IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205291 |

Network Intrusion Detection System

Dr. S.K. Wagh[1], Aditya Shinde[2], Onkar Tambe[3], Apurva Lokhande[4], Vaishnavi Dusane[5]

Associate Professor, Department of Computer Engineering, Modern Education Society's Wadia College of Engineering, Pune, India[1]

Department of Computer Engineering, Modern Education Society's Wadia College of Engineering, Pune, India[2 3 4 5]

ABSTRACT: Over the last ten years, there has been a notable increase in intrusions within computer networks, driven by a profitable underground cybercrime sector and the accessibility of sophisticated intrusion tools. To address these challenges, researchers from industry and academia have extensively investigated methods to detect and prevent security breaches.Two main categories of solutions have emerged: signature-based and anomaly-based intrusion detection systems. Signature-based systems identify known attack patterns, while anomaly-based systems detect unknown attacks by modeling legitimate user behavior. Machine Learning (ML) techniques have played a crucial role in classifying such behavior, leading to the development of numerous ML-based intrusion detection systems.This paper provides a comprehensive and critical review of ML-based approaches for intrusion detection as presented in the literature over the past decade. It serves as a valuable resource for researchers and practitioners interested in ML-based intrusion detection systems and complements general surveys on intrusion detection. Additionally, the paper highlights unresolved issues in the field that require further investigation and attention.

KEYWORDS: KNN, SVM, LDA, QDA, Hping, Wireshark

I. INTRODUCTION

The escalating use of the internet has led to a surge in potential cyber threats, necessitating advanced detection systems for mitigation. An Intrusion Detection System (IDS) scrutinizes network traffic to pinpoint any malicious activities. Typically, IDS is categorized into two primary types: misuse-based and anomaly-based. Anomaly-based detection focuses on identifying abnormalities in network behavior, flagging any deviations from the norm as potential threats. This approach is particularly vital for recognizing zero-day attacks, where assailants exploit undiscovered vulnerabilities. Anomaly-based detection's ability to detect previously unseen threats is invaluable in the face of evolving cyber threats. It complements traditional signature-based methods, forming a robust defense against emerging attacks without relying solely on known attack patterns.

II. RELATED WORK

I. A Network Intrusion Detection System (NIDS) is essential for maintaining the security and integrity of network infrastructure by monitoring and analyzing network traffic for suspicious activities and potential threats. In recent years, machine learning techniques have been increasingly applied to enhance the capabilities of NIDS. This project aims to develop a sophisticated NIDS leveraging a combination of k-Nearest Neighbors (k-NN), AdaBoost, and Random Forest algorithms, integrated within a Flask-based web application to serve the model and provide a user-friendly interface for monitoring and managing network security

II. The k-NN algorithm, known for its simplicity and effectiveness in classification tasks, works by identifying the closest training examples to the input data point and using them to determine its class. However, k-NN can be computationally intensive, especially with large datasets. To address this, we incorporate AdaBoost, an ensemble learning technique that combines multiple weak classifiers to form a strong classifier, thereby improving the detection accuracy and robustness of the NIDS. AdaBoost adjusts the weights of misclassified instances iteratively, focusing more on difficult cases, which enhances its predictive performance.

III. Additionally, we employ the Random Forest algorithm, which constructs multiple decision trees and merges their outputs to produce a more accurate and stable prediction. Random Forest is highly effective in handling large datasets and complex decision boundaries, making it suitable for detecting various types of network intrusions.

