RootDefender: Strengthening Network Security with Random Forest Intrusion Detection

Anshul Kumar[1], Prashant Sharma[2], Avinash[3], Pummy[4] Harish Kumar[5], Shiva Garg[6]

[1,2,3,4]B. Tech (CSE) IV Year, H.R. Institute of Technology, Ghaziabad, India
[5,6] Professor CSE, H.R.Institute of Institution, Ghaziabad, India

---***---

Abstract – An IDS Intrusion Detection System play a crucial role in modern cybersecurity, which figure out and outputs to unauthorized access and cyberattacks within a network or internet. IDS aims to enhance flexibility and adaptability in detecting diverse intrusion attempts. This approach allows for seamless integration into existing infrastructures, minimizing deployment complexities. By using advance machine learning tools and techniques, IDS use to analyze network traffic patterns, system logs, and behavioral anomalies to identify the strengthen behavior in live scenarios. This proactive stance enables timely responses to potential threats, reducing the risk of data breaches and system compromises. Moreover, easy customization and scalability, empowering organizations to tailor IDS solutions to their specific security requirements. This adaptability ensures efficient threat detection across varying network environments and evolving cyber threats. Overall the abstract concept of intrusion detection system implementation represents a significant advancement in cybersecurity, offering enhanced detection capabilities and operational flexibility to safeguard digital assets and preserve data integrity.

1. INTRODUCTION

In this growing interconnected digital era, ensuring the integrity of computer networks and systems has become an imperative concern for organizations in all over the world. With the exponential growth of cyber threats and advance attack strategy, the need for robust intrusion detection mechanisms has never been more critical. Intrusion Detection Systems (IDS) serve as a frontline defense, persistently surveilling network activities and system activities to recognize and respond to malicious behavior promptly addressing. Traditional IDS solutions often face challenges in terms of flexibility, scalability, and adaptability to evolving threats. However, recent advancements in technology have led to the development of IDS architectures that offer greater freedom in deployment and configuration. One such innovation is the concept of free-form plug-and-play intrusion detection systems. This research paper explores the concept of free-form plug-and-play IDS and its implications for enhancing cybersecurity defenses. By breaking away from rigid architectures and embracing a more flexible approach, free-form plug-and-play IDS systems offer several potential benefits. These include easier integration into existing network infrastructures, reduced deployment complexity, and improved scalability to accommodate changing organizational needs. Furthermore, the incorporation of machine learning algorithms and advanced analytics techniques empowers free-form plug-and-play IDS to adapt dynamically to emerging threats. By analyzing network traffic patterns, system logs, and behavioral anomalies, these systems can detect and promptly addressing unauthorized access attempts and malicious activity in real time The. Final goal of this paper is to furnish a thorough understanding of IDS principles, and its practical implications for cybersecurity research and practice. Through the review of existing literature, case studies, and empirical analyses, we focus to evaluate the effectiveness and feasibility of implementing such IDS architectures in diverse organizational contexts. Ultimately, this research paper seeks to contribute to the ongoing discourse on intrusion detection systems and advance the development of innovative cybersecurity solutions capable of addressing the evolving threat landscape effectively. By harnessing the potential of free-form plug-and-play IDS, organizations can bolster their cyber defenses and safeguard critical assets against sophisticated cyberattacks.

