IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

INTRUSION DETECTION OF CYBER ATTACK

GANGADHAR M L[1], AISHWARYA T S[2], JYOTHIKA M H[3] ,KAVANA S[4]

Asst. Prof, Dep of ISE, Sri Siddhartha Institute of Technology, Tumkur, India [1]

UG Student, ISE dept, Sri Siddhartha Institute of Technology, Tumkur, India [2]

UG Student, ISE dept, Sri Siddhartha Institute of Technology, Tumkur, India[3]

UG Student, ISE dept, Sri Siddhartha Institute of Technology, Tumkur, India[4]

Abstract: The worldwide reach and density of information have also raised the risk of integrity and confidentiality. Security lapses are become far too common. Thus, the enhancement of network security is emphasized these days. Network protection lets in unintentional interference of some kind and helps to prevent it. It is made up of network intrusion detection software that follows the network. To trace traffic within the network from source to destination apps, NIDS is strategically placed within the network. The device would efficiently filter all incoming and outgoing traffic, but this would lead to congestion, which would slow down the system's speed as a whole. Lastly, these techniques incorporate machine learning algorithms that provide dependable performance and flexibility for the gadget. Machine learning techniques can be used to identify patterns in the auditing data that indicate the difference between malicious and normal activity. This is because intrusion activities leave evidence behind.

Keywords: Intrusion Detection, Machine learning, Deep learning, HTML, Phishing Technique.

.

I. INTRODUCTION

Information systems constitute the cornerstone of each business, regardless of size or industry. Nevertheless, these information systems' services and the data they contain make them open to several kinds of attacks. These attacks, due to their extreme variety and system-specificity, can be disastrous. Given this, computer security has grown to be a significant concern, and more study is being done in this field. To guarantee a level of safety that satisfies the needs of modern living, a variety of instruments and systems are devised. The Intrusion Detection System (IDS) is one of these tools.

IDS are tools made to recognize unusual activity and behaviors intended to obstruct the system's normal operation, as well as to detect attempted network attacks. The three types of intrusion detection systems are hybrid intrusion detection systems (IDS), host-based IDS, and network-based IDS. and keep an eye on all network traffic to spot malicious activities. Generally speaking, network interface cards are placed in promiscuous mode to record all network traffic segments when installing intrusion detection systems. On the other hand, encrypted traffic data to a particular host is monitored by HIDS. It utilizes data gathered from within a single computer system. Combining the best features of both NIDS and HIDS, hybrid IDS. They make network and terminal monitoring possible. IDS that is network-based.IDS are technologies made to find instances of insider or outsider misuse, unwanted access, and signatures on a computer network. It takes specialist software to gather data flowing through the system, which is then used in the detection phase, in order to identify potential attacks on the system. Several tools are available to do this duty; Wireshark, Snort, and Prelude are a few examples of network traffic sniffers. Unfortunately, processing the vast amounts of data from this collection instrument using the current techniques takes a long time.

Algorithms like K-means, the Hidden Markov Model, and Self-Organizing Maps (SOM); neural networks, decision trees, Naive Bayes, and Support Vector Machine are examples of machine learning (ML) based IDS systems.

Recently, Deep Learning (DL) has brought state-of-the-art capabilities to domains like computer vision and natural language processing, revolutionizing numerous fields in new ways.

II. BACKGROUND STUDY

2.1 Wang Peng, Xiangwei Kong, Goujin Peng proposed a “Network Intrusion Detection Sytem”.With the continuous development of computer network technology, security problems in the network are emerging one after another, and it is becoming more and more difficult to ignore. For the current network administrators, how to successfully prevent malicious network hackers from invading, so that network systems and computers are at Safe and normal operation is an urgent task. This paper proposes a network intrusion detection method based on deep learning. This

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

method uses deep confidence neural network to extract features of network monitoring data, and uses BP neural network as top level classifier to classify intrusion types. The method was validated using the KDD CUP'99 dataset from the Lincoln Laboratory of the Massachusetts Institute of Technology. The results show that the proposed method has a significant improvement over the traditional machine learning accuracy.

