NETWORK INTRUSION DETECTION SYSTEM

N.Teja sai [1], B.Ganesh[2], DR. K. KRANTHI KUMAR[3], Dr.V.Saravana Kumar[4]

B.TECH Scholars, Dept.ofInformation Technology and Engineering
Hyderabad-501301, India

ABSTRACT

The increasing in the using of technology was head to the raise in the usage of count of data that is being worked over the Internet gradually when time changes. With the huge amount of usage of data that is going through the Internet, will come with the situation of giving security to the particular amount of data, and here the Intrusion Detection System (IDS) comes into the scenario and helps in detecting any virtual security threats. Intrusion Detection System (IDS) is a process that monitors and analyses data to detect any intrusion in the system or network. Intruders find different ways to penetrate into a network. The particular process (IDS) which we are using is came into picture using trending technologies like Machine Learning Algorithms to classify them and to know about attacks which was happend and to detect them where and how an attack occurs and also used to find which type of machine learning algorithm is best working for identify the type of attack occurred.

INTRODUCTION

An Interruption Location Framework (IDS) may be a significant program application that plays a critical part in keeping up the security of computer systems or frameworks. The essential work of an IDS is to screen arrange activity and framework exercises, analyse the information collected, and recognize any suspicious or unauthorized behaviour that might posture a risk to the system's security. Once an IDS recognizes any interruption action or infringement, it produces cautions that are either sent to an administrator or collected at a central area employing a Security Data and Occasion Administration (SIEM) framework.

A SIEM system is a powerful tool that combines information from various sources, such as firewalls, antivirus software, and IDS, to create a comprehensive view of the system's security status. This allows security teams to identify and respond to potential security threats quickly. One of the most significant advantages can focus their efforts on real security issues, and avoid wasting time and resources on false alarms.

In summary, IDS and SIEM systems are critical components of any organization's security infrastructure. They provide real-time monitoring and detection of security threats, enabling security teams to respond quickly and effectively to protect their networks and systems from potential cyber-attacks.

The level of network around the world has given openings for cybercriminals who make a living breaking into systems, as well as novice programmers who have as well much time on their hands. The decided programmer can discover a way into you organize either by building up a few sort of association and entering your virtual "front entryway" or by utilizing social building strategies to get client ID and watchword data. Anything the strategy utilized, the truth is that a gate crasher can get into you organize and hurt your trade.

The intrusion detection system (IDS) plays an important role in extracting and analysing the network traffics to detect aberrant activity.

1. LITERATURE SURVEY

The current work on security systems has improved a lot in gathering evidence for users using data mining and investigation methods. These systems have a problem- they can't recognize certain types of attacks. For example, when attackers use more than one session to attack or when they do a DDoS attack.

Many ways of detecting harmful attacks on computer networks and learning about the features of these attacks using the information stored in log files. But it is difficult to detect attacks as they happen quickly. There is a big problem when it takes a long time to realize there has been an attack, and this can cause a lot of harm to the computer and its information.

The current methods can't tell if someone is using a remote computer to log in or stop certain types of unauthorized attempts to log in with valid user information. This means that some attacks can happen without people knowing, which can cause big problems and make the whole computer system less safe.

In summary, while existing security systems have made significant progress in collecting forensic features and detecting malicious attacks, there is still a need for improved techniques that can detect multistage attacks, DDoS attacks, and real-time attacks at incoming rates. Additionally, detecting and preventing specific types of intrusions, such as invalid login attempts, is crucial for ensuring network security and data

2. PROPOSED MODEL

Keeping the computer network safe from hackers and other bad people is super important for companies. A smart tool called an intrusion detection system (IDS) is a really good way to do it. But the current security system may not find all new types of attacks. To solve this problem, computers are taught to recognize when someone is trying to break into a system using a process called machine learning.

We use three different methods, called Support Vector Machines, K-Nearest Neighbour, and Multi-Layer Perceptron, to help us tell apart different patterns and recognize intrusions. These ways have worked well in finding when someone is trying to break into security, and can change to keep up with different network settings.

Furthermore, our proposed system also includes a user interface that allows the user to upload the status information of the network. Through the use of ML models, the system can detect the status of the network as normal or abnormal and identify the type of intrusion if the status is abnormal. This user interface provides an easy-to-use, intuitive platform for users to monitor the security of their networks and take appropriate action if necessary.

