

tg

**ABstract (Moiz, SE-22)**

An Intrusion Detection System (IDS) helps systemadministrators to detect security breaches in theirorganization. However, many challenges arise while developing a flexible and effective IDS for unexpected and irregular attacks in this work, many existing systems for intrusion detection are developed in C, C++ programming languages, we design and develop intrusion detection system using Java programming language to make it more flexible and effective to secure the systems present in the networks that are directly or indirectly connected to the Internet.

**INTRODUCTION (Mubashir, SE-31)**

In today’s modern era , security’s concerns are more than ever . According to the report from CERT statistics , intrusions is increasing on a daily basis . Malicious attack due to vulnerabilities in either in the system or in the network exposed the whole network and thus violating the security policies which are basically known as CIA Triad i.e. *confidentiality, Integrity and availability*. Therefore, Intrusion detection system (IDS) are becoming an essential component in security.

An intrusion detection system is a monitor-only application designed to recognize and report on anomalies before hackers can damage your network infrastructure. IDS are either installed on your network or a client system (host-based IDS).

Typical intrusion detection systems look for known attack signatures or abnormal deviations from set norms. These anomalous patterns in the network traffic are then sent up in the stack for further investigation at the protocol and application layers of the OSI (Open Systems Interconnection) model.

An IDS is placed out of the real-time communication band (a path between the information sender and receiver) within your network infrastructure to work as a detection system. It instead leverages a SPAN or TAP port for network monitoring and analyzes a copy of inline network packets (fetched through port mirroring) to make sure the streaming traffic is not malicious or spoofed in any way. The IDS efficiently detect infected elements with the potential to impact your overall network performance, such as malformed information packets, DNS poisonings, Xmas scans, and more.[1]

The application we build is basically based on Java programming language , with the framework of java i.e. Jpcap used for implementation . Basically it functions in a way as the end-user or administrator ( which owns the system ) has to log in and show his authentication . Since user giving wrong credentials and after many times , IDS will generate an error since it detects on Anomaly behavior . It also monitors the audit logs throughout when the user is using the system . It will look for the ingoing and the outgoing packets which came from firewall either data packets are malware free or not . Since it checks in the sense by comparing the signature of packets with affected packets in the database of the application which is running on backend . Mysql will be used as a database . IDS is running in background to check and detect anomalous behavior in the system . The application is trained with data sets which are gathered from all over the world

**Datasets for Intrusion Detection Evaluation**

The Canadian institute for Cyber Security (CIC) provides a comprehensive set of network traffic datasets used by security researchers world-wide. The datasets that were encountered in the research and considered for this project are:

• The CICIDS2017 dataset consists of benign traffic generated by users mixed with malicious traffic from the most common(according to McAfee 2016) cyber attacks. The traffic was recorded in a controlled network environment over 5 days and include attacks such as Brute-forcing, DDoS and Botnets. The dataset is delivered as a set of packet capture (PCAP) files, which can be replayed on a computers network interface. The dataset also comes with a time schedule for the attacks and a spreadsheet file which contains more than 80 extracted features for each traffic flow. The total size is around 50 GB.

• The CSE-CIC-IDS2018 dataset is similar to CICIDS2017 but includes more attacks and traffic from a larger network. It is organized in different PCAP files for each host on the network and also comes with spreadsheets for ML-analyzis. The total size is over 400 GB.

• The NSL-KDD dataset is an improvement of it’s predecessor KDDCUP99. It is distributed as a set of Attribute-Relation files (ARFF) and has 42 features per record.

• ISCX-SlowDoS-2016 is a DoS dataset based on benign traffic from the ISCX-IDS dataset. It comes as a PCAP file with 24 hours of benign traffic mixed with different application layer DoS attacks. [2]

OBJECTIVES & RESEARCH QUESTIONS

**(ANEEQ, SE-47)**

|  |  |
| --- | --- |
| Objective | Question |
| * The first objective is to integrate data in a secure environment and have a distance from intrusion activity. | Why to secure data as we can also set normal password to device? |
| * Make a platform which supports high performance application system that keep Shut the doors for intrusion acts.   Using Al and machine learning we can achieve success to kill intrusion . | Why to make such big systems to keep away from intrusion activity? |
| * To guide people that how they can secure there systems in different ways? | How can we achieve maximum level security for our systems? |

STATEMENTS OF THE PROBLEMS

**(UMAIR, SE-39)**

* To identify the gap and hurdles that take place within complete network of the organization
* To have a lifelong and efficient Intrusion Detection System(IDS) is one of the major aims that has yet to be achieved by management and security related organizations , thus motivates the developers to do a considerable amount of research in order to find ways for the efficiency of operations that are witnessed in the organization.
* To manage the insecurity within the organization
* To protect data from getting misused and get accessed by unauthorized person, the organizations need security to their available resources and information. To achieve this goal, the complete digitalization of the resources and information is observed in the current scenario. An intrusion which is an unauthorized activity on a network which may be either internally or externally for specific purpose with unwanted intensions that can cause harm to the security of the network and data. Such malicious activities have to be kept under control so as to safeguard the data, through intrusion detection system in the IT management firms.