2.2 Yin Chuan-long, Zhu Yue-fei, Fei Jin-long, He Xin-zheng proposed "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" Showing that intrusion detection plays an important role in ensuring information security, and the key technology is to accurately identify various attacks in the network. In our study, we explore how to model an intrusion detection system based on deep learning, and we propose a deep learning approach for intrusion detection using recurrent neural networks (RNN-IDS). Moreover, we study the performance of the model in binary classification and multiclass classification, and the number of neurons and different learning rate impacts on the performance of the proposed model. We compare it with those of J48, Artificial Neural Network, Random Forest, Support Vector Machine and other machine learning methods proposed by previous researchers on the benchmark dataset. The experimental results show that RNN-IDS is very suitable for modeling a classification model with high accuracy and that its performance is superior to that of traditional machine learning classification methods in both binary and multiclass classification. The RNN-IDS model improves the accuracy of the intrusion detection and provides a new research method for intrusion detection.

2.3 Mr. Gunjal Somnath P, Prof. Aher S M, proposed "Network Intrusion Detection using Recurrent Neural Network Algorithm" Which describes that Internet is a widely used platform nowadays by people across the word. This has led to the advancement in science and technology. Many surveys conclude that network intrusion has registered a consistent increase and lead to personal privacy theft and has become a major platform for attack in the recent years. Network intrusion is unauthorized activity on a computer network. Hence there is a need to develop an effective intrusion detection system. In proposed system acquaint an intrusion detection system that uses improved recurrent neural network (RNN) to detect the type of intrusion. In proposed system also shows a comparison between an intrusion detection system that uses other machine learning algorithm while using smaller subset of kdd99 dataset with thousand instances and the KDD-99 dataset.

2.4 Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, Farhan Ahmad have published the IEEE papers based on "Network intrusion detection system: A systematic study of machine learning and deep learning approaches" Which shows that the rapid advances in the internet and communication fields have resulted in a huge increase in the network size and the corresponding data. As a result, many novel attacks are being generated and have posed challenges for network security to accurately detect intrusions. Further, the presence of the intruders with the aim to launch various attacks within the network cannot be ignored. An intrusion detection system (IDS) is one such tool that prevents the network from possible intrusions by inspecting the network traffic, integrity, and availability. IDS still faces challenges in improving detection accuracy while reducing false alarm rates and in detecting novel intrusions. Recently, deep learning (DL)-based IDS systems are being deployed as potential solutions to detect intrusions across the network in an efficient manner. This article first clarifies the concept of IDS and then provides the taxonomy based on the notable DL techniques adopted in designing network-based IDS (NIDS) systems. A comprehensive review of the recent NIDS-based articles is provided by discussing the strengths and limitations of the proposed solutions.

III. EXISTING SYSTEM

- Several real attacks are far less than the number of false alarms raised. This causes real threats to go often unnoticed.
- Noise can severely reduce the capabilities of the IDS by generating a high false-alarm rate.
- Constant software updates are required for signature-based IDS to keep up with the new threats.
- IDS monitor the whole network, so are vulnerable to the same attacks the network's hosts are. Protocol-based attacks can cause the IDS to fail.
- Network IDS can only detect network anomalies which limit the variety of attacks it can discover.
- Network IDS can create a bottleneck as all the inbound and outbound traffic passes through it.
- Host IDS rely on audit logs, any attack modifying audit logs threaten the integrity of HIDS.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

IV. PROPOSED SYSTEM

4.1 Data gathering

Is the initial and most important stage of intrusion detection. Two essential components that determine an intrusion detection system's design and efficacy are the kind of data source and the place from which data is gathered. This study suggests a network-based intrusion detection system (IDS) to verify our suggested strategies and give the optimum protection for the targeted host or networks.

The suggested intrusion detection system (IDS) tracks incoming network data while operating on the router closest to the victim(s). The gathered data samples are labelled against the domain knowledge and categorised according to the transport/Internet layer protocols during the training phase. Nevertheless, the test stage data collection is merely categorised based on protocol kinds.