In summary, the proposed IDS that utilizes ML methods such as SVM, KNN, and MLP, combined with a user-friendly interface, provides a comprehensive and effective solution for network security and intrusion detection.

3. SYSTEM ANALYSIS

This project needs something called a Graphical User Interface (GUI) so people can use the intrusion detection system more easily. The GUI makes it easy for you to add a file with information about the network. You only need to add one instance of this information. The computer screen should show a list that lets you choose which way the computer will learn.

The GUI must be designed in a way that is easy to use and understand for the user. It must have a simple and intuitive layout that allows the user to navigate through the various options and features. The user should be able to upload a file with a few clicks and select the machine learning model to be used.

The GUI must to show the comes about of the interruption discovery framework in a clear and brief way. It ought to demonstrate whether an interruption has been recognized or not and give extra points of interest on the sort of interruption recognized in case pertinent. This data ought to be displayed in a way that's simple to get it and decipher by the client.

Overall, the GUI is a critical component of the intrusion detection system. It provides a user-friendly interface that enables the user to interact with the system, upload network status information, select machine learning models, and view the results of the intrusion detection system. The GUI must be well-designed and intuitive to ensure that the user can easily use and interpret the information presented.

Window

It was quite easy to change the window. It can be opened or closed by clicking of a one icon. It can be move to any area by dragging them back in a multitasking environment, the more than one windows can be open at the same time, all windows would perform different tasks.

Menu

Menus are a fundamental component of graphical user interfaces (GUIs) that allow users to execute commands by selecting them from a list of options. Menus present the available options in a hierarchical format that can be navigated with a mouse or keyboard. Menus are essential in GUIs because they provide an intuitive and straightforward way to access and use software commands. Using menus, users can easily select and execute the desired command without having to memorize complex commands or search through lengthy documentation. The graphical nature of menus also simplifies the learning process for new users, making the software more accessible and user-friendly.

Input widgets

Input widgets are an essential component of any application that requires user input. These widgets allow users to input data into the application using various forms such as check boxes, radio buttons, select boxes, and file uploaders. Two important input widgets commonly used in applications are the file uploader widget and the select box widget.

The file uploader widget enables users to upload files from their devices to the application. This widget is essential for applications that require users to upload files such as images, documents, or videos. Users can simply click on the file uploader widget and select the file they wish to upload. Once selected, the file is uploaded to the application, and the user can proceed with their task.

3.2 PERFORMANCE REQUIREMENTS

Execution can be calculated in terms of the result given by the application. For the examination of the framework to know almost its usefulness prerequisites detail gives exact result. As it were when the necessities details would be given legitimately, it is conceivable to plan a framework, agreeing to the specified environment. It rests generally with the clients of the existing framework to provide the prerequisites determinations since these are individuals who uses the framework at long last. This is often since to know prerequisites at beginning arrange so that the framework can be outlined, concurring to those prerequisites. It is getting to be exceptionally difficult to alter the framework once it is done with plan and on the other side planning a framework, which does not full fill there's no utilize in prerequisites in client. The requirement specification for any process can be gradually stated is given below:

The prerequisite detail for any handle can be continuously expressed is given underneath:

The existing framework is totally subordinate on the clients to perform all the operations. The existing system is completely dependent on the users to perform all the operations.

Additionally, the new system should be user-friendly and easy to use. It should have a simple and intuitive user interface that allows users to easily upload the network status information and select the machine learning model to be used. The system should also have a fast process speed to enable real-time detection of intrusions and minimize the amount of damage caused to the network. It should also be able to handle a large amount of data without crashing or slowing down. Overall, the requirement specifications should be well-defined and comprehensive to ensure the success of the project.

3.3 SOFTWARE REQUIREMENTS

PYTHON

Python may be a sort of dialect which back uh oh concepts and it is a translated programming dialect additionally it contains energetic semantics. It contains high-level built-in information. Python is basic dialect and simple to memorize language structure reasonable and numerous individuals shoe intrigued to memorize python.