IV. The Flask framework serves as the backbone of our web application, enabling us to create a scalable and easy-to-deploy interface for users. Through Flask, users can upload network traffic data, initiate real-time monitoring,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205291 |

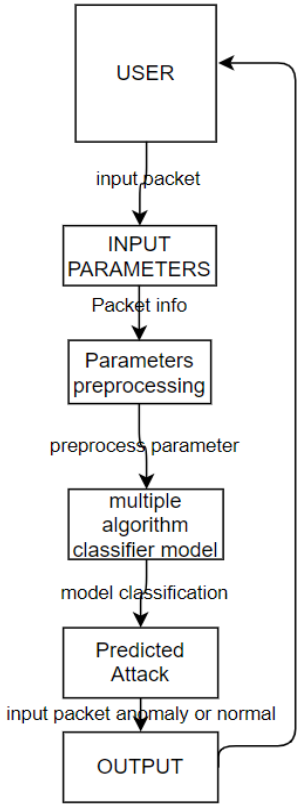
and visualize detection results. The integration of these machine learning models within a Flask application ensures that the system is both powerful and user-friendly, providing real-time insights and alerts on network intrusions.

V. This approach builds upon existing research and practices in the field of network security and machine learning, addressing the limitations of individual algorithms by combining their strengths. By utilizing k-NN for its simplicity and interpretability, AdaBoost for its boosting capabilities, and Random Forest for its robustness and accuracy, this NIDS offers a comprehensive solution for detecting and mitigating network threats efficiently.

III. METHODOLOGY

1. K-Nearest Neighbours (KNN):
KNN is a promising algorithm for Network Intrusion Detection Systems (NIDS). It classifies network traffic by comparing similarities between data points. During training, it learns from labelled instances, distinguishing between normal and anomalous behaviour.

2. Support Vector Machine (SVM):
The kernel trick allows for the discovery of complex relationships, while margin maximization enhances generalization and resilience to noise. SVMs contribute significantly to proactive threat detection and effective network security in NIDS.



3. Linear Discriminant Analysis (LDA):
LDA identifies discriminative features and constructs linear decision boundaries. It prioritizes class separability and enhances discriminatory power, contributing to proactive threat detection and effective network security in NIDS.

4. Quadratic Discriminant Analysis (QDA):
QDA constructs quadratic decision boundaries to separate normal and malicious activities. Its non-parametric nature makes it suitable for diverse network environments, contributing to enhanced network security and threat mitigation in NIDS.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205291 |

The number of machine learning algorithms including bagging and boosting are used to train the model. However the model uses NSL-KDD train and test dataset to predict the attacks. The library Pandas_profiling is used to provide an extensive overview of a DataFrame's statistics, distributions, correlations, missing values, and more. The requirements are Flask==1.1.2, gunicorn==19.9.0, scikit-learn==0.22.1, joblib==0.14.1, etc. The values are set for the attacks such as 0 for Normal, 1 for DoS, 2 for Probe, 3 for R2L, else U2R. The model takes user input values for certain specific attributes like Attack, Number of connections to the same destination host as the current connection in the past two seconds,

The percentage of connections that were to different services, among the connections aggregated in dst_host_count, The percentage of connections that were to the same source port, among the connections aggregated in dst_host_srv_count ,The percentage of connections that were to the same service, among the connections aggregated in dst_host_count ,Number of connections having the same port number, Status of the connection –Normal or Error Last Flag 1 if successfully logged in; 0 otherwise ,The percentage of connections that were to the same service, among the connections aggregated in count ,The percentage of connections that have activated the flag (4) s0, s1, s2 or s3, among the connections aggregated in count, Destination network service used http or not. On the basis of the user input values the types of attacks are predicted such as probe, DoS, U2R, R2L or otherwise normal.

The algorithm automatically generates mask image without user interaction that contains only text regions to be inpainted.