REQUIREMENT ENGINEERING

**Stake holder identification: (MUBASHIR, SE-31)**

* **A company:**

Any company can be a stakeholder of intrusion detection system. Corporate sector, banking sector, public or private firms may be stakeholders.

* **Employs:**

If the company need this system for their employs (e.g. for the safety of personal information of their employs or for the safety of network that can only be accessible by employ) then employs are also stakeholders of this system.

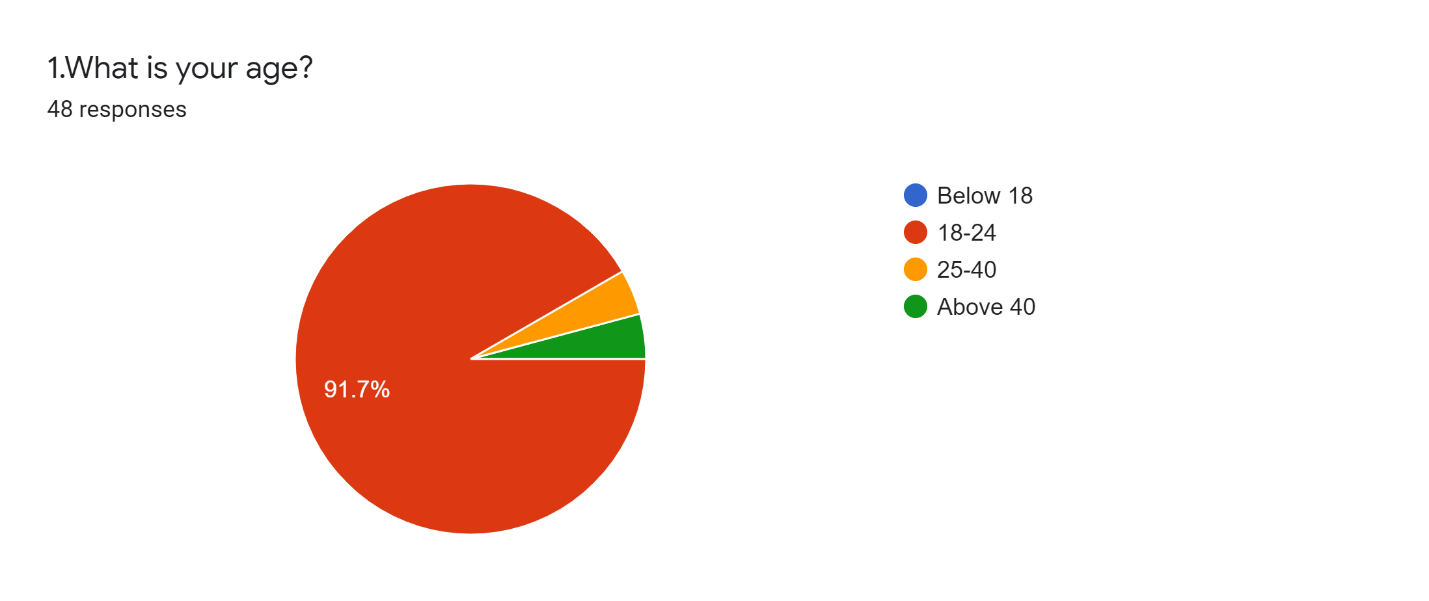
* **Clients:**

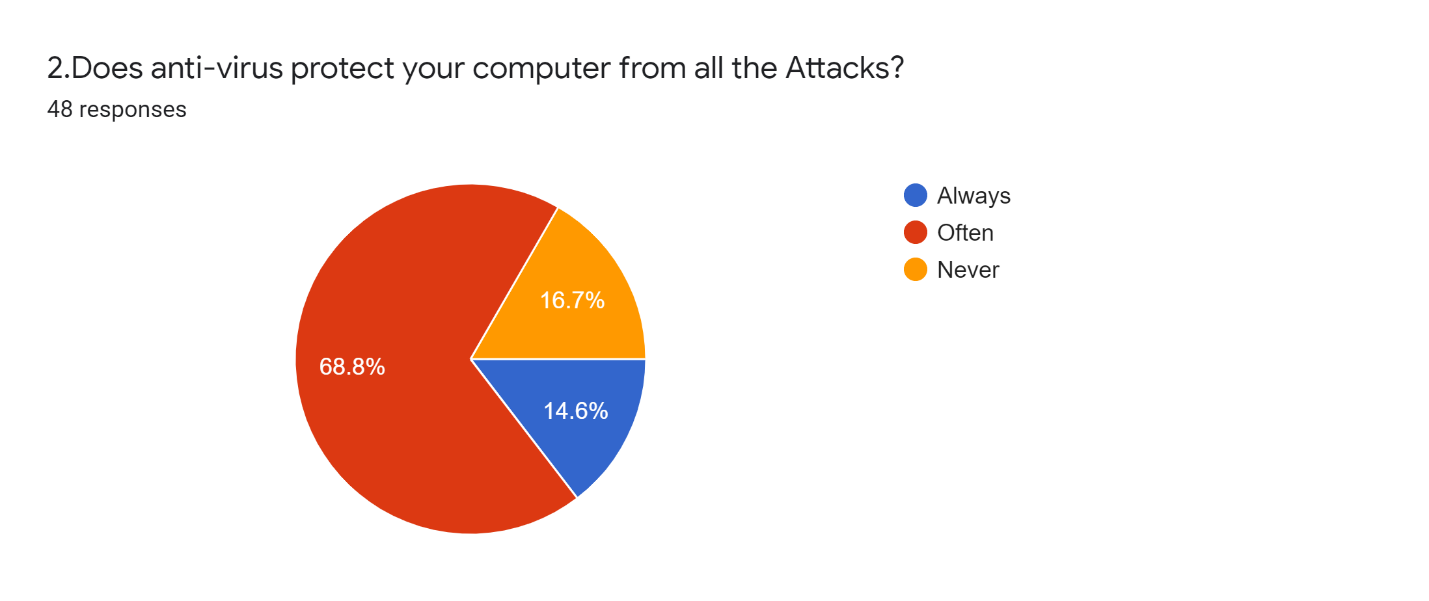
If the company need this system for its clients (e.g. an e-commerce company for the safe transactions of clients) then clients are also stakeholders.