WEB BROWSER(CHROME)

Chrome may be a sort of browser which was discharged beneath governance of google on December 11, 2008. highlights incorporate the adjust of information with Google administrations and account visit browsing, and programmed interpretation and spell check of web pages. It moreover highlights an coordinates address bar/search bar, called the omnibox Chrome works exceptionally well with Google websites such as YouTube and Gmail. It too utilized to oversee its framework assets in an unexpected way compared to other browsers.

STREAM LIT

Stream lit is a tool that helps people make web apps and work with data quickly using Python. It's free to use and anyone can use it! The framework is often used together with well-known tools in Python like NumPy, Pandas, and Matplotlib. Stream lit makes it easier for developers to create interactive apps and visualize data. This is a strong tool that helps make web pages and analyse information using the programming language called Python**.**

WINDOWS 7

In addition to its visual appeal, Windows 7 also provides several key features that enhance the user experience. One of its most notable features is its enhanced taskbar, which provides users with a more intuitive way to manage their open windows and applications. The taskbar now includes larger icons that provide thumbnail previews of open windows when the user hovers over them. This allows users to quickly switch between windows and applications without having to hunt for them on their desktop. Additionally, Windows 7 also introduced Aero Peek, which lets users quickly preview the contents of a window by hovering their mouse over its thumbnail on the taskbar**.**

Another feature of Windows 7 that sets it apart from its predecessors is its improved file management system. The new Libraries feature allows users to easily organize and access their files, regardless of where they are stored on their computer. With Libraries, users can quickly access their documents, pictures, music, and videos from a single location. Windows 7 also introduced a revamped search feature, which allows users to easily search for files and applications on their computer. The search results are now displayed in a more intuitive way, making it easier for users to find what they're looking for.

Windows 7 also includes several performance and security enhancements that make it a reliable and secure operating system. It features a more efficient use of system resources, improved power management features, and better support for multi-core processors. It also includes several security enhancements, such as improvements to the User Account Control (UAC) feature, which helps prevent unauthorized changes to the system. Overall, Windows 7 is a robust and user-friendly operating system that offers many features and enhancements that improve the overall computing experience.

Windows 7 also includes several performance and security enhancements that make it a reliable and secure operating system. It features a more efficient use of system resources, improved power management features, and better support for multi-core processors. It also includes several security enhancements, such as improvements to the User Account Control (UAC) feature, which helps prevent unauthorized changes to the system. Overall, Windows 7 is a robust and user-friendly operating system that offers many features and enhancements that improve the overall computing

WINDOWS XP

Windows XP could be a broadly utilized working framework that has been well known among clients for numerous a long time. One of the key highlights of this working framework is its capacity to run a assortment of diverse applications and program, making it a flexible and versatile stage for many distinctive sorts of clients. Whether you're a understudy, proficient, or domestic client, you'll utilize Windows XP to oversee your reports, information, and media records with ease.

Overall, Windows XP is a reliable and powerful operating system that has been used by millions of people around the world. Its versatility, ease of use, and adaptability make it a great choice for anyone who wants to manage their data and applications with confidence and efficiency.

4. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

A system architecture is a blueprint that illustrates how all the components of a system fit and operate together. It is a formalized description that explains and illustrates the specific structure of a building or infrastructure. The system architecture helps to comprehend the interconnectedness and functions of different elements that make up the system.

The architecture consists of various parts that work in collaboration to form the system. It involves integrating multiple systems to form a larger system. The language used to describe the system architecture is essential in comprehending its overall structure and design.

Architecture description languages (ADLs) are used to formally represent and communicate system architectures. ADLs provide a standard notation for describing the components, interfaces, and interactions of a system, making it easier for different stakeholders to understand and communicate about the architecture. ADLs can also be used to support automated.