2. LITERATURE SURVEY

[1]"A Survey of Intrusion Detection Systems: Techniques, Challenges, and Future Trends" by Alazab et al. (2012):This comprehensive survey provides an synopsis of different intrusion detection techniques, including Anomaly-based and signature-based techniques. It discusses the challenges faced by traditional IDS solutions and explores emerging trends, such as machine learning and data mining, in enhancing detection capabilities.[2]**"Intrusion Detection Systems: A Review and Comparative Study"** by Garcia Teodoro et al. (2009):The paper presents a comparative analysis of different intrusion detection systems, highlighting their strengths, weaknesses, and performance metrics. It covers both network-based and host-based IDS solutions, offering insights into their effectiveness in detecting and mitigating cyber threats.[3]**"Anomaly-Based Intrusion Detection: Techniques, Challenges, and Opportunities"** by Patcha and Park (2007):Focusing on anomaly-based intrusion detection techniques, this paper explores the principles, methodologies, and challenges associated with detecting abnormal behavior in network traffic. It discusses the potential of anomaly detection in addressing zero-day attacks and emerging threats.[4]**"Machine Learning Techniques for Intrusion Detection: A Review"** by Muda et al. (2011):This research paper uses the application of machine learning algorithms in intrusion detection systems. It works on various machine learning methodology including the neural networks, support vector machines, and decision trees, and evaluates the efficiency in identifying the intrusion and anomalies.[5]**"A Survey of Intrusion Detection Systems Utilizing Machine Learning Techniques"** by Alazab et al. (2011):Focusing specifically on machine learning-based IDS solutions, this survey explores the use of supervised, unsupervised, and semi-supervised learning algorithms in detecting and classifying intrusions. It discusses the advantages and limitations of different machine learning approaches in real-world deployment scenarios.[6]**"Intrusion Detection Systems: A Review"** by Darwish et al. (2010):[7]This review provides an in-depth analysis of intrusion detection systems, covering their architecture, components, and detection mechanisms. It discusses the evolution of IDS technologies over time and evaluates their efficacy in mitigating various types of cyber threats.[7]**"A Review of Intrusion Detection Systems Based on Machine Learning Techniques"** by Siddiqui et al. (2019):Focusing on recent advancements in intrusion detection systems, this review paper examines the role of machine learning techniques in enhancing detection accuracy and reducing false positives. It discusses the integration of deep learning and ensemble learning approaches in IDS solutions.[8]**"Intrusion Detection Systems: A Review"** by Hameed and Hussain (2016):This review provides an overview of intrusion detection systems, covering their classification, detection techniques, and evaluation methodologies. It discusses the importance of real-time monitoring and response capabilities in modern IDS architectures.

3.METHODOLOGY

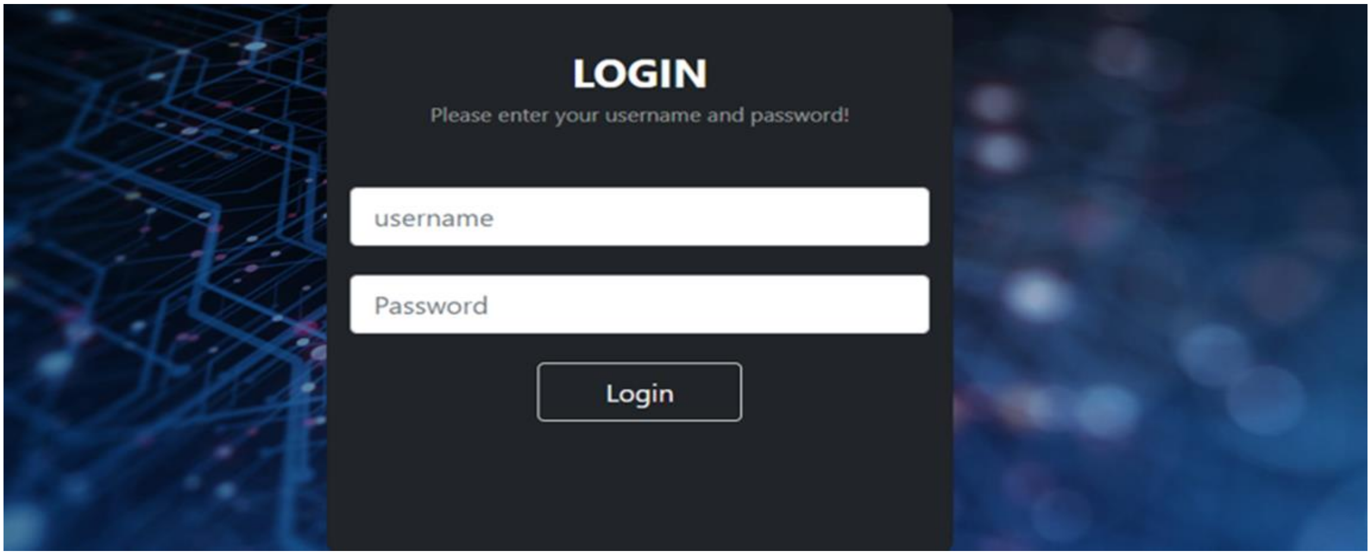
We made an IDS which works on real-time role-based scenarios which access the data from the Dataset that would first open the user to login, then further user with login, after the successful login user will be able to pass the input credentials to the machine learning model. After passing the details the user has a start detection button to starting the detection. After successful detection the user will get one popup on the screen about the information of what type of attack identified which is shown with the help of input data.