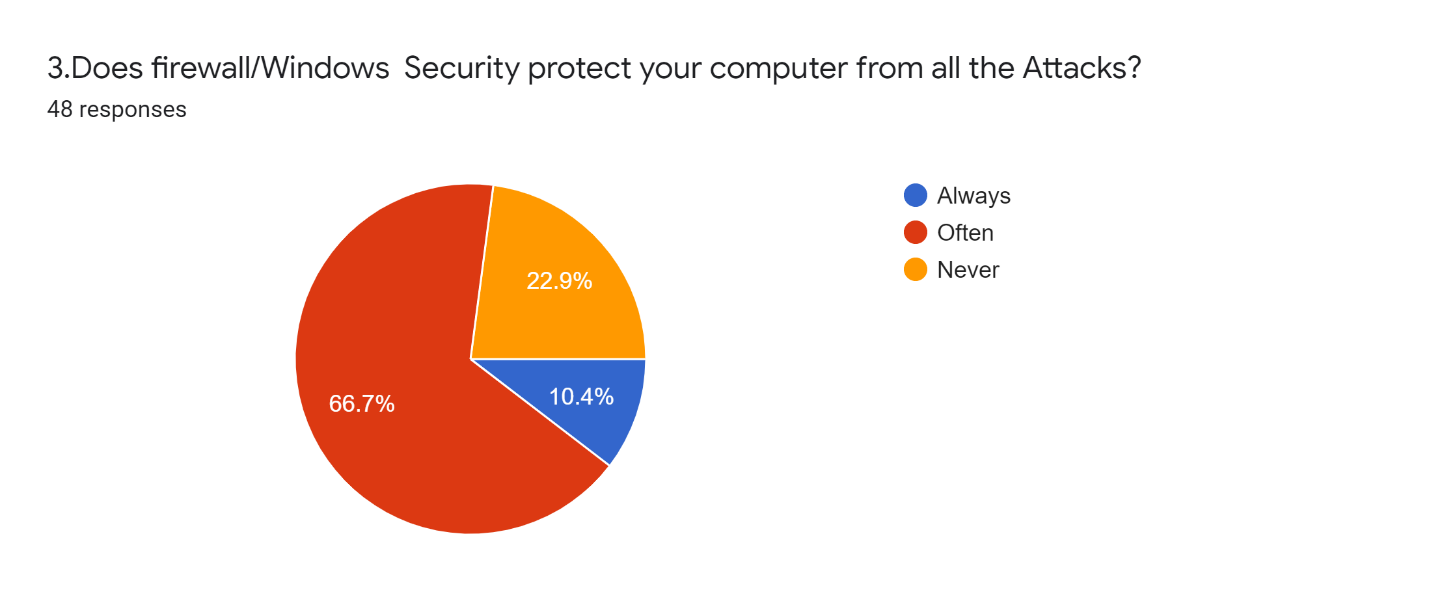
* **Developer:**

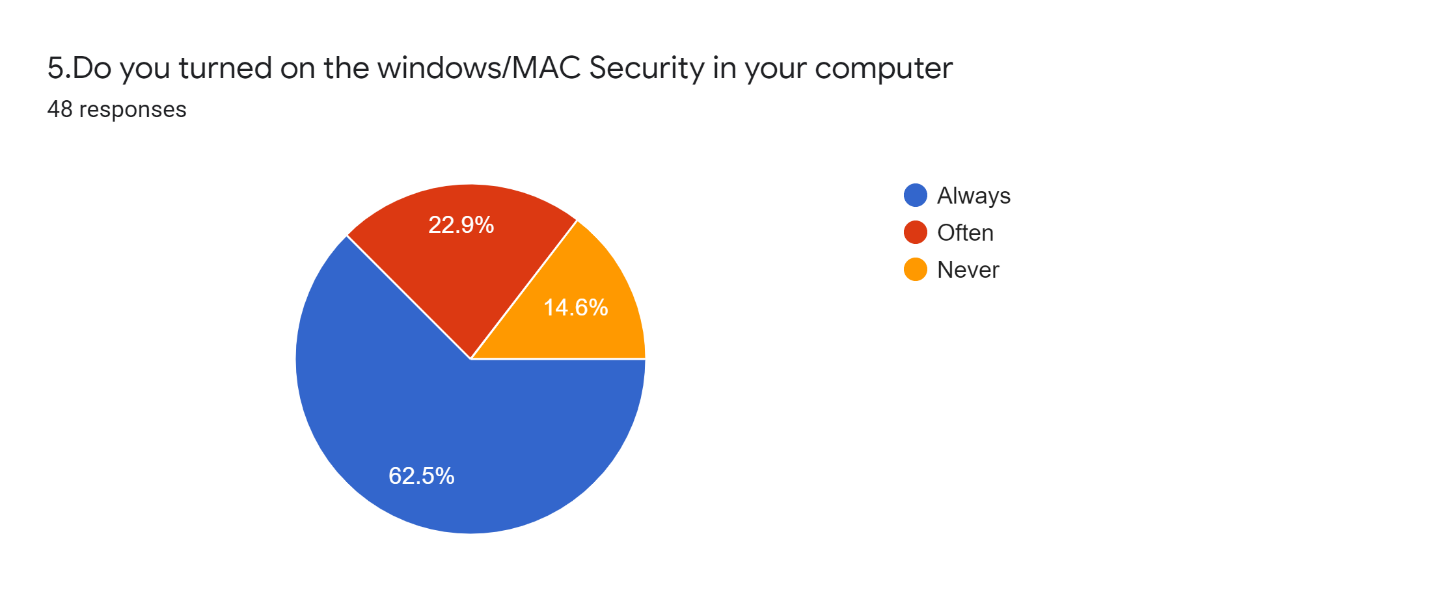
As it is obvious that Developers are the stakeholders of every project therefore in the design of this system developers are also another stakeholder.

