"In Pursuit of Technical Excellence"

INTRUSION DETECTION SYSTEM USING ML

For the Degree of

Bachelor of Engineering

In

Information Technology

Submitted By

ANAND INGLE	**BE16S06F006**
AKSHAY CHACHARKAR	**BE15F06F008**
HITESH TAPDIYA	**BE15F06F054**
VISHAL POTGANTE	**BE15F06F043**

Under the Guidance of

Prof. S. M. Chavan

Department of Information Technology

Government College of Engineering, Aurangabad

Maharashtra State, India

(An autonomous Institute of Government of Maharashtra)

(2018-19)

CERTIFICATE

This is to certify that the thesis entitled **"Intrusion Detection System Using ML",** which is being submitted herewith for the award of the **'Degree of Bachelor of Engineering'** in **'Information Technology'** of Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. This is the result of the research work and contribution by **'Anand M. Ingle, Akshay B. Chacharkar, Hitesh A. Tapdiya, Vishal B. Potgante'** under my supervision and guidance.

Place: Aurangabad.
Date :

Prof. S. M. Chavan
Project Guide
(Information Technology Department)

Prof. C. M. Gaikwad
Head of Department
(Information Technology Department)

Dr. P. B. Murnal
Principal
Government College of Engineering,
Aurangabad (M.S) – 431005

ABSTRACT

An Intrusion Detection System (IDS) is a software that monitors a single or a network of computers for malicious activities (attacks) that are aimed at stealing or censoring information or corrupting network protocols. Most techniques used in today's IDS are not able to deal with the dynamic and complex nature of cyber-attacks on computer networks. Hence, efficient adaptive methods like various techniques of machine learning can result in higher detection rates, lower false alarm rates and reasonable computation and communication costs. It attempts to identify intrusions, which we define to be unauthorized uses, misuses, or abuses of computer systems by either authorized users or external perpetrators. Some IDSs monitor a single computer, while others monitor several computers connected by a network. IDSs detect intrusions by analyzing information about user activity from sources such as audit records, system tables, and network traffic summaries.

Intrusion detection is the process of dynamically monitoring events occurring in a computer system or network, analyzing them for signs of possible incidents and often interdicting the unauthorized access. This is typically accomplished by automatically collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems.

Traditional intrusion detection and prevention techniques, like firewalls, access control mechanisms, and encryptions, have several limitations in fully protecting networks and systems from increasingly sophisticated attacks like denial of service. Moreover, most systems built based on such techniques suffer from high false positive and false negative detection rates and the lack of continuously adapting to changing malicious behaviors. In the past decade, however, several Machine Learning (ML) techniques have been applied to the problem of intrusion detection with the hope of improving detection rates and adaptability.

INDEX

LIST OF ABBREVIATIONS

IDS	Intrusion Detection System
DOS	Denial of Service
DDOS	Distributed Denial of Service
IP	Internet Protocol
TCP	Transmission Control Protocol
DARPA	Defense Advanced Research Projects Agency
ML	Machine Learning
API	Application Programming Interface
NSS	National Security Strategy
LAN	Local Area Network
WAN	Wide Area Network
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 The Introduction of an IDS

There are many types of dangers on the internet, including malware and DDOS attacks. A network can be protected against such attacks using an intrusion detection system. An IDS system can detect intrusions and intrusion de-generates an alert when it detects an intrusion. This intrusion detection system in a network analyses all traffic. For large datacentres this is a difficult task. There's an enormous amount of data through the network of a datacentre. Standard intrusion systems cannot then all traffic completely. A way to fix this is by IP flows is regeneration of packet data. Using IP flows ensures that an intrusion detection system can check all traffic. Intrusion detection systems also require a lot of maintenance. This depends on course and also involves high cost. Sensitive data is also increasingly being stored digitally. All these new services could contain security flaws which could leak private data, such as passwords or other sensitive data. This means that security flaws become more and more important since they can cause so much damage.

1.2 Need of this Project

It is not just the leaking of sensitive data that is an issue, but also protecting a computer or network against malware is important. Considering this, it becomes more important to be able to detect and prevent attacks on network systems. Intrusion detection systems are used for this purpose. An intrusion detection system can alert administrators of malicious behaviour. In order to have good performance, most intrusion detection systems need a lot of manual maintenance. This thesis tries to find out whether an intrusion detection system can work out-of-the-box with an acceptable performance. This is done by using machine learning algorithms. These are algorithms which can learn and find patterns in input. Machine learning algorithms seem promising for the problem of automatic intrusion detection. This thesis tries to view therefore that an intrusion detection system out-of-the-box may have a good performance. This is done via machine learning algorithms. These are algorithms that can learn from data and patterns. This seems well applicable to the problem of intrusion detection, this will also view this thesis, as well as the algorithms may or may not work.

The term intrusion refers to any unauthorized access that attempt to compromise confidentiality, integrity and availability of information resources. In general, we can say that any malicious use or misuse of any entity in a network can be referred as an intrusion. The intruder tries to find the vulnerability in the security system and then prepare for attack. Intrusion detection is the process of fast detection of unwanted violation in system’s normal behaviour due to attacks performed by the malicious user. Intrusion detection system (IDS) deals with detection of such type of attacks in just in time or real time and report, alert or countermeasure on the attack to the administrator. Now a days, artificial Intelligence, data mining and machine learning algorithms have been subjected to extensive research in intrusion detection with emphasis on improving the accuracy of detection and make an immune model