4.1. User Interface:

From the starting of the user interface design there are five file pages are as follow, HTML files which are used for the website – index, dashboard, home, home_2, and home_2 page. When user get the successful login then, user will get the dashboard where user will found the information or insight of the KDD dataset which is necessary for the detection of the attack and on the same screen there is a button which is provided to start the detection, after clicking on that button user will directed to the next screen which is home screen where user will have to provide the required data or information to detect the cyberattack. Similarly after the home page user will directed to home_2 and home_3 to fill the more details for the further detection. At the end , after entering all details the user can start the detection by simply clicking on the button, this button is connected with the functions which will provide the input data or information of the attack into the ML trained model and will show the result on the same screen using popup window which already contains the information of the type of different - different intrusion attack.

4.2. Django as Framework: This Ids model is based on Django framework, Django uses the high-level Python web framework that is used for the rapid development and clear, sensible design. Every Web app which we create in Django is known as project; and a project is a combination of applications. Set of code file is known as application relying on the MVT pattern. For example, suppose we want to build a website, the website is our project and the forum, news, contact engine are applications. Every application is independent because this structure makes it easier to move an application between projects. Following structure is the output of every Django web-app.

4.3.Application UI Design or Output: The below Fig 4.1 shows the user login page where users will enter the credentials to login to the IDS which is the login page of output



LOGIN

Please enter your username and password!

Fig 4.1 Dashboard page with login details

These 2 Fig 4.2 are showing the data, like protocol type and attack type at different- different time, which are stored inside our dataset KDD99 Which is learned by us to our model