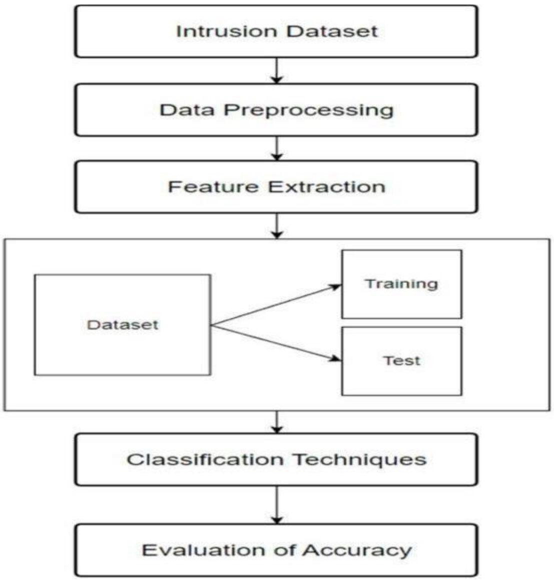


Fig 4.1 System Architecture

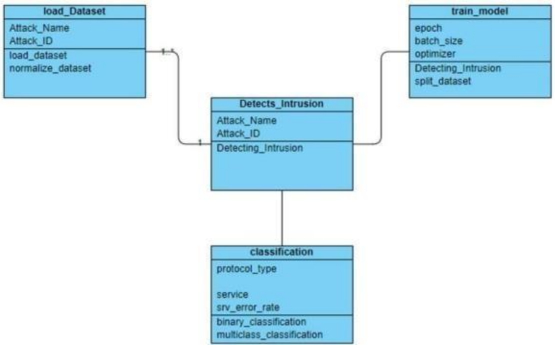
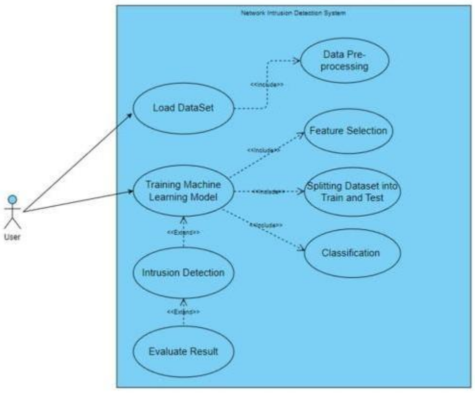
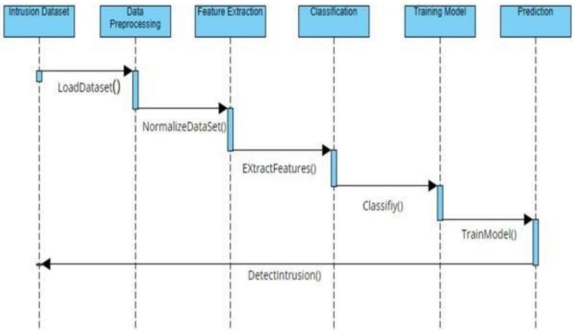


Fig 4.2.1 Class Diagram

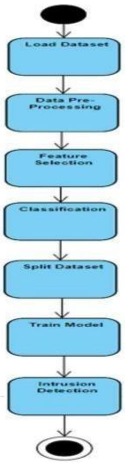
4.2.2 Use Case Diagram



4.2.3 Sequence Diagram



4.2.4 Activity Diagram



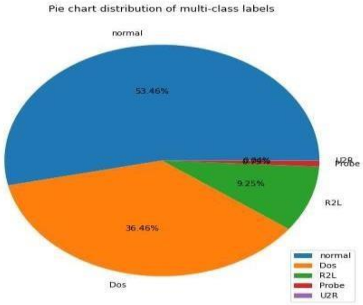
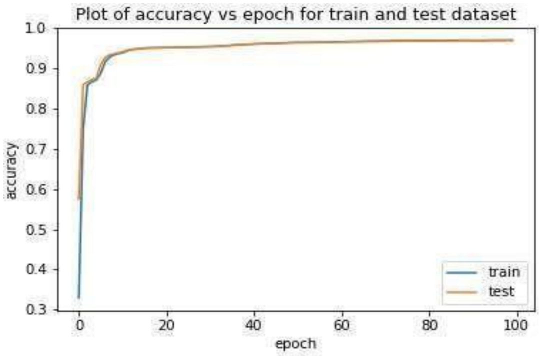
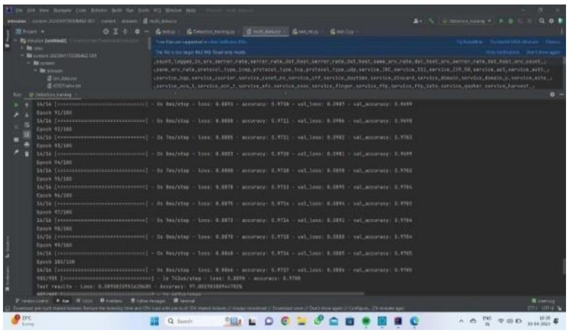