4.2 Preprocessing the Data

The initial step involves processing the data collected to produce fundamental features, similar to those found in the KDD Cup 99 dataset. There are three primary stages in this phase, which are as follows.

4.3 Transferring data

Every record in the input data must be represented as a vector of real numbers by the trained classifier. As a result, each symbolic feature in a dataset is initially assigned a numerical value. For instance, the KDD CUP 99 dataset has both symbolic and numerical properties. The protocol type (e.g., TCP, UDP, and ICMP), service type (e.g., HTTP, FTP, Telnet, and so forth), and TCP status flag (e.g., SF, REJ, and so forth) are examples of these symbolic properties. All that the method does is substitute numeric values for the values of the category characteristics.

4.4 Data transfer

The trained classifier needs to represent each record in the input data as a vector of real values. Consequently, a numerical value is first assigned to each symbolic feature in a dataset. The KDD CUP 99 dataset, for example, contains both numerical and symbolic attributes. These symbolic properties include the protocol type (e.g., TCP, UDP, and ICMP), service type (e.g., HTTP, FTP, Telnet, and so on), and TCP status flag (e.g., SF, REJ, and so on). The approach just modifies the values of the category features by replacing them with numerical values.

V. SYSTEM MODELLING AND DESIGN

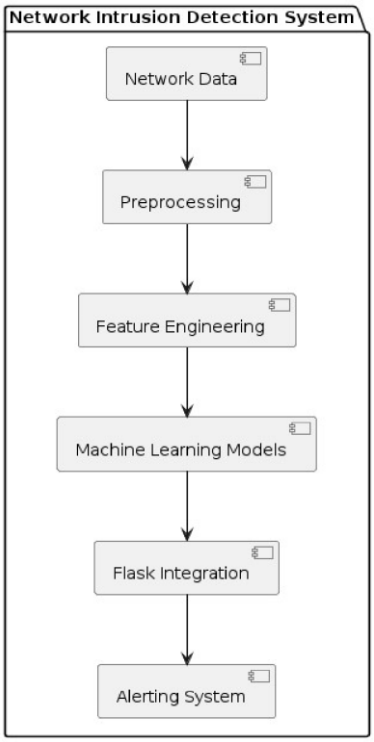

Fig 5.1 System Architecture

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

STATE DIAGRAM:

A flowchart is a type of diagram that represents an algorithm, workflow or process. Flowchart can also be define as a diagrammatic representation of an algorithm (step by step approach to solve a task). The flowchart shows the steps as boxes of various kinds, and their order by connecting the boxes with arrows.

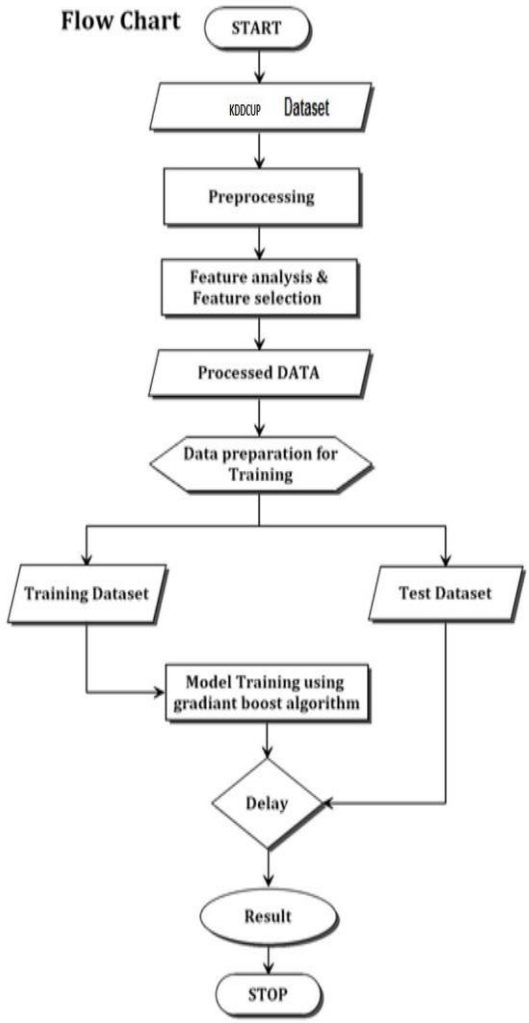

Fig 5.2 State Diagram

At the core of our NIDS is the utilization of two powerful machine learning algorithms: XGBoost and Random Forest. These algorithms excel in detecting patterns and anomalies within vast datasets, making them ideal candidates for identifying suspicious network behavior indicative of potential intrusions

.