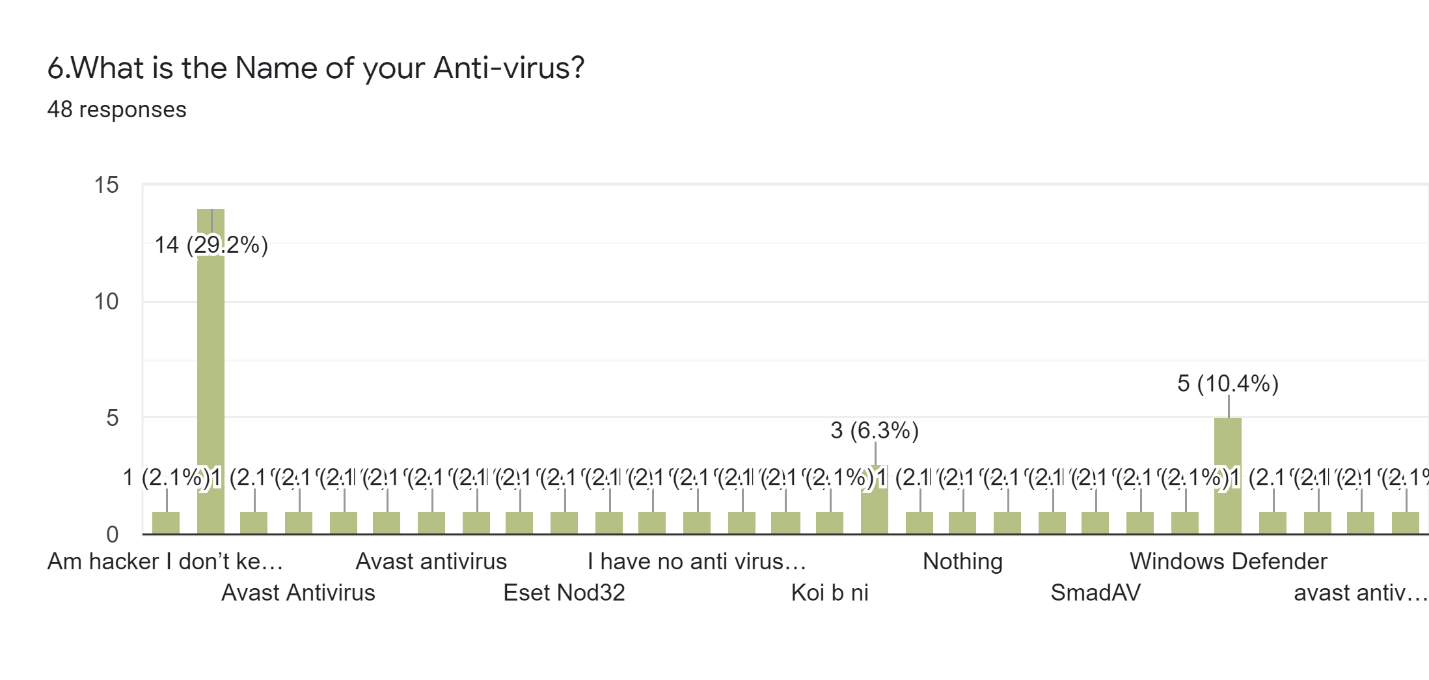
**Requirement Gathering: (KABEER, SE-28)**











**Selection of Software Development Life Cycle model**

**(moiz, SE-22)**

As we observe the necessities we came to understand following basic things.

1. All the **functional and non-functional** requirements are well-defined and understood earlier.
2. Project is large and complex.
3. System must be flexible and Maintainable.
4. It is high risk to develop the whole system at once.
5. System must be **Reliable.**

Form these requirements we are able to choose **Iterative Model** for our system.

**Preparation of SRS (Software Requirement Specification) (kABEER, SE-28)**

1. **User Requirements:**

Easy to Use, means that the system automatically Starts their working whenever it is required and It is not so much complex to use. Analyze all types of dataset come from all types of sources, so the host data became protected from all the cyber-attacks.

1. **System Requirements:**
2. **Functional Requirements.**

* **Monitoring**

The System should monitor all the Data and their Source From which the data comes from. Also scan all the data to assure either the data has thread or not.

* **Warning**

The System should give the warning to the administration whenever the System detect any type of known attack and also abnormal behaviour of the Datasets comes from other sources.

* **Data Security**

The System should protect the host data from all the warnings and threads so that if it appear as attack late on ,so the data should protected from it.

1. **Non-Functional Requirements.**

* The Presence of the Authentication Form.
* Enter the Admins Login and Password.
* Checking the Login and Password.
* System should response in Microseconds.
* Loopholes of the system must be hide.
* System should not Decrease the performance of the host machine.

**Literature Review**

SUMMARY:

* Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach(JABEZ Ja, Dr.B.MUTHUKUMAR 2015) (Mumtaz, SE-36)

