ScienceDirect

Materials Today: Proceedings

Volume 68, Part 1, 2022, Pages 26-34

Detection analysis of malicious cyber attacks using machine learning algorithms

R.A. Karthika [a], M. Maheswari [b]

Show more

https://doi.org/10.1016/j.matpr.2022.05.510

Get rights and content

Abstract

Cybersecurity is the practice of safeguarding information and the systems that store or process information. Cybersecurity violations are the foremost persecution instigated by cyber attackers through one or more systems on single or several networks or systems. This kind of cyber threats can ruthlessly trigger data loss or theft besides halting the network systems partially or fully. Among various cybersecurity attacks, the Denial of Service (DoS) attack is one of the most dominant hacking modus operandi over the internet. The hackers use the weapons at their disposal to disrupt traffic in and around the network surroundings or the target system by bombarding it with a lot of malicious requests. This paper introduced machine learning algorithms such as Gaussian Naïve Bayes and Nearest Centroid to identify the attacks via classifying the given dataset into normal and malicious traffic. Furthermore, metrics such as accuracy, f-score, FNR, precision, and prediction time etc., were calculated to identify the best performing model.

Introduction

In this digital world, networks are considered a part of our life. Without it, we can't survive in today's world, i.e. networks benefit the world. With that network, intrusion hazards became very widespread, putting the institution and the networked systems in danger of cyberattacks. Attackers construct several novel techniques to hack the system endlessly. The objective of cybersecurity is to improve situational awareness and shorten the time to respond to threats. Speed of analysis is of crucial importance because an unnoticed attack can cause severe damage to information systems. The network administrators need to look for patterns in traffic that indicate a possible assault and swiftly see the events leading up to an attack. It requires a lot of real-time data to distinguish such suspicious conduct and drill down into the underlying data with a wide variety of tools to help us decide. The most important feature of such systems may be focusing on crucial elements to identify malicious traffic from massive data as individuals cannot deal with it efficiently. There are many approaches in building defence in such scenarios, and one such mechanism is the deployment of an Intrusion Detection System (IDS). It can play a vital role in shielding the network and the connected systems. An IDS is a device used to identify and mitigate such threats by continuously monitoring the traffic of interest. Fig. 1 explains how the IDS device makes the network or systems very secure and safe, i.e. how the IDS stops the hackers or attackers. An IDS device is also known as an Intrusion Prevention System (IPS) when deployed to detect and protect the networked systems in question. IPS systems are promoted as an enhancement to passive IDS, having the ability to intercept the direct line of communication between the source and destination and automatically act on

identified abnormalities. The deployment location is a critical factor in mapping the role as either IDS or IPS.(See Table 1.Table 2.).

Muhammad et. al [6] describes how Network Intrusion Detection system works also how it makes significance to identify intruders in the network environment. Therefore, Intrusion Detection System in network is categorized into two namely:

a. Network based Intrusion detection system (NIDS)

This kind of intrusion detection is highly cost-effective since it scrutinizes inbound network traffics for identifying risk happening in the network region. The NIDS monitors entire network traffic via linked hosts, and from that connected hosts information, it finally makes their assessment. A NIDS deployed correctly is quite helpful in discovering threats on the network in question. It works by snooping in on the raw traffic on the wire using one or more network taps placed throughout the network or in line with the traffic flow.

b. *Host* based *Intrusion detection system (HIDS)*

This formulates decision-based on information handover by every single user in the network. It allows an assortment of data from every single host in the network, providing good results rather than monitoring the entire network. Usually, a HIDS will be deployed to many hosts rather than a few key monitoring points like a NIDS. A HIDS detects bad actors on a particular host. HIDS operate within the host domain and are usually far more varied than NIDS.Stephen et. al [11] suggested NIDS and also HIDS for detecting intruders entering in the network either to steal data or to hack the network system. The left figure indicates NIDs and right figure indicates HIDS in Fig. 2. When compare to HIDS, monitoring power is high in NIDS which may interrupt attacks.

The main objective of this study related to detection and classification of intruders in networks are specified as follows:

- To study and analyze the intrusion detection system in computer network security based on feature extraction, statistical analysis, training and testing, utilizing supervised machine learning for classifying the attacks in the networks.
- To find metrics such as accuracy, f-score, FNR, prediction time and also precision to predict the model performance in classifying malicious and normal.
- Perform statistical analysis in which training and testing datasets that gives variation from some other researchers.
- Construct machine learning algorithms like Gaussian Naïve Bayes, Nearest Centroid algorithm to distinguish the dataset as normal and malicious.

Section snippets

Background

Hoda et. al [3] introduced data mining approaches to identify as well as classification of attacks in the network through performance calculation of J48 decision tree algorithm which contrast with two rule based algorithms such as decision table and also oneR. In this work, decision tree algorithm achieves better outcome of more than 99%.Rohan et. al [8] exhibited Internet of Things to monitor certain network activities to update feature extraction which results in greater accuracy detection of …

Proposed **architecture**

The proposed schematic diagram is explained as following steps which is shown in Fig. 3.

The first and foremost step is to collect data from specified source mainly KDD cup 99 dataset regarding DoS attack. The next step is data pre-processing in which reduction of unnecessary features (data samples contains 38 features

which is further reduced to 29 features) and also dimensionality reduction. This paper mainly presented a statistical analysis for finding attackers in the networks. It undergoes…

Results and discussions

The metrics calculation had been found using Gaussian Naïve Bayes algorithm with 180, 1803, 18,035 samples as 1%, 10%, 100% training samples to identify better accuracy.…

Conclusions

This study showed that the statistical analysis and machine learning approaches could complement each other and make the DoS detection more efficient. Furthermore, it also proves that the attack detection can accurately differentiate both the normal and malicious (DoS) traffic. We developed two machine learning algorithms such as Gaussian Naïve Bayes and Nearest Centroid, to identify and categorize the network traffic as either normal or attack. Moreover, metrics evaluations like accuracy,…

CRediT authorship contribution statement

R.A. Karthika: Supervision, Writing – original draft, Resources, Investigation, Formal analysis, Validation, Conceptualization. **M. Maheswari:** Writing – review & editing, Investigation, Formal analysis, Validation, Methodology, Software.…

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.…

Special issue articles Recommended articles

References (14)

A. Sanmorino
A study for DDOS attack classification method
J. Phys.: Conf. Ser. (2019)

I. Ahmad *et al.*
Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection
IEEE Access (2018)

HodaWaguih “A Data Mining Approach for the Detection of Denial of Service Attack”, IAES International Journal of...

Khaled Elleithy, Wang Cheng “Denial of Service Attack Techniques: Analysis, Implementation and Comparison”, SYSTEMICS,...

Kok S.H, Azween Abdullah, Mahadevan Supramaniam, ThulasyammalRamiah Pillai, Ibrahim AbakerTargio Hashem “A Comparison...

Muhammad K. Asif, Talha A. Khan, Talha A. Taj, Umar Naeem, Sufyan Yakoob “Network Intrusion Detection and its Strategic...

S.M. Othman *et al.*
Intrusion detection model using machine learning algorithm on Big Data environment

J. Big Data (2018)

There are more references available in the full text version of this article.

Cited by (2)

Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City ↗
2023, Sustainability (Switzerland)

Man-in-the-middle and denial of service attacks detection using machine learning algorithms ↗
2023, Bulletin of Electrical Engineering and Informatics

View full text