XGBoost: Known for its scalability and efficiency, XGBoost is a gradient boosting algorithm that excels in classification tasks. By leveraging its ensemble learning capabilities, our NIDS can effectively classify network traffic and identify deviations from normal behavior, thereby flagging potential intrusions with high accuracy.

Random Forest: Renowned for its robustness and versatility, Random Forest is an ensemble learning technique that operates by constructing a multitude of decision trees during training and outputting the mode of the classes for classification. By harnessing the collective wisdom of multiple decision trees, our NIDS can effectively handle large volumes of network data while maintaining high detection rates and low false positive rates.

Flask Integration for Seamless Deployment:

In addition to its advanced machine learning capabilities, our NIDS features seamless integration with Flask, a lightweight web framework for Python. This integration allows for easy deployment and management of the detection system, enabling organizations to quickly deploy and scale their intrusion detection infrastructure as needed.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

Real-time Monitoring: With Flask integration, administrators can access real-time dashboards and reports, providing insights into network activity and intrusion alerts as they occur. This enables swift response to potential threats and enhances overall network security posture.

Scalability and Flexibility: Flask's modular architecture and extensibility make it well-suited for deployment in a variety of environments, from small-scale deployments to enterprise-level networks. Whether deployed on-premises or in the cloud, our NIDS with Flask integration offers scalability and flexibility to meet the evolving needs of organizations of all sizes.

VI. SYSTEM REQUIREMENTS SPECIFICATION

6.1 **Hardware Conditions**

- CPU: 2.4 GHz Pentium IV.
- 250 GB Hard Drive.
- Monitor: Colour 15 VGA.
- Memory: 1 GB
- Multimedia keyboard; optical mouse

6.2 **Software Conditions**

- Operating system: Windows 7 or later, or Windows XP Professional

Python is the coding language, and Jupiter Notebook is the IDE.