In this research paper, it has been proposed the idea of making intrusion detection system more efficient . However, IDS are made to detect any intrusion that can impact the data integrity of the end users and monitor each and every data packet that came into their network , but smart intruders know ways to bypass both firewall and IDS by different means and that’s a big risk . It has been seen that different machine learning algorithms are considered to be effective to train IDS with different large datasets but this process considered as much time consuming with less successful detection where as there is a better one i.e.; Anomalous detection approach using layered technology. this idea has been presented throughout this report. By using this technique , IDS become efficient by detecting affected packets at a very less time because it had been trained not only with big data sets at distributed environments but also with KDD data sets , which are usually collected from all over the world , making IDS to execute in a less time with accuracy , thus decreasing the chances of false positives

* AN INTRUSION DETECTION SYSTEM ALERT REDUCTION AND ASSESSMENT FRAMEWORK BASED ON DATA MINING (*1-Karim Al-Saedi* *2012)* (Ahmed, SE-31)

The proposed framework contains three parts: Traffic data recovery and collection mechanism system, reduction IDS alert processes framework and risk score process of IDS alert framework. The traffic data recovery and collection mechanism frameworks creates a mechanism to spare IDS cautions, extricate the standard features as intrusion detection message exchange arrange and save them in DB record (CSV-type). It contains the Intrusion Detection Message Exchange Format (IDMEF) which works as procurement alarms and field lessening is used as information standardization to create the format of caution as standard as conceivable. As for Feature Extraction (FE) framework, it is planned to extricate the features of alarm by employing a gain data algorithm, which gives a rank for each feature to encourage the selection of the feature with the highest rank. The main work of reduction IDS caution processes system is to diminish the amount of false alerts based on a modern aggregation algo.

