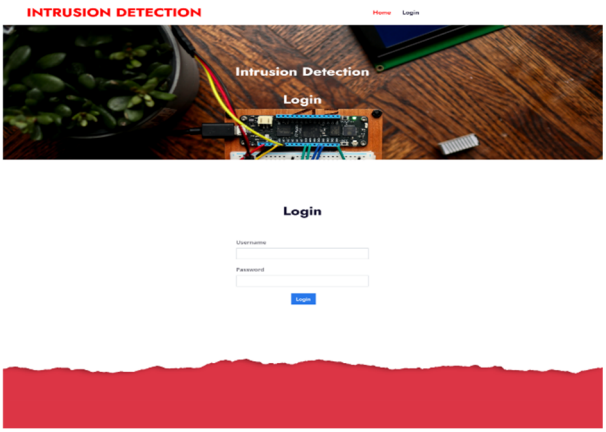
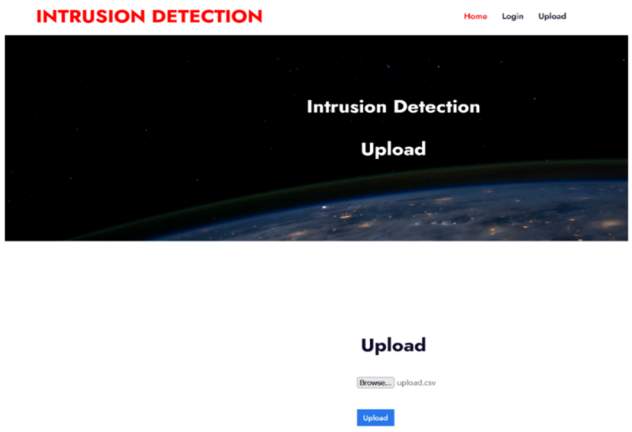


Fig.2 Web Application Login



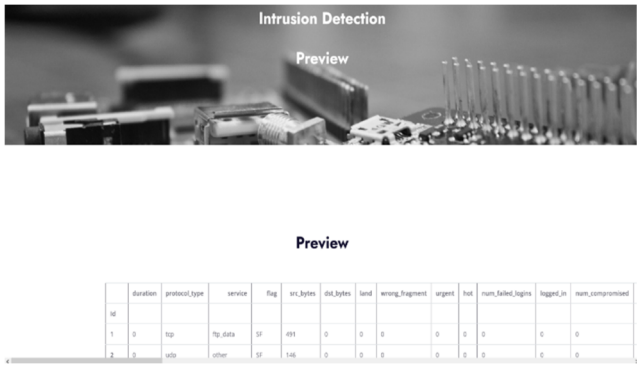


Fig.3 Data Collection and Training System

Fig.4 Data Output Analysis

5. Conclusion and Future Scope

In summary, the proposed intrusion detection system leveraging a decision tree classifier offers numerous improvements over the existing powerful convolutional neural network-based technique. The recommended approach provides astounding precision, with a training and validation accuracy of 99%. It also offers improved transparency, reduced computing demands, tolerance for noisy data, flexibility, and a powerful tool for safeguarding data and systems against hostile attacks. The project was split into numerous phases, including data gathering, material preparation, model selection, analysis and prediction, test set accuracy, and learning model storage.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 6, Issue 2 , 2024 , https://doi.org/10.63328/IJRDES-V6RI2P2

Each module played a crucial role in the creation of the recommended intrusion detection system. Overall, the recommended approach may be applied to discover network risks instantly, making it a significant tool for privacy specialists and enterprises. The system may be modified with novel data or features to adapt to evolving threats, making it an obtainable and robust network security solution. In the future, the aforementioned intrusion detection system will operate on the basis of predetermined incursions in the form of datasets, but it may be extended by applying the infrastructure itself to the ML algorithms.

References

[1]. Szegedy C, Ioffe S, Vanhoucke V, et al. Inception-v4, inception resent and the impact of residual connections on learning[C]//Thirty-first AAAI conference on artificial intelligence. 2017.

[2]. B. S. Sharma, "Post-translational modifications (PTMs), from a cancer perspective: an overview," Oncogen Journal, vol. 2, no. 3, p. 12, 2019.

[3]. Kingma D P, Ba J. Adam: A method for stochastic optimization[J]. arXiv preprint arXiv:1412.6980, 2014.

[4]. Y. Yang and G. E. Gibson, "Succinylation links metabolism to protein functions," Neurochemical Research, vol. 44, no. 10, pp. 2346–2359, 2019.

[5]. P. Montague and J. Kim, "An efficient semi-supervised SVM for anomaly detection," 2017 International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, 2017, pp. 2843-2850.

[6]. Owezarski P, Mazel J, Labit Y. 0day anomaly detection made possible thanks to machine learning[C]// 2010.

[7]. A. Sreedhar, E. K. Wiese, and T. Hitosugi, "Enzymatic and metabolic regulation of lysine sacculation," Genes & Diseases, vol. 7, no. 2, pp. 166–171, 2020.

[8]. A. Martín-Martín, M. Thelwall, E. Orduna-Malea, and E. D. López-Cózar, ''Google scholar, Microsoft academic, scopus, dimensions, web of science, and OpenCitations' COCI: A multidisciplinary comparison of coverage via citations,'' Scientometrics, vol. 126, no. 1, pp. 871–906, Jan. 2021.

[9]. Microsoft. Microsoft Academic. Accessed: Dec. 20, 2020. [Online]. Available: https://academic.microsoft.com.

[10]. M. Bishop, ''Trends in academic research: Vulnerabilities analysis and intrusion detection,'' Comput. Secur., vol. 21, no. 7, pp. 609–612, Nov. 2002.

[11]. P. Kabiri and A. A. Ghorbani, ''Research on intrusion detection and response: A survey,'' Int. J. Netw. Secur., vol. 1, no. 2, pp. 84–102, 2005.

[12]. M. Zamani and M. Movahedi, ''Machine learning techniques for intrusion detection,'' 2013, arXiv:1312.2177.

[13]. S. Agrawal and J. Agrawal, ''Survey on anomaly detection using data mining techniques,'' Proc. Comput. Sci., vol. 60, no. 1, pp. 708–713, 2015.

[14]. M. Ahmed, A. N. Mahmood, and J. Hu, ''A survey of network anomaly detection techniques,'' J. Netw. Comput. Appl., vol. 60, pp. 19–31, Jan. 2016.

[15]. D. Camacho, ''Bio-inspired clustering: Basic features and future trends in the era of big data,'' in Proc. IEEE 2nd Int. Conf. Cybern. (CYBCONF), Jun. 2015, pp. 1–6.

[16]. A. A. Gendreau and M. Moorman, ''Survey of intrusion detection systems towards an end-to-end secure Internet of Things,'' in Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud), Aug. 2016, pp. 84–90.

[17]. Y. Hamid, Balasaraswathi, V. Ranganathan, L. Journaux, and M. Sugumaran, ''Benchmark datasets for network intrusion detection: A review,'' Int. J. Netw. Secur., vol. 20, no. 4, pp. 645–654, 2018.

Author's Profile

N. Satish Kumar pursuing MCA in Vignan's Institute of Information and Technology (A) from 2022-2024.

A. Sirisha Completed MCA from TJPS College Guntur in 2009 and M.Tech in Pragati engineering college, Kakinada in 2014. Presently pursuing Ph.D. from VFSTR, vadlamudi, Guntur in the domain of Network security. She is currently working as assistant Professor in Department Of IT, VIIT, Duvvada, Visakhapatnam. She has 14 years of academia experience. Her main research focuses on Network Security and Machine Learning.