Fig 4.3 Class Labels

5. RESULTS:

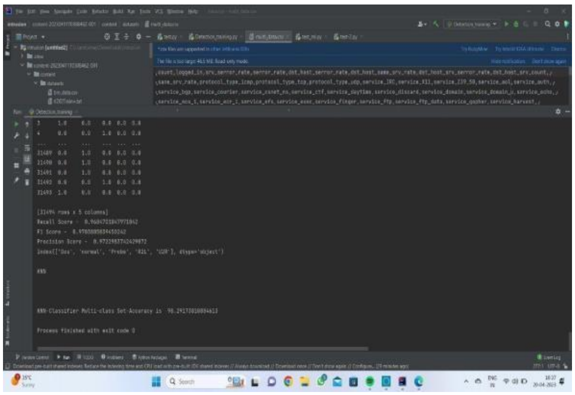




```
,count,logged_in,srv_serror_rate,serror_rate,dst_host_serror_rate,dst_host_same_srv_rate,dst_host_srv_serror_rate,dst_host_srv_count,
,same_srv_rate,protocol_type_icmp,protocol_type_tcp,protocol_type_udp,service_IRC,service_X11,service_Z39_50,service_aol,service_auth,
,service_bgp,service_courier,service_csnet_ns,service_ctf,service_daytime,service_discard,service_domain,service_domain_u,service_echo,
,service_eco_i,service_ecr_i,service_efs,service_exec,service_finger,service_ftp,service_ftp_data,service_gopher,service_harvest,
```

```
16/16 [==============================] - 0s 8ms/step - loss: 0.0893 - accuracy: 0.9730 - val_loss: 0.0907 - val_accuracy: 0.9699
Epoch 91/100
16/16 [==============================] - 0s 8ms/step - loss: 0.0888 - accuracy: 0.9711 - val_loss: 0.0906 - val_accuracy: 0.9698
Epoch 92/100
16/16 [==============================] - 0s 7ms/step - loss: 0.0885 - accuracy: 0.9731 - val_loss: 0.0902 - val_accuracy: 0.9703
Epoch 93/100
16/16 [==============================] - 0s 8ms/step - loss: 0.0883 - accuracy: 0.9730 - val_loss: 0.0901 - val_accuracy: 0.9699
Epoch 94/100
16/16 [==============================] - 0s 7ms/step - loss: 0.0880 - accuracy: 0.9730 - val_loss: 0.0898 - val_accuracy: 0.9702
Epoch 95/100
16/16 [==============================] - 0s 8ms/step - loss: 0.0878 - accuracy: 0.9733 - val_loss: 0.0895 - val_accuracy: 0.9706
Epoch 96/100
16/16 [==============================] - 0s 8ms/step - loss: 0.0875 - accuracy: 0.9734 - val_loss: 0.0894 - val_accuracy: 0.9703
Epoch 97/100
16/16 [==============================] - 0s 9ms/step - loss: 0.0873 - accuracy: 0.9734 - val_loss: 0.0891 - val_accuracy: 0.9704
Epoch 98/100
16/16 [==============================] - 0s 8ms/step - loss: 0.0870 - accuracy: 0.9738 - val_loss: 0.0888 - val_accuracy: 0.9704
Epoch 99/100
16/16 [==============================] - 0s 9ms/step - loss: 0.0868 - accuracy: 0.9736 - val_loss: 0.0885 - val_accuracy: 0.9705
Epoch 100/100
16/16 [==============================] - 0s 8ms/step - loss: 0.0866 - accuracy: 0.9737 - val_loss: 0.0886 - val_accuracy: 0.9705
985/985 [==============================] - 1s 763us/step - loss: 0.0890 - accuracy: 0.9700
Test results - Loss: 0.08910... - Accuracy: 97.0019...%
```

