INTRUSION DETECTION SYSTEM WITH MACHINE LEARNING ALGORITHMS AND COMPARISON ANALYSIS

A Project Work Synopsis

Submitted in the partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE WITH SPECIALIZATION IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Submitted by:

21BCS8804

JAIN KARAN ANAND

Under the Supervision of:

<Prof. Siddharth Kumar >

CHANDIGARH UNIVERSITY, GHARUAN, MOHALI - 140413,
PUNJAB, September, 2022

Abstract

The incremental increase in the usage of technology has led to an increase in the amount of data that is being processed over the Internet significantly over the time period. With the huge amount of data that is being flown over the Internet, comes the scenario of providing security to the data, and this is where an Intrusion Detection System (IDS) comes into the picture and helps in detecting any virtual security threats. Intrusion Detection System (IDS) is a system that monitors and analyzes data to detect any intrusion in the system or network. Intruders find different ways to penetrate into a network. The IDS which is being proposed is being implemented using latest technologies such as Machine Learning Algorithms to classify the attacks and detecting them whenever an attack happens and also to find which machine learning algorithm is best suitable for identifying the attack.

Keywords:

Intrusion, Intrusion Detection System, Denial of service, User to Root attacks, Remote to User attacks, Local Area Network, Principal Component Analysis, Support Vector Machine, Random Forest, Decision Tree, KNN Algorithm, Logistic Regression, Alerts, False Positives, False Negatives.

Table of Contents

1. INTRODUCTION

1.1 Problem Definition

An Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

Although Intrusion Detection Systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

1.2 Problem Overview

Intrusion detection begins where the firewall ends. Preventing unauthorized entry is best, but not always possible. It is important that the system is reliable and accurate and secure. Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential Vulnerabilities and attacks in progress.

1.3 Hardware Specification

Processor	: Any Processor above 500 MHz.
Ram	: 4 GB
Hard Disk	: 4 GB
Input device	: Standard Keyboard and Mouse.
Output device	: VGA and High Resolution Monitor.

1.4 Software Specification

Operating System	: Windows 7 or higher
Programming	: Python 3.6 and related libraries

2. LITERATURE SURVEY

2.1 Existing System

In existing work, a security system, which collects forensic features for users at command level rather than at SC level, by invoking data mining and forensic techniques, was developed. Moreover, if attackers use many sessions to issue attacks, e.g., multistage attacks, or launch DDoS attacks, then it is not easy for that system to identify attack patterns. Hu et al. presented an intelligent lightweight IDS that utilizes a forensic technique to profile user behaviors and a data mining technique to carry out cooperative attacks. The authors claimed that the system could detect intrusions effectively and efficiently in real time. However, they did not mention the SC filter.

2.2 Proposed System

In our proposed method, Decision Tree, Logistic regression, Random Forest and KNN is developed as learning methods in solving the classification problem of pattern recognition and intrusion identification.

Compared with other classification algorithms, Decision Tree, Logistic regression, Random Forest and KNN can better solve the problems of small samples, nonlinearity and high dimensionality.

2.3 Literature Review Summary **(Minimum 7 articles should refer)**

Year and Citation	Article/ Author	Tools/ Software	Technique	Source	Evaluation Parameter
2010	**Vipin, Das & Vijaya, Pathak**		IDS, RST, SVM, PCA		
2013	**Choi, J & Choi, Chang & Ko, Byeongkyu**		DDoS Attack, HTTP GET Flooding Attack, Web Security, MapReduce		
2012	**Gamboa, Karen & Monroy, Raúl & Trejo**		HMM , Sequiter		

3. OBJECTIVES

The objective of an Intrusion Detection System (IDS) is to ensure the security and reliability of a system. It works by identifying intrusions and generating alerts based on predefined rules for any detected intrusions within a network or system. There are two main categories of IDS: Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection System (NIDS). HIDS monitors the internal components of a computing system while NIDS monitors network traffic for unauthorized access or suspicious activity. The detection method used by IDS can be Signature-based or Anomaly-based. However, IDS can produce false alarms, and when developing an IDS, it is crucial to keep the false alarm rate as low as possible compared to other existing IDS.

The process of detecting an intrusion occurs beyond the firewall's scope. While prevention of unauthorized access is preferable, it may not always be feasible. Intrusion Detection refers to the real-time surveillance and examination of data and network activity to identify potential vulnerabilities and ongoing attacks.

4. METHODOLOGY

Proposed smart intrusion detection system (IDS) is viewed as an effective solution for network security and protection against external threats. However, the existing IDS often has a lower detection rate under new attacks and has a high overhead when working with audit data, and thus machine learning methods have been widely applied in intrusion detection.

In our proposed method, Decision Tree, Logistic regression, Random Forest and KNN is developed as learning methods in solving the classification problem of pattern recognition and intrusion identification.

Compared with other classification algorithms, Decision Tree, Logistic regression, Random Forest and KNN can better solve the problems of small samples, nonlinearity and high dimensionality

5.CONCLUSION

The main aim of Intrusion Detection System is to detect the attacks and malicious activities that occur within a network and to reduce the rate of false positives. By using the machine learning algorithms, the output of the IDS would be accurate, advanced and reliable. This system also shows the accuracy rate of the attacks that have been detected by the different machine learning algorithms that have been implemented. The incremental increase in the use of technology has led to huge amount of data that needs to be processed and stored securely for the users. Security is a major aspect for any user. If a system is secure, we can highly ensure user’s privacy is high. The more secure the system, the more reliable it is. If an Intrusion Detection System is capable of providing good security for user’s data, we can say that the developed Intrusion Detection System is good.

7. REFERENCES

[1] A B. Athira, V. Pathari, “Standardisation and Classification of Alerts Generated by Intrusion Detection Systems”, IJCI, International Journal on Cybernetics & Informatics, Vol 5 Issue 2, 2016.

[2] Johansson Daniel, Andersson Par, “Intrusion Detection Systems with Correlation Capabilities”

[3] Yasm Curt, “Prelude as a Hybrid IDS Framework”, March, 2009

[4] Kumar Vinod, Sangwan Prakash Om, “Signature Based Intrusion Detection System Using SNORT”, IJCAIT, International Journal of Computer Applications & Information Technology, Vol. I, Issue III, November 2012.

[5] Singh Deepak Kumar, Gupta Jitendra Kumar, “An approach for Anomaly based Intrusion detection System using SNORT“, IJSER, International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September 2013.

[6] S, Vijayarani, and Maria Sylviaa S. “Intrusion Detection System – A Study”, IJSPTM, International

Journal of Security, Privacy and Trust Management ,Vol 4, Issue 1, pp. 31–44, February 2015.