FINAL Report

Title: IntrusionDetectionSystemforSocialNetworks

Submitted To: SagarPande

Assistant Professor-LPU

Subject: Artificial Intelligence (INT-404)

Project BY

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | REG.NO | ROLL.NO | SECTION |
| R.LOHITH RAJ | 11802342 | 40 | K18GX |

### OVERVIEW

* Network Intrusion Detection (NID) is the process of identifying network activity that can lead to the compromise of a security policy. In this paper, we will look at four intrusion detection approaches, which include ANN or Artificial Neural Network, SOM, Fuzzy Logic and SVM. ANN is one of the oldest systems that have been used for Intrusion Detection System (IDS), which presents supervised learning methods. However, in this research, we also came across SOM or Self Organizing Map, which is an ANN-based system, but applies unsupervised methods. Another approach is Fuzzy Logic (IDS-based), which also applies unsupervised learning methods. Lastly, we will look at the SVM system or Support Vector Machine for IDS. The goal of this paper is to draw an image for hybrid approaches using these supervised and unsupervised methods.

### INTRODUCTION

. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate 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.

### MOTIVATION:-

Using software-based network intrusion detection systems

Like SNORT to detect attack in the network.

Fraud detection involves in the data manipulation, applying

Algorithms and help to gain knowledge about

Intrusion detection using historical network things& IP addresses security.

### \*AIM:-

The aim of the project is as follows

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching.

### \*Scope:-

The scope of this project does not exceed more than a generalized suggestion tool.

### Abstract:-

A computer-implemented intrusion detection system and method that monitors a computer system in real-time for activity indicative of attempted or actual access by unauthorized persons or computers. The system detects unauthorized users attempting to enter into a computer system by comparing user behavior to a user profile, detects events that indicate an unauthorized entry into the computer system, notifies a control function about the unauthorized users and events that indicate unauthorized entry into the computer system and has a control function that automatically takes action in response to the event.

### \*RELATED POINTS:-

### Detection Method of IDS:

### Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Anomaly-based Method:  
Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.

Comparison of IDS with Firewalls:  
IDS and firewall both are related to the network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening

A Packet Decoder: It takes packets from different networks and prepares them for preprocessing or any further action. It basically decodes the coming network packets.

A Preprocessor: It prepares and modifies the data packets and also perform defragmentation of data packets, decodes the tcp streams.

A Detection Engine: It performs the packet detection on basis of Snort rules. If any packet matches the rules, appropriate action is taken, else it is dropped.

Logging and Alerting System: The detected packet is either logged in system files or incase of threats, the system is alerted.

Output Modules: They control the type of output from the logging and alert system

.

### \*BENEFITS OF USING NETWORKS

The network or computer is constantly monitored for any invasion or attack.

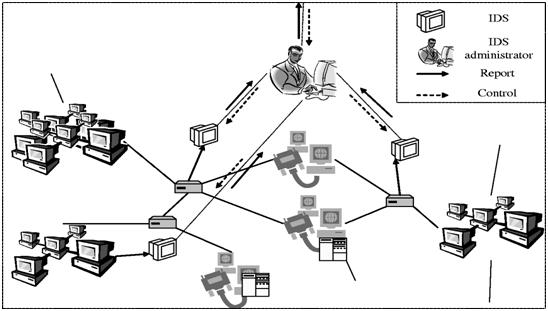
The system can be modified and changed according to needs of specific client and can help outside as well as inner threats to the system and network.

It effectively prevents any damage to the network.

It provides user friendly interface which allows easy security management systems.

Any alterations to files and directories on the system can be easily detected and reported