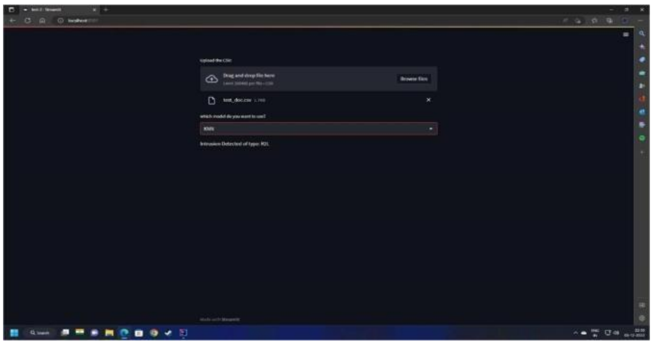
Fig 5.1 KNN Accuracy



```
,count,logged_in,srv_serror_rate,serror_rate,dst_host_serror_rate,dst_host_same_srv_rate,dst_host_srv_serror_rate,dst_host_srv_count,
,same_srv_rate,protocol_type_icmp,protocol_type_tcp,protocol_type_udp,service_IRC,service_X11,service_Z39_50,service_aol,service_auth,
,service_bgp,service_courier,service_csnet_ns,service_ctf,service_daytime,service_discard,service_domain,service_domain_u,service_echo,
,service_eco_i,service_ecr_i,service_efs,service_exec,service_finger,service_ftp,service_ftp_data,service_gopher,service_harvest,
```

```
3      1.0    0.0    0.0  0.0  0.0
4      0.0    0.0    1.0  0.0  0.0
...    ...    ...    ...  ...  ...
31489  0.0    1.0    0.0  0.0  0.0
31490  0.0    1.0    0.0  0.0  0.0
31491  0.0    1.0    0.0  0.0  0.0
31492  0.0    0.0    1.0  0.0  0.0
31493  1.0    0.0    0.0  0.0  0.0

[31494 rows x 5 columns]
Recall Score -  0.9684721047971842
F1 Score -  0.9703885834650242
Precision Score -  0.9722983742429872
Index(['Dos', 'normal', 'Probe', 'R2L', 'U2R'], dtype='object')

KNN



KNN-Classifier Multi-class Set-Accuracy is  98.29173818884613

Process finished with exit code 0
```

Fig 5.2 SVM Accuracy



Upload the CSV

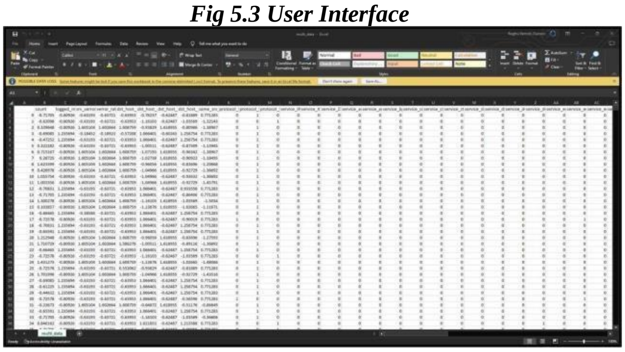
test_doc.csv

which model do you want to use?

KNN

Intrusion Detected of type: R2L

Fig 5.3 User Interface



6. TESTING

TYPES OF TESTING

Software testing is an important step where a detailed plan is made to test the software. This plan has lots of parts that will make the product better in general. A product is something that is made to sell or use. The testing guide tells you what to do, when to do it, and how much to do. To do this well, you need to put in a lot of effort, spend a lot of time, and use many materials. The process is about making a plan, doing tests, gathering information, and analysing the results. This process helps experts and gives management a list to look at. Using exact numbers is important to track how far we have come, and we need to find and fix any problems early on to prevent them from getting worse. It is important to make a plan quickly to make sure the product is good and does well.

6.1 UNIT TESTING:

Unit testing is a critical aspect of software development that focuses on testing individual modules or components of software to ensure their functionality meets the designer's requirements. Typically, unit testing is performed on completed modules after they have been turned into an executable format. The primary goal of unit testing is to test the individual module's functionality in isolation, without the need for the entire system to be fully implemented.

The scope of unit testing is limited to the designer's requirements and focuses on testing the functionality of the software module. This approach enables developers to identify and correct any defects or bugs in the software early in the development process, saving time and resources in the long run.

Unit testing becomes even more critical when a module is composed with high cohesion, which reduces the number of experiments required to ensure the module's functionality. By simplifying the testing process, errors can be more easily predicted and revealed, allowing developers to address them promptly before they cause significant problems in the system.