* The Architecture of a Network Level Intrusion System (Richard Heady, George Luger, Mark Servilla, Arthur Maccabe) August 15 1990 (Ahmed, SE-43)

The research paper has discussed about the protection of computer resources, specifically network resources. The key objective is to use network intrusion systems for detection of malware such as worms and to secure the network resources. For designing such a system first, the overview of a basic architecture is given which is moved to a more complex understanding covering various aspects like Data Sampling and Preprocessing, Network Patterns and Flagging Deviations in these aspects several minor issues have been addressed. The main aim of the research has been to provide a secure network for the shift from offline to online systems at that time.

* Intrusion Detection using Naive Bayes Classifier with Feature Reduction ( S. Mukherjee, N. Sharma 2012 ) (Ahmed, SE-28)

Intrusion Detection System (IDS) is use to used to monitor and analyze the events occur in any machine in order to detect signs of known attacks and anonymous Behavior. The IDS is computationally effective and efficient as it uses three standard feature selection methods that are Correlation-based Feature Selection, Gain Ratio and Information Gain. We propose the new feature selection method **Feature Vitality Based Reduction Method (FVBRM)** by using the Naive Bayes Classifier for Intrusion detection on reduced data sets. We perform the Experiments on NSL-KDD labeled Datasets then by using three standard method and our proposed method, we found that the Feature reduction performed on 41 features and in this 41, 10 using CFS, 14 using GR, 20 using IG and 24 using FVBRM. In this way we found this (FVBRM) faster and more efficient.

* *A Deep Learning Approach for Network Intrusion Detection**System* ***(****Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam****) (MOIZ, SE-22)***

A deep learning based approach shows robust potential to be used for anomaly detection in network intrusion detection system (NIDS). An NIDS is important tool that monitors, analyzes, and raises alarms for the network traffic entering into or exiting from the network devices of an organization.to make it more flexible and effective self-taught learning, a deep learning techniquebased on sparse auto-encoder and soft-max regression, is implemented. Researcher used thebenchmark network intrusion dataset - NSL-KDD to evaluate anomaly detection accuracy. They observed that the NIDSperformed very well as compared to previously implementedNIDSs for detection when evaluatedon the test data. The performance can be further enhancedby applying techniques like Stacked Auto-Encoder, anextension of sparse auto-encoder in deep belief nets.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Author** | **Problem** | **Tools** | **Result** | **Future Research** |
| Jabez, J.Muthukumar, B. -2015 | To analyze and monitor each data packet minutely so that no malware can be transferred , although IDS is capable of doing that but signature detection of IDS is not found much efficient | Outlier Detection Approach ( using Neighborhood Outlier Factor (NOF) ) | As a result of using Layered technology for anomalous behaviour , it has been found out from no. of experiments that it success rate is much greater than other machine learning algorithms because it takes less CPU resources and detect affected data packets at a faster than any other |  |
| 1-Karim Al-Saedi 2- Selvakumar Manickam 3-Sureswaran Ramadass 4-Wafaa Al-Salihy 5-Ammar ALmomani | The IDS creates tremendous amount of cautions that are mostly false positives. The abundance of untrue positive alerts makes it troublesome for the security examiner to identify effective assaults and to require remedial actions. | Data Mining | This system anticipate to decrease the false positive cautions and to reduce the alert repetition. |  |
| Richard Heady, George Luger, Mark Servilla, Arthur Maccabe  August 15 1990 | To design a Network Intrusion Detection System’s Architecture that can detect and respond to worm programs as well as other types of Anomalies. | Network Interface Tap (NIT) provided by SUN Microsystems | Easier access to the Ethernet service. Reading from and writing to the ethernet device made easier. This helps in monitoring activity patterns and respond to them. This will be essential for a sound Network-based Intrusion Detection System Architecture. | When NIT is initialized as a reading device it makes copies of packets entering the ethernet device and returns them as stream modules and when initialized as a writing device NIT requires the user to supply an input stream which is then transmitted out to the network through the ethernet device. This gives the user power to monitor data packets effectively. The NIT records only the Transport information packets as they are considered unbiased data. The user information packets which are called biased data are removed by NIT buffering module. By this way NIT weeds out the potential threats making the network secure. |
| S. Mukherjee, N. Sharma  2012 | To monitor and analyze the events in order to detect signs of security problems, the three standard feature selection methods use but they are not found too efficient. | Feature- Vitality Based Reduction Method (FVBRM) | As a result, by using Naive Bayes Classifier technology the IDS is become more efficient. From No. of Experiments we found that the Feature reduction performed on 41 features and in this 41, 10 using CFS, 14 using GR, 20 using IG and 24 using FVBRM on NSL-KDD dataset. This made this faster and more efficient. | Future work will include customize of FVBRM feature selection method to improve the results for intrusion particularly for U2R attacks with reduced complexity and overheads. |
| Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam (2016-05-24) | Build  network intrusion detection system To scan, analyzes the unusual activity occurring in network. | Network intrusion detection system with Deep Learning Approach | By using deep learning approach in network intrusion detection system the performance of NIDS enhanced as compared to previous one.as experiments show that deep learning approach achieved 98% more accuracy rate than all types of  classification. | To implement deep learning approach on real time network using real time NIDS. |
|  |  |  |  |  |
|  |  |  |  |  |