VII. RESULTS AND DISCUSSION

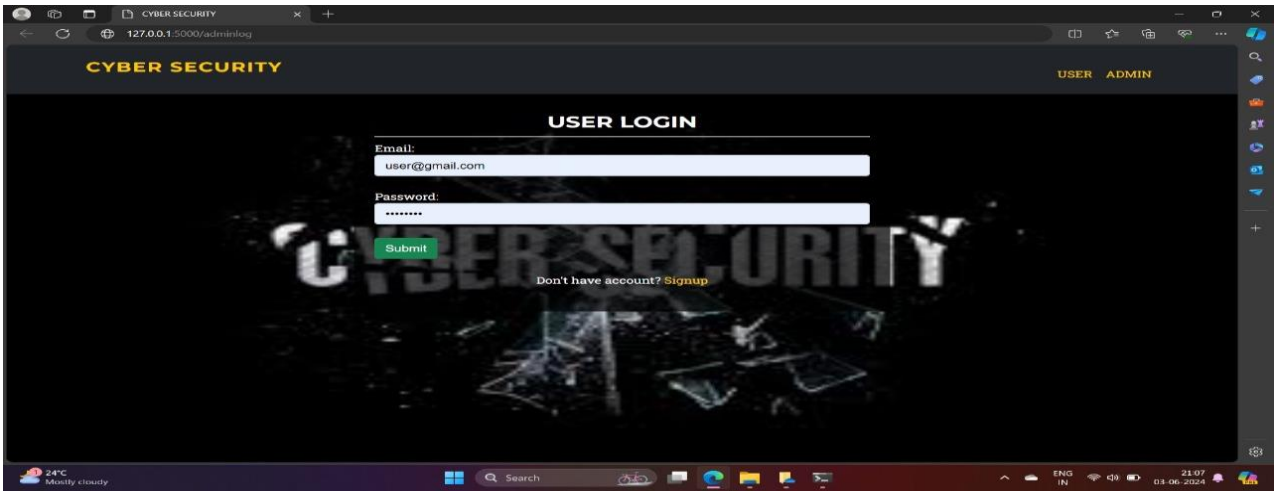

Fig 7.1 Login page

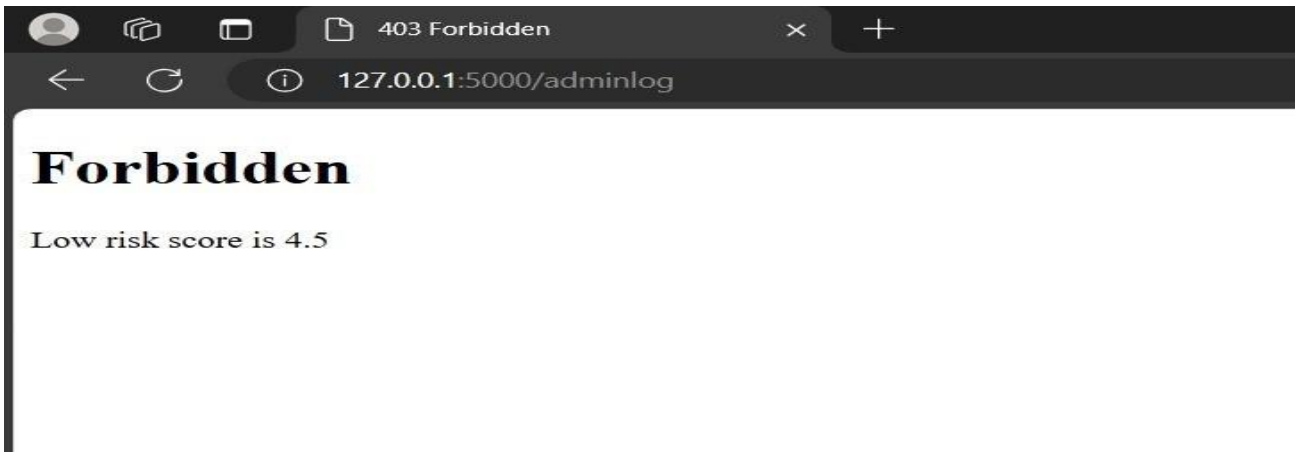

Fig 7.2 Showing Forbidden for admin log

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

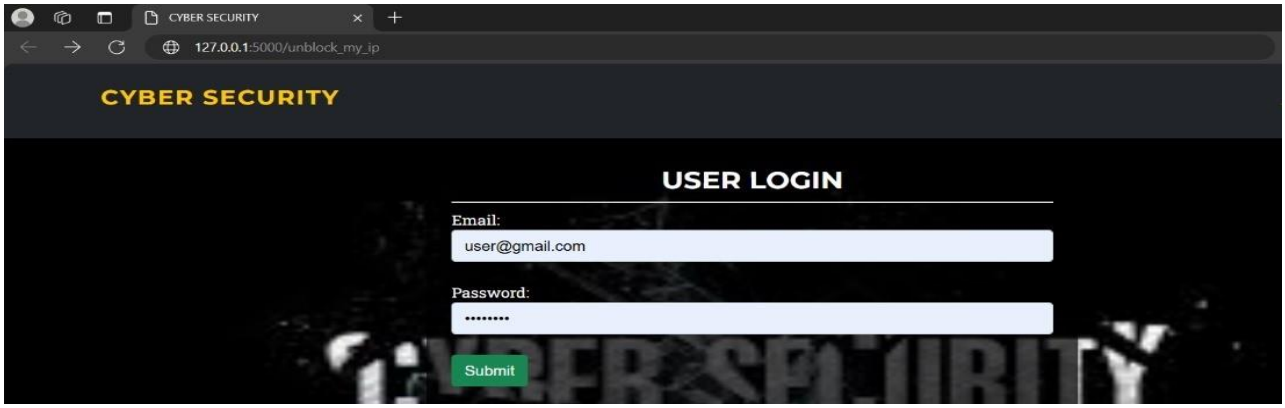

Fig 7.3 Unblocking ip

Fig 7.4 Unblocking successfully

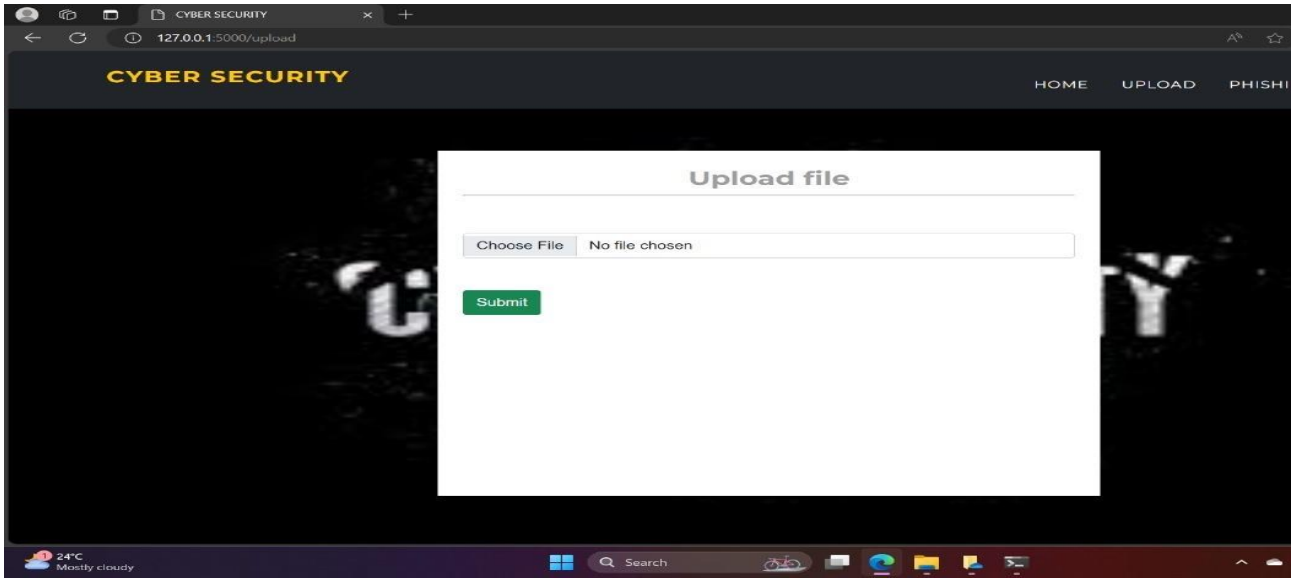

Fig 7.5 Uploading file

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

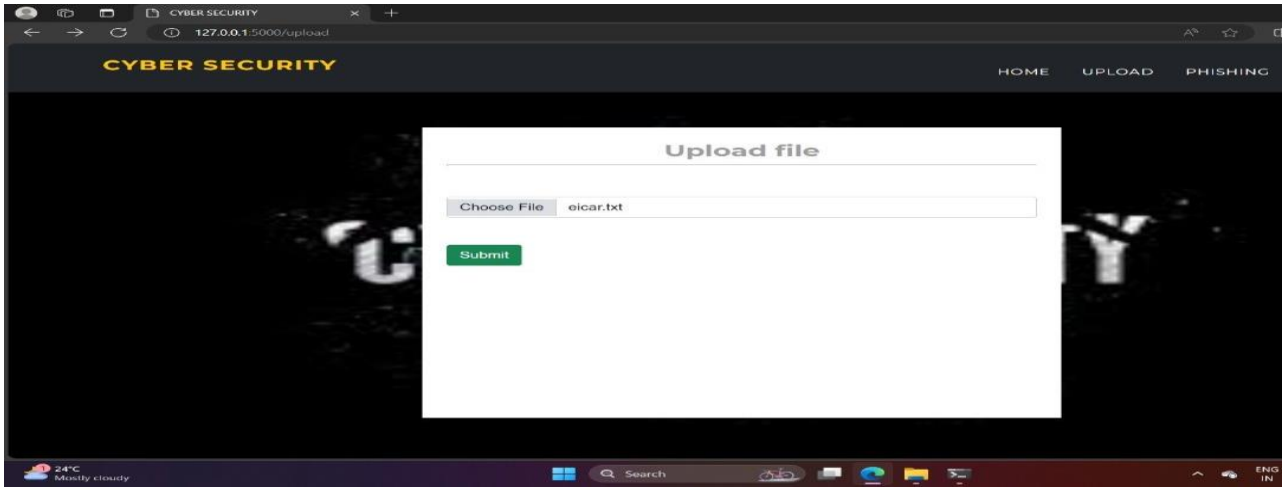

Fig 7.6 Uploading malicious file

Fig 7.7 Forbidden upload

VIII. CONCLUSION

In conclusion, the implementation of network intrusion detection using XGBoost and Random Forest machine learning techniques, integrated with Flask, marks a significant step forward in bolstering cybersecurity measures for modern networks. Through the amalgamation of powerful machine learning algorithms and the flexibility of Flask web framework, our solution offers a robust and dynamic approach to detecting and mitigating network intrusions.By harnessing the predictive capabilities of XGBoost and Random Forest, our system can effectively analyze network traffic patterns and identify suspicious