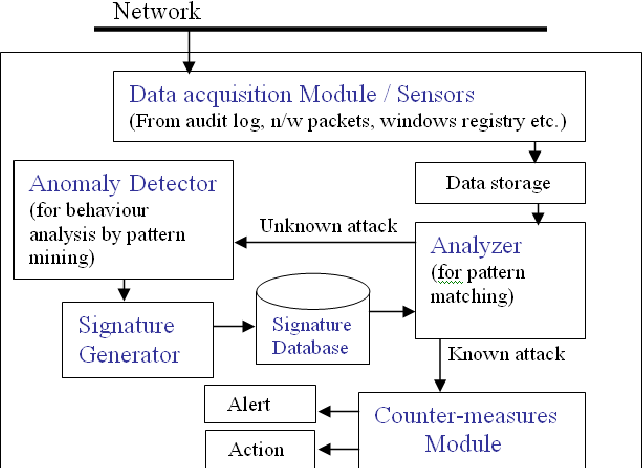
Network Intrusion Detection System: This system monitors the traffic on individual networks or subnets by continuously analyzing the traffic and comparing it with the known attacks in the library. If an attack is detected, an alert is sent to the system administration. It is placed mostly at important points in the network so that it can keep an eye on the traffic travelling to and from the different devices on the network. The IDS is placed along the network boundary or between the network and the server. An advantage of this system is that it can be deployed easily and at low cost, without having to be loaded for each system.

[](https://www.elprocus.com/wp-content/uploads/2013/09/Network-Intrusion-Detection-System.jpg)Network Intrusion Detection System

Host Intrusion Detection System: Such system works on individual systems where the network connection to the system, i.e. incoming and outgoing of packets are constantly monitored and also the auditing of system files is done and in case of any discrepancy, the system administrator is alerted about the same. This system monitors the operating system of the computer. The IDS is installed on the computer. Advantage of this system is it can accurately monitor the whole system and does not require installation of any other hardware.

Host Intrusion Detection System

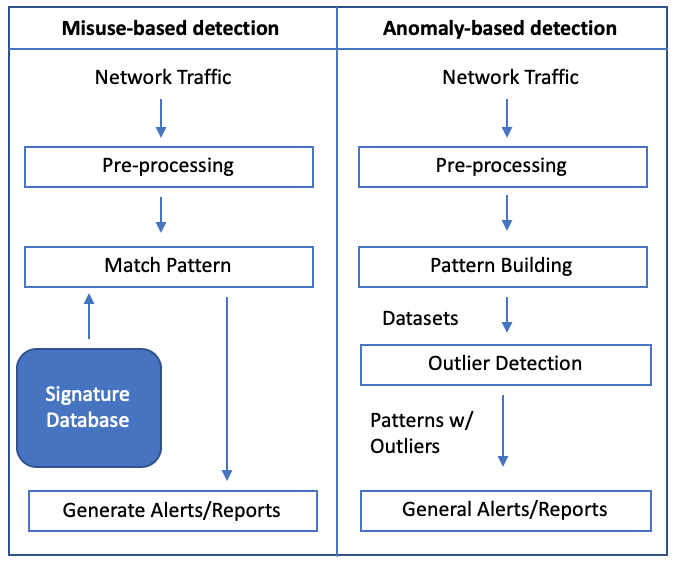
Based on the method of working:

Signature based Intrusion Detection System: This system works on the principle of matching. The data is analyzed and compared with the signature of known attacks. In case of any matching, an alert is issued. An advantage of this system is it has more accuracy and standard alarms understood by user. 

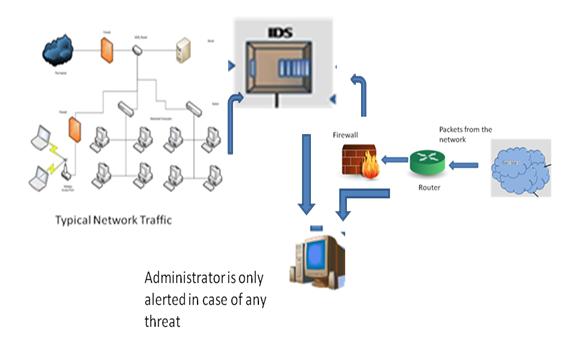
Signature based Intrusion Detection System

Anomaly based Intrusion Detection System: It consists of a statistical model of a normal network traffic which consists of the bandwidth used, the protocols defined for the traffic, the ports and devices which are part of the network. It regularly monitors the network traffic and compares it with the statistical model. In case of any anomaly or discrepancy, the administrator is alerted. An advantage of this system is they can detect new and unique attacks.

Anomaly based Intrusion Detection System



Passive Intrusion Detection System: It simply detects the kind of malware operation and issues an alert to the system or network administrator. (What we have been seeing till now!).The required action is then taken by the administrator.