**Software Design/Architecture**

**Platform independent system design according to requirements**

(RAAMIZ, SE-43)

***Flow Diagram:***

Provide

***Flowchart:***

***Alarm information***

Network

Network packet capture

Decoding captured packets

Pattern matching in each captured packet

Different intrusion detection method

Output

Diagram for the procedure flow in making and utilizing platform /technology

***Packet information***

***Use Case Diagram:***

System

System Administrator

Loop until 3 unfruitful results

**RISK MANAGEMENT**

(Mumtaz, SE-36)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Probability** (P) 1 = low  5 = high | **Severity (S)** 1 = low  5 = high | **Risk Score**  (P x S) | **Mitigation** |
| Zero – day Vulnerability | 3 | 4 | 12 | User should keep updating the application as a security measure |
| False Positives | 3 | 3 | 9 | There should be rules and policy made for the application to highlighting false alarm issue |
| Data Integrity of end user | 2 | 5 | 10 | Data should be made backup at all the time to ensure integrity of data |
| Encrypted Packets | 2 | 5 | 10 | Firewalls should me made stronger ensuring the stoppage of encrypted and affected packets |

**Project Management**

**Platform/technology selection** (Aneeq,SE-47)

The network intrusion detection we developed is tested on x86 architecture machines. The programming language chosen is Java. This is motivated by little literature in the field of network intrusion detection development in such a language. Among them WinPcap, JpCap, JavaMail, MySQL. The following subsections give an overview on each of them.

1. **WinPcap: [4]**

Packet Capture is a programming interface that allows to capture the traffic over networks. Supervision tools can use pcap (or WinPcap) to capture packets over the network; and to record captured packets in a file and to read saved file.

1. **JpCap:**

Jpcap is an open source library for capturing and sending network packets from Java applications .

1. **JavaMail:**

The JavaMail API provides classes that model a mail system. JavaMail classes and interfaces are set within four packages namely javax.mail, java.mail.internet, javax.mail.event, and javax.mail.search. **[5]**

**Description of the Implemented Database :**

The MySQL is used as the relational database management system. The implemented database has four database’s tables: Table TCPCAPTURES is used to record information about captured TCP packets. Table UDPCAPTURES is used to record information about captured UDP packets. Table ICMPCAPTURES is used to record information about captured ICMP packets. Finally, the table DONNEESALERTES is used to record information about different detected intrusions.

**Implementation Description**

The proposed network intrusion detection system is implemented according to the following five steps, namely listening to the network and capturing the packets, decoding the packets, detecting specific attacks, detecting process heuristically, and printing the output module

1) Listening to the network and capturing the packets:

Atthis first step, a sniffor is developed using Jpcap library already presented in subsection V-F2. In a Ethernet network, each system has a network card which has its own physical address. The network card examines each packet over the network and catches it once intended to the host machine. One withdraws from this package the various layers such as Ethernet, IP, TCP, etc. to forward information it contains to the application. When a network card is configured in the promiscious mode thanks to the Jpcap library, all packets are captured without being out from the traffic. [6]

2) Decoding the packets:

Packet decoding process also is based on the Jpcap library. The decoder receives one after another all the packets from the sniffer and finds their category (TCP, UDP, ICMP, etc.) by comparing them to different available classes in the Jpcap library namely IPPacket, TCPPacket, UDPPAcket, ICMPPacket, etc. For instance, if the concerned packet is TCP, the decoder collects its source and destination addresses, source and destination ports, data field and TCP flag.

3) Detecting specific attacks:

In the proposed architecture, intrusion detection is done at levels 3 and 4. At level 3, a first search of intrusion is done based on the patterns while at level 4 three modules namely deny of service, Bruteforce, Trojan based upon heuristic analysis are done.

4) Heuristic detection process:

Patterns are stored in a database and scanned for intrusion detection.