Overall, unit testing is an essential practice in software development that allows developers to identify and correct issues in individual modules before they impact the entire system. By conducting unit tests, developers can ensure that each module is functioning as intended, which can increase the overall quality of the software and minimize the risk of errors or bugs that could impact the end-users.

6.2 Black Box Testing

Black-box testing is a type of software testing where we check if the program works correctly without knowing how it was made. It's also called functional testing. The tester does not know how the software works inside. The main idea Black-box testing checks the software's features by looking at what goes into it. This means that you get results from the computer program, but you don't know how the program came up with those results. In black-box testing, the tester focuses solely on the software's specifications and requirements, without considering the software's internal code. This approach is beneficial because it does not require the tester to have any specific knowledge of the programming language or the internal workings of the software.

Black-box testing typically involves analysing the software's inputs and expected outputs, and comparing them to the actual results to identify any discrepancies or defects. By conducting black-box testing, testers can ensure that the software meets the specified requirements and performs as expected, regardless of its internal workings.

Black-box testing is an important way to test software. It helps testers understand how well the software works. This means that the software can be used easily without needing to understand how it works behind the scenes. When you pay attention to one thing, it helps you do it better. Testers can find and fix problems in software early by looking at what goes into it and what comes out of it. Making better software and decreasing the chances of things going wrong by working on it. This means mistakes or problems that could affect the people who use something.

6.3 WHITEBOX TESTING:

In white-box testing, the person checking the software can see how it works inside and can judge it. The way something is built, looks, and the methods used to create it. White-box testing aims to analyse the internal workings of a system or program in order to evaluate its accuracy and effectiveness. Make sure that the program works the way it is supposed to by checking the code. The person who checks if things work as they should, checks to see if something is working correctly. The program is working how it's supposed to and you should be able to see all of the code. For the person who is testing.

White-box testing is typically performed during the development phase and is useful in identifying issues such as incorrect calculations or missing functionalities that might have been missed during black-box testing.

7. CONCLUSION

After undergoing these algorithms and processes, it can be concluded that it is possible to create and machine learning model which can accurately predict and detect intrusions within a network. Accurate and timely detection of intrusions by unauthorized parties into the network can lead to better security of user data for an organization and also allow for detecting and auditing which data was compromised in the intrusion. The models and the data do not require much overhead and negligible data pre-processing, so it is light-weight and does not require much processing power once the model is trained. A NIDS is essential for every organization that values security.

8. FUTURE SCOPE

The project discovered really good results in detecting unwanted people with a high success rate. In the future, the Network Intrusion Detection System (NIDS) could be combined with a Security Information and Event Management (SIEM) system to watch over a network and keep track of what's happening. Adding a Network Intrusion Prevention System (NIPS) can help stop intruders before they cause problems. NIPS can do more than just detect intrusions, which is all that a NIDS can do. These improvements would make the network much safer and more secure.

9. REFERENCES

[1]A novel statistical analysis and autoencoder driven intelligent intrusion detection approach https://doi.org/10.1016/j.neucom.2019.11.016

[2] Towards a Reliable Comparison and Evaluation of Network Intrusion Detection Systems Based on Machine Learning Approaches **https://doi.org/10.3390/app10051775**

[3] Agarwal A, Sharma P, Alshehri M, Mohamed AA, Alfarraj O. 2021. Classification model for accuracy and intrusion detection using machine learning approach. PeerJ Computer Science 7:e437 https://doi.org/10.7717/peerj-cs.437

[4]J. Alikhanov, R. Jang, M. Abuhamad, D. Mohaisen, D. Nyang and Y. Noh, "Investigating the Effect of Traffic Sampling on Machine Learning-Based Network Intrusion Detection Approaches," in IEEE Access, vol. 10, pp. 5801-5823, 2022, doi: 10.1109/ACCESS.2021.3137318.

[5]F. Mosaiyebzadeh, L. G. Araujo Rodriguez, D. Macêdo Batista and R. Hirata, "A

Network Intrusion Detection System using Deep Learning against MQTT Attacks in IoT," 2021 IEEE Latin-American Conference on Communications (LATINCOM), 2021, pp. 1-6, doi: 10.1109/LATINCOM53176.2021.9647850.