[](https://www.elprocus.com/wp-content/uploads/2013/09/Passive-Intrusion-Detection-System.jpg)Passive Intrusion Detection System

Reactive Intrusion Detection System:  It not only detects the threat but also performs specific action by resetting the suspicious connection or blocks the network traffic from the suspicious source. It is also known as Intrusion Prevention System.

.

PRINCIPLES OF SUPPORT VECTOR MACHINE:-Binary classification problems can be solved using SVM [4]. An SVM maps linear algorithms into non-linear space. It uses a feature called, kernel function, for this mapping. Kernel functions like polynomial, radial basis function are used to divide the feature space by constructing a hyper plane

This process will involve a quadratic programming problem, and this will get a global optimal solution. Suppose we have N training data points {(x1, y1), (x2,y2), (x3, y3), ..., (xN , yN )}, where xi € Rd and yi €{+1,−1}. Consider a hyper-plane defined by (w, b), where w is a weight vector and b is a bias. The classification of a new object x is done with f(x) sign(w.x b) sign( α y (x x) b)

### Network Protocols

**Network Protocols** are a set of guidelines governing the exchange of information in a simple, dependable and secure way. Network protocols are formal standards and policies comprised of rules, methodology, and configurations that define communication between two or more devices over a network. To effectively send and receive information, devices on the two sides of a communication exchange must follow protocols.

Network Time Protocol:  
Network Time Protocol (NTP) is a protocol that synchronizes the clocks of computer systems over data networks. NTP was designed by David L. Mills. NTP permits network devices to synchronize their time settings with the NTP server. NTP is one of the most established internet protocols in current use.

Domain name system  
DNS resolves a Uniform Resource Locator or website address to the IP address of the site. When users type a web address into the address bar they rely on DNS servers to resolve the actual IP address of that destination. DNS translates domain names to IP addresses.

Routing Information Protocol  
It constrains the number of hops permitted in a path on a network from the source device to the destination. The maximum number of hops permitted for RIP is fifteen. It is a routing protocol used to exchange routing information. It figures the best route based on hop count. It actualizes the split horizon, route poisoning and, hold-down mechanisms.

Dynamic Host Control Protocol  
Dynamic Host Control Protocol (DHCP) uses a server to allocate an IP address and other configuration information to network devices. As a result, the device is getting a permission slip from the DHCP server to use the network. DHCP enables users to send a request to the DHCP server whenever they connect to a network. The server recognizes by providing an IP address to the user. DHCP is also known as RFC 2131.

### HOST DATA SAFE GUARDING

Hosts include clients and servers that send or receive data or services. It is essential to protect host data because an organization can lose data if cyber criminals steal it or device fails. Few methods to protect host data are given below:

Encryption:  
Encryption changes data using a complicated algorithm to make it unreadable. A special key returns the unreadable information again into readable data. Users can encrypt a whole hard drive in Windows utilizing a component called BitLocker. To use BitLocker, at least two volumes must be available on a hard disk. Only the user that encrypted the data will have the option to access the encrypted files. File encryption uses block ciphers.

Data Backups:  
Backing up data is one of the best methods for securing against data loss. In Data backup, a copy of the information from a computer is stored to removable backup media. If the computer hardware fails, the user can restore the data from the backup once the system is functional. Secure backups with passwords. The administrator at that point enters the password before restoring the data on the backup media. For additional security, keep backups to an offsite storage area.

File Access Control:  
File Access control provides the ability to grant and revoke access to valuable files. Users ought not have the option to access all files on a server if they only need access to a single file.

Types of Permissions:

**Write:**  
Users can create new files and folders and modify existing files and folders.

**Read:**  
Users can open files and folders and read them.

**Modify:**  
Users can modify and delete existing files and folders but cannot create new ones.

**Full Control:**  
Users can read file contents, create new files and folders, and modify existing files and folders.

**Read and Execute:**  
Users can read the contents of files and folders and executes the programs.

CONCLUSION: - The paper proposes the above novel multiclass SVM algorithm for implementation of Intrusion Detection System. The integration of Decision tree model and SVM model gives better results than the individual models. The final results for the proposed system are not available yet, but it seems that multiclass pattern recognition problems can be solved using the tree structured binary SVMs and the resulting intrusion detection system could be faster than other methods.