activities in real-time, enabling timely responses to potential threats. Moreover, the integration with Flask provides a user-friendly interface for administrators to monitor network security status, configure detection parameters, and take appropriate actions as needed.

REFERENCES

[1] . Adetunmbi, Adebayo O et al. (2008). “Network intrusion detection based on rough set and k-nearest neighbour”. In: International Journal of Computing and ICT Research 2.1, pp. 60–66.

[2] . Bambrick, Noel (2016). Support Vector Machines: A Simple Explanation. https: / / www .kdnuggets . com / 2016 / 07 / support - vector - machines - simple - explanation.html. — (2017). Understanding Support Vector Machine(SVM) algorithm. https://www. analyticsvidhya . com / blog / 2017 / 09 / understaing - support - vector - machine-example-code/.

[3] . Bouckaert, Remco R (2004). “Naive bayes classifiifiers that perform well with continuous variables”. In: Australasian joint conference on artifificial intelligence. Springer, pp. 1089–1094.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11625

[4] . Brownlee, Jason (2019). What is Deep Learning. https://machinelearningmastery. com/what-is-deep-learning/. ML-Cheatsheet(2017).Logistic Regressionhttps://ml-cheatsheet.readthedocs. ssio/en/latest/logistic_regression.html.

[5] . Conrad, Eric, Seth Misenar, and Joshua Feldman (2017). "Chapter 7 - Domain 7: Security operations". In: Eleventh Hour CISSP R(Third Edition). Ed. by Eric Conrad, Seth Misenar, and Joshua Feldman. Third Edition. Syngress, pp. 145– 183. isbn: 978-0-12-811248-9. doi: https : / / doi . org / 10 . 1016 / B978 - 0 - 12 - 811248 - 9 . 00007 - 3. url: http : / / www . sciencedirect . com / science / article/pii/B9780128112489000073.

[6] . Dey, Amitabha (2018). Data Preprocessing for Machine Learning. https://medium. com / datadriveninvestor / data preprocessing - for - machine - learning - 188e9eef1d2c.

[7] . Dong, Bo and Xue Wang (2016). "Comparison deep learning method to traditional methods using for network intrusion detection". In: 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN).IEEE,pp.581–585.Educba(2020).Classifification https://www.educba.com/classificationalgorithms/. 7071.

[8] . LeCun, Yann, Yoshua Bengio, and Geoffffrey Hinton (2015). "Deep learning". In: nature 521.7553, pp. 436–444.