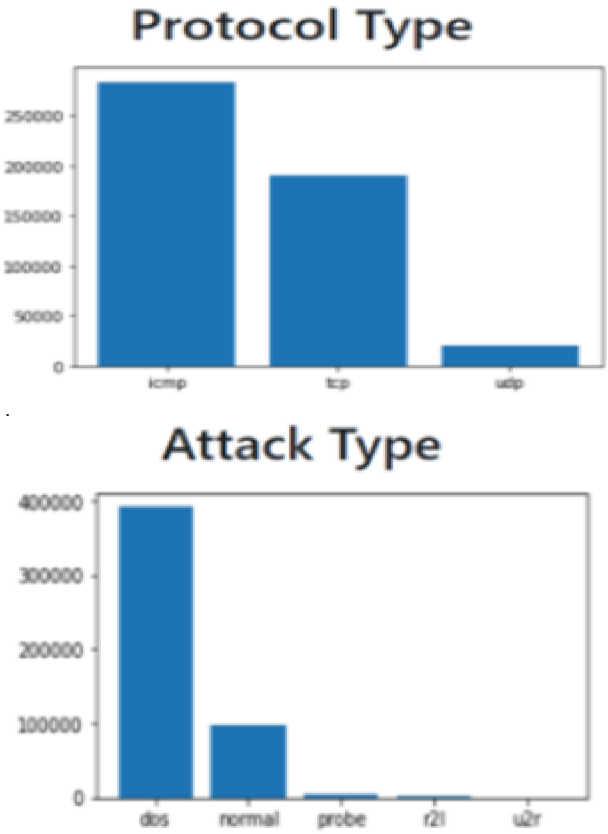
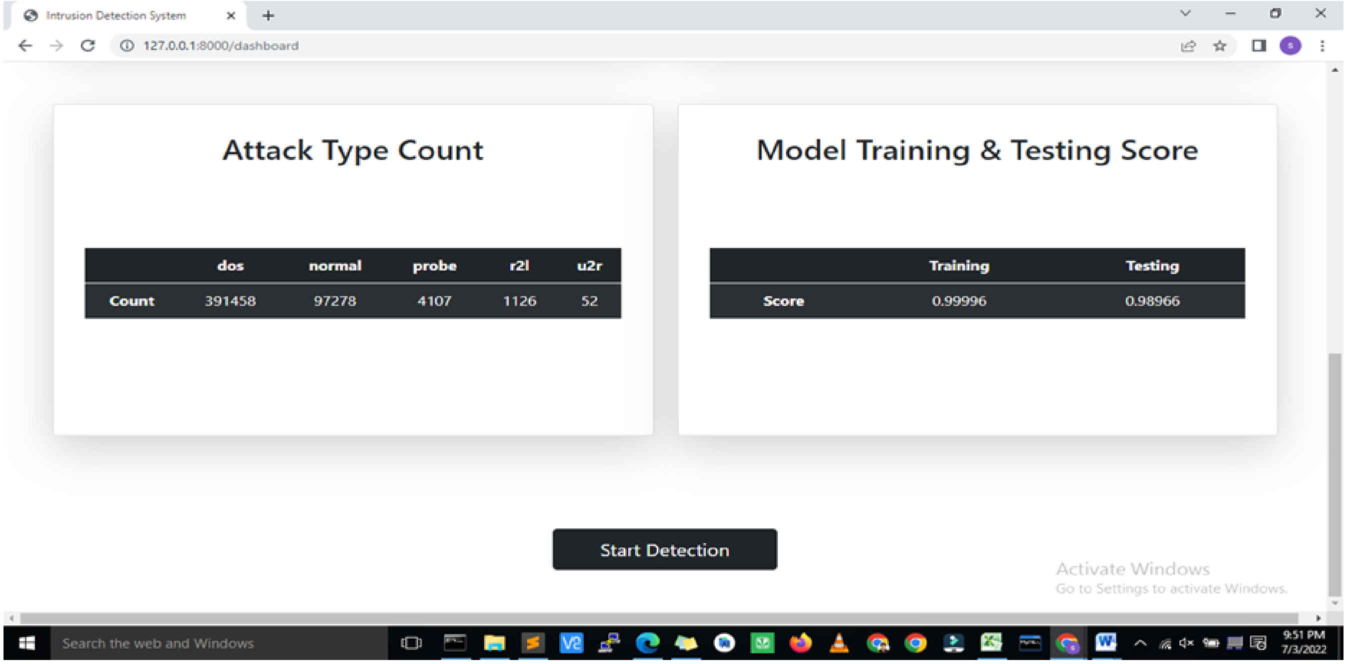


Fig 4.2 Dashboard page with type of protocol used and what type of attack is

This below first Fig 4.3 providing the details like what type of attack our project will show along with the count of attack in the respective fields like

Dos, normal, probe, r21, u2r, second Fig 4.3 is showing the testing and training score of the model, means how efficient our model is.


Intrusion Detection System
127.0.0.1:8000/dashboard
Start Detection
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
9:51 PM
7/3/2022

Attack Type Count

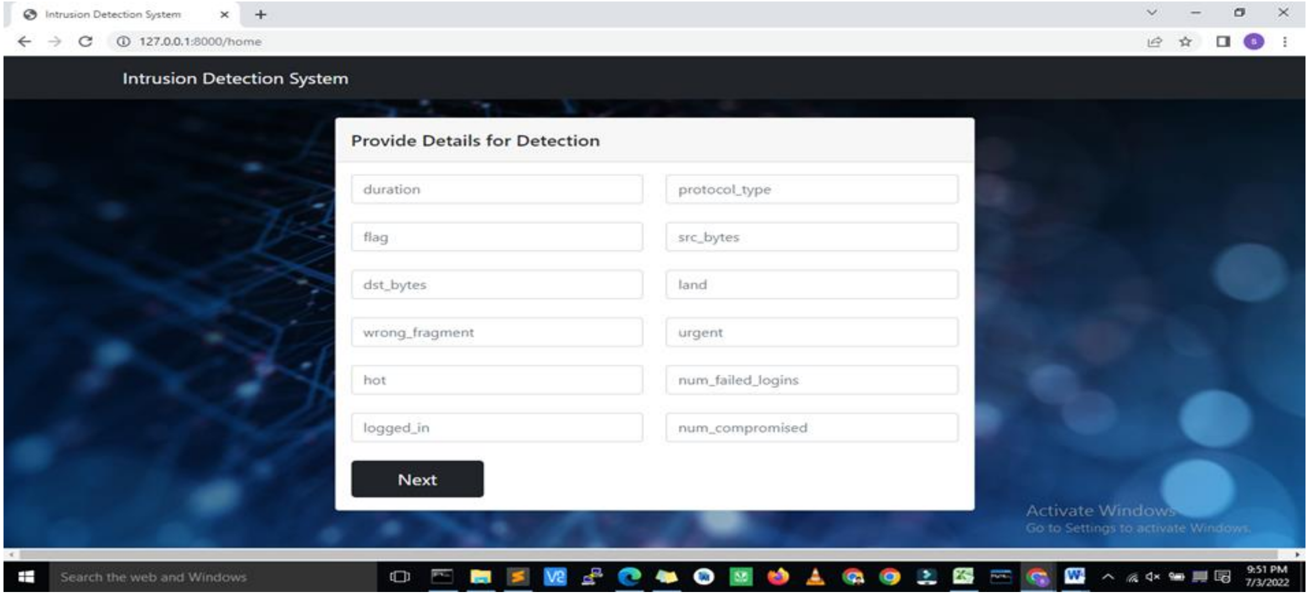
	dos	normal	probe	r2l	u2r
Count	391458	97278	4107	1126	52