IV. EXPERIMENTAL RESULTS

Figures shows the results of Network Intrusion System Detected Attack Type Figs. 1,2,3 shows the System User Interface(UI) with along total predicted class and type of the Attack

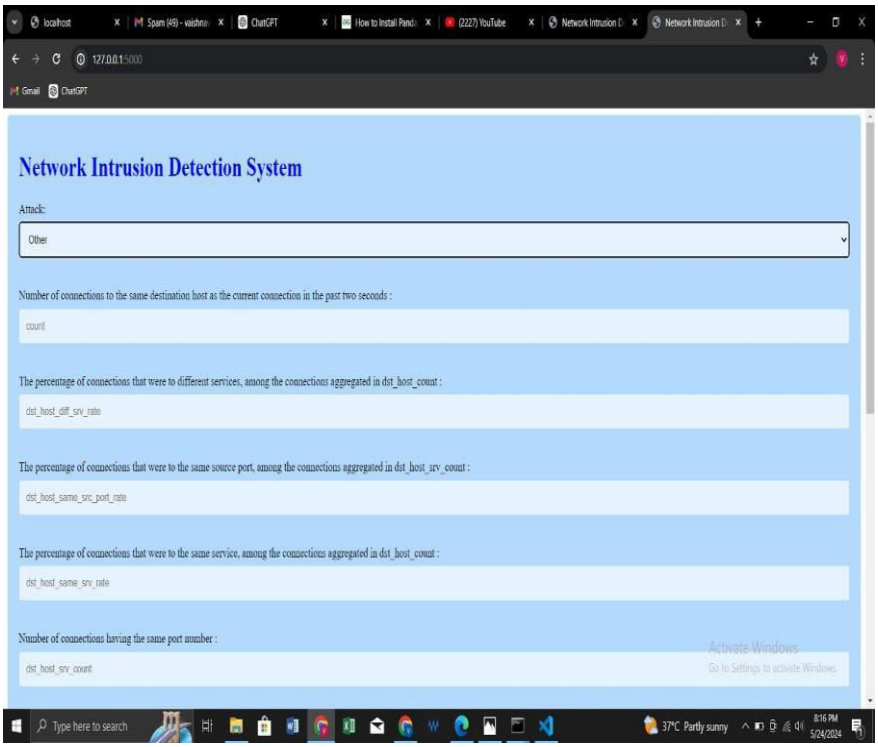


Fig.1 User Interface

Fig. 1. After successfully launch System we need to enter the Parameters of Packet to identitfy Type of Attack in System.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205291 |

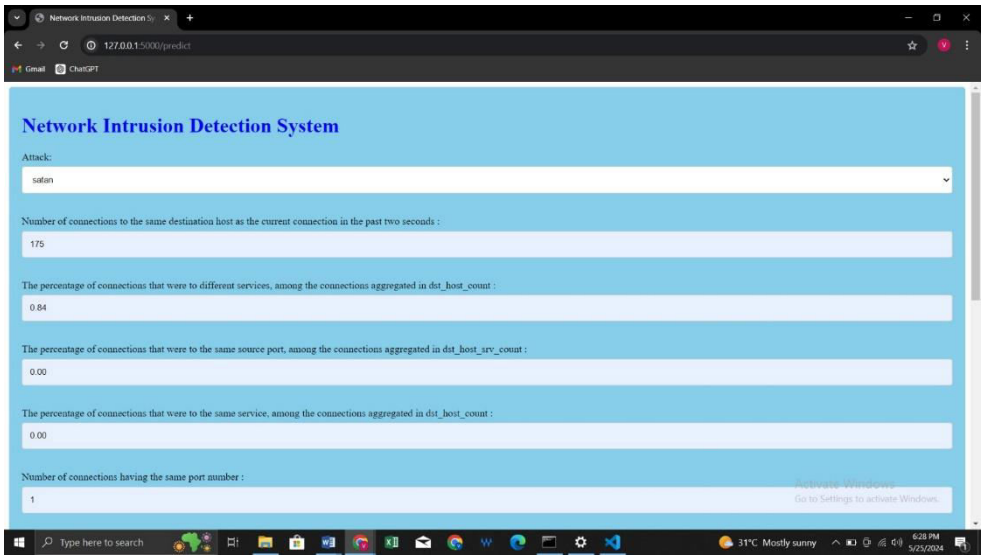


Fig. 2 After entering the Parameter we need to Check the parameter and then Enter