5) Output module:

This module is executed once an attack is detected. It has three distinct modes. The first one is an alarm that informs about intrusion detection. The second mode uses one table in the database for recording attacks through a graphical user interface. The third mode is an alarm through an electronic mail sent to the system administrator. This last mode uses the Javamail library.

**2) Cost estimation** (Aneeq,SE-47)

We will find out the cost of our intrusion detection system with the help of Cocomo Model.According to Cocomo model cost of software depends upon line of code(LOC),therefore according to our implementation description and our team efforts the cost would be as follows:

Estimation=a1x (K LOC)^a2 \*PM(Person per month)

Here a1 is the coefficient and calculated value for it is 2.4 and a2 appears to be 1.05.

Estimation= (2.4) x (80000) ^1.05x7

Estimation=Rs 2.36 Million would be our final cost of product which will work efficiently.

**3) Human resource management**

**4)**  **Time scheduling**

**Significance of Project**

(Mumtaz, SE-36)

This project proposed some significance as it helps to overcome security issues which we we normally face during surfing the internet or using our system

* Our Java based IDS is strong enough to detect attacks in a way like it comprises of complete database and datasets of attacks which are updated time to time
* As one of the issue in IDS is to produce false alarm ,we tried to minimize this error. Our project aims to have Higher Detection precision and stronger detection stability
* We aimed to make encrypted communications between components of the IDS
* The application is smart enough to work with majority systems with high efficiency providing accuracy in detecting the intruder fast and securing the system
* An easy to use graphical user interface is provided for the end user making it easy to use different tools

**Recommendations**

(Raamiz, SE-43)

Intrusion Detection System (IDS) is an automatic system that monitors the network traffic. They detect patterns of malicious activity and generate “alerts”. IDS alerts can also activate secondary tasks like recording activity and tracing the IP address of the spyware device. So, IDS protect our sensitive information from malicious users.

IDS do strengthen the security of our network connection but just like anything else it is not perfect and has some issues that need to be highlighted and how we can overcome these issues. There are three main issues relating to management, technical and website.

The management issue is that how will the IDS system respond to the alerts. The response to an intrusion involves legal, public affairs, networking, and systems administration personnel, as well as lost productivity and system downtime. The organization making the IDS product should be supportive of these responses for a successful product. Technical issue is concerned with the installation of IDS and dealing with the additional network that can be generated by the IDS. For managing this problem, technical knowledge of the organization workers must be strong. They must be able to identify the storage and communication resources which need to be protected and able to handle the data integrity. The Website issues relate with additional vulnerability of the website as web servers have a higher risk of being manipulated so this problem can be solved by using multiple IDS of different types. All the three issues can be overcome easily if the organization is customer supportive, has strong technical workforce and skillful in configuration management.

So, the IDS is an essential security product for the user. It is up to the user entirely to have a host-based or network-based IDS depending on users’ requirements. Host-based IDS requires more security as access to the operating system is mandatory for it while network-based IDS is more secure.

CONCLUSION

(Kabeer, SE-28)

Intrusion Detection System (IDS) Analyze and monitor all events occur in the system in order to protect it from anonymous attacks and malwares. Now a days, the Intrusion detection systems are built by using programming languages like visual basic and C++, but we build IDS by using libraries of Java (Jpcap and JavaMail) with MySQL (database management system) to protects the Datasets like CICIDS2017, CSE-CIC-IDS2018, NSL-KDD, ISCX-SlowDoS-2016.

By Using this IDS, the Warnings are highly accurate and faster of the abnormal behavior of the unauthorized user and intrusions. The False alarming is minimize so the user can access the zip file will contain a folder (includes the Crack files and Patch files) called new/board\_files[7] and the user can also use some Cheep software.

This IDS works on five steps on which the whole process act, are listening to the network and capturing the packets, decoding the packets, detecting specific attacks, detecting process heuristically, and printing the output module. The IDS Itself is secure by using encryption and decryption techniques in the inter-communication so that the loopholes of our IDS is also protected from the Cyber-attacks. By using some more m we will update this IDS for wireless sensor networks and show how it can be configured to detect Sinkhole attacks. A Sinkhole attack forms a serious threat to sensor networks.[8]

**REFERENCES**

[1] <https://www.tek-tools.com/>

[2] Machine Learning for a Network-based Intrusion Detection System By Vilhelm Gustavsson (May 2019)

[3] [4] [5] [6] Ezin, Eugène & Djihountry, Hervé. (2011). Java-Based Intrusion Detection System in a Wired Network. International Journal of Computer Science and Information Security. 9. 33-40.

[7] <http://www.heavent.it/rxes1g52a/copy-crack-file-to-installation-directory.html>

[8] Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks By Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, Marios Mpasoukos. (2007)