Model Training & Testing Score

	Training	Testing
Score	0.99996	0.98966

Fig 4.3 Start Detection Button

The below mentioned Fig 4.4 is asking for the details to the user for detecting the attack type

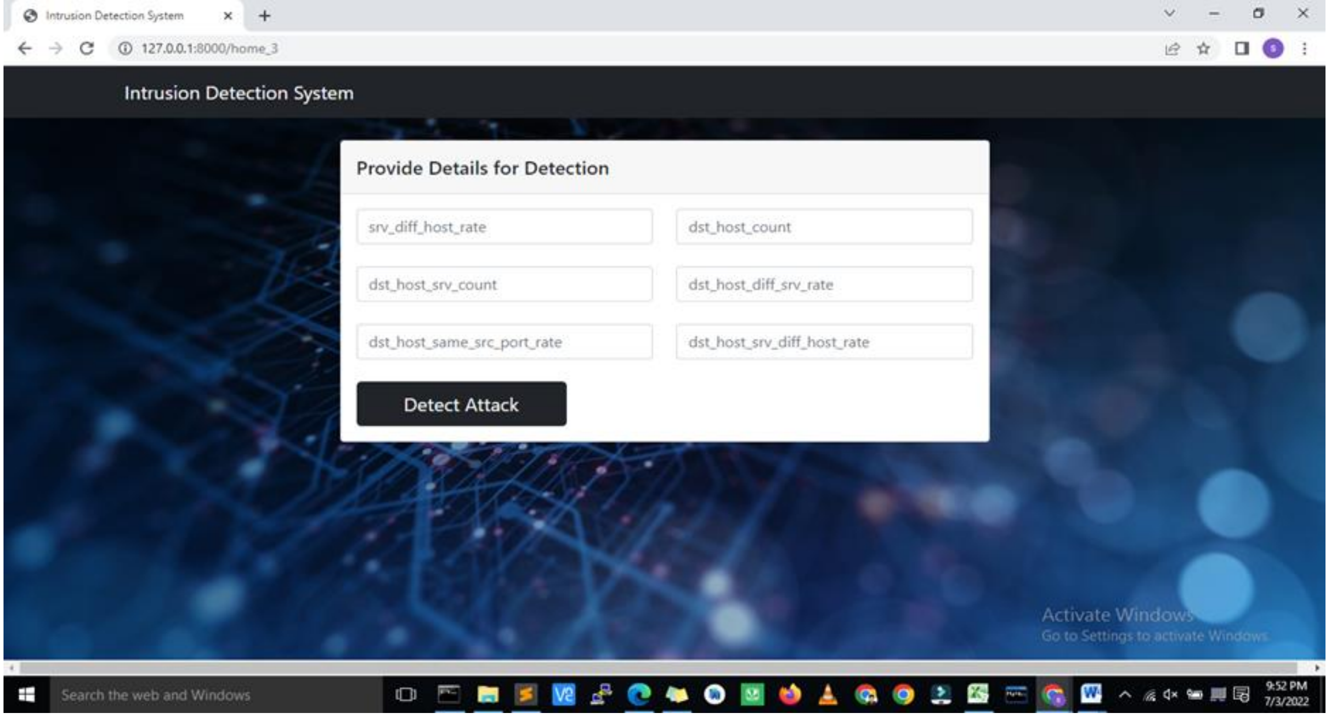

Intrusion Detection System
127.0.0.1:8000/home
Intrusion Detection System
Next
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
9:51 PM
7/3/2022

Provide Details for Detection

duration	protocol_type
flag	src_bytes
dst_bytes	land
wrong_fragment	urgent
hot	num_failed_logins
logged_in	num_compromised

Fig 4.4 asking for the Details Page for detection

The below Fig 4.5 is asking for the other required details needed during the detection of the attack


Intrusion Detection System
127.0.0.1:8000/home_3
Activate Windows
Go to Settings to activate Windows
Search the web and Windows
9:52 PM
7/3/2022

Intrusion Detection System

Provide Details for Detection

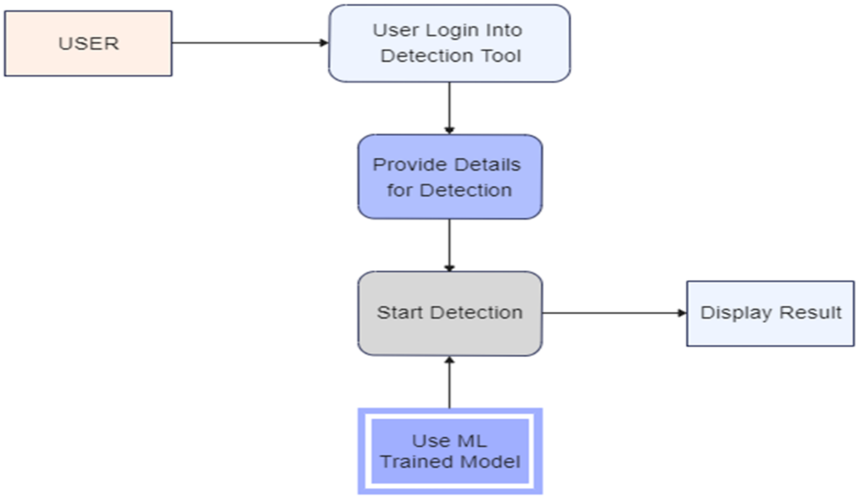
srv_diff_host_rate
dst_host_count
dst_host_srv_count
dst_host_diff_srv_rate
dst_host_same_src_port_rate
dst_host_srv_diff_host_rate

Detect Attack

Fig 4.5 is asking for the further Details required in detection of the attack type with start button

The given Fig 4.6 is showing the full implementation of the project that what is required for the designing of the project and how all the algorithms are working and display the final output of the detected result.

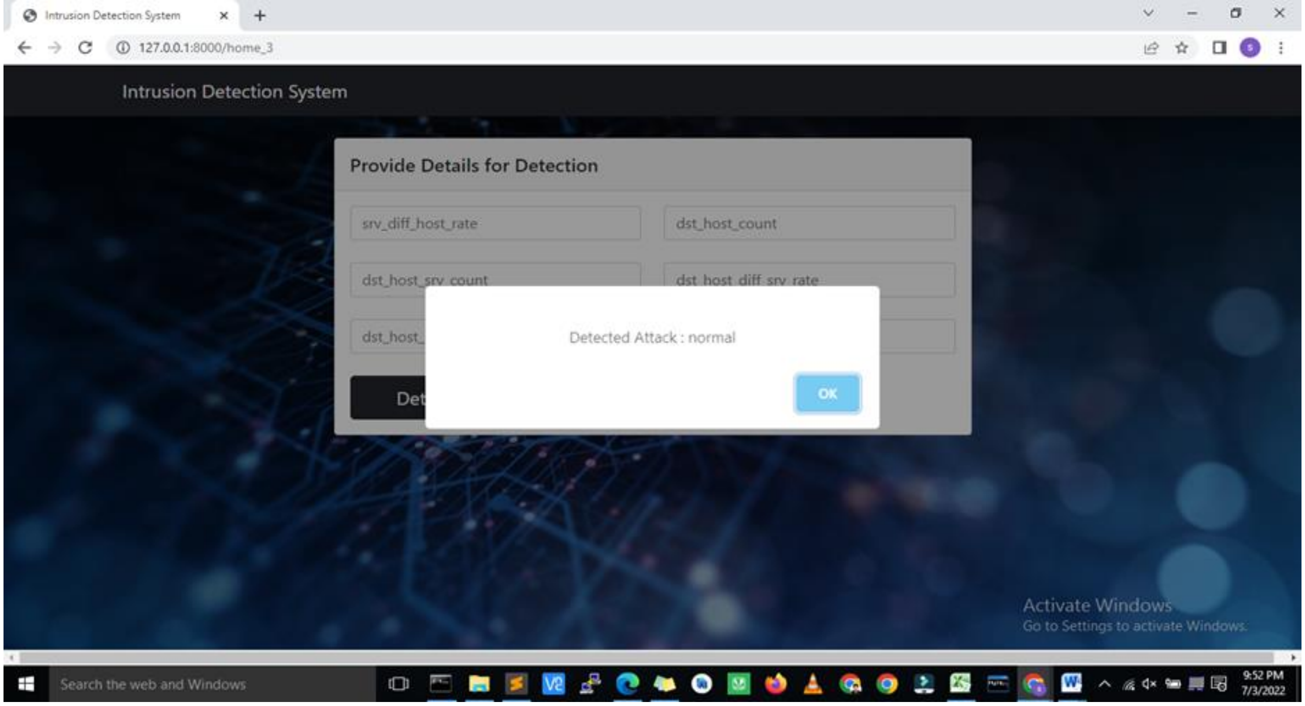
Implementation



4.RESULTS

The IDS demonstrates high accuracy in detecting attack type, normal , advance, or doc by putting different values for checking the correct output as we require. User feedback indicates a positive experience with desired output.

Future importance could include implementing IDS for personal and normal open to all use.


Intrusion Detection System
127.0.0.1:8000/home_3
Intrusion Detection System
OK
Det
Search the web and Windows
9:52 PM
7/3/2022

Provide Details for Detection

srv_diff_host_rate
dst_host_count
dst_host_srv_count
dst_host_diff_srv_rate
dst_host_

Detected Attack : normal

Activate Windows
Go to Settings to activate Windows.

5. CONCLUSION AND FUTURE SCOPE

Now at the end, output of this project Intrusion Detection System is valuable during finding out the type of attack over the network or Internet. This tool can be used by any user very easily because its User Interface is completely user-friendly and responsive due to that reason user can work easily on this tool and easily understand the behavior of the tool. Moreover, this id system have good accuracy which is our ultimate requirement for any type of detection using this tool and this type of tool. With the help of random forest algorithm and KDD CUP 99 dataset We are able to detect the five different types of attacks. In the upcoming future we can do some enhancement in this tool to make it more productive and fast so it can solve multiple problem of the different users at the time of need:

oFacility to onboard additional users

oMore engaging user interface

oFacilities to identify the alternative forms of attacks

oIn the future we aim to enhance precision for better outcomes

oMake the application live so that everyone can use this.

REFERENCES

[1]"A Survey of Intrusion Detection Systems: Techniques, Challenges, and Future Trends" by Alazab et al. (2012)

[2]"Intrusion Detection Systems: A Review and Comparative Study" by Garcia Teodoro et al. (2009)

[3]"Anomaly-Based Intrusion Detection: Techniques, Challenges, and Opportunities" by Patcha and Park (2007)

[4]"Machine Learning Techniques for Intrusion Detection: A Review" by Muda et al. (2011)

[5]"A Survey of Intrusion Detection Systems Utilizing Machine Learning Techniques" by Alazab et al. (2011)

[6]"Intrusion Detection Systems: A Review" by Darwish et al. (2010)

[7]"A Review of Intrusion Detection Systems Based on Machine Learning Techniques" by Siddiqui et al. (2019)

[8]"Intrusion Detection Systems: A Review" by Hameed and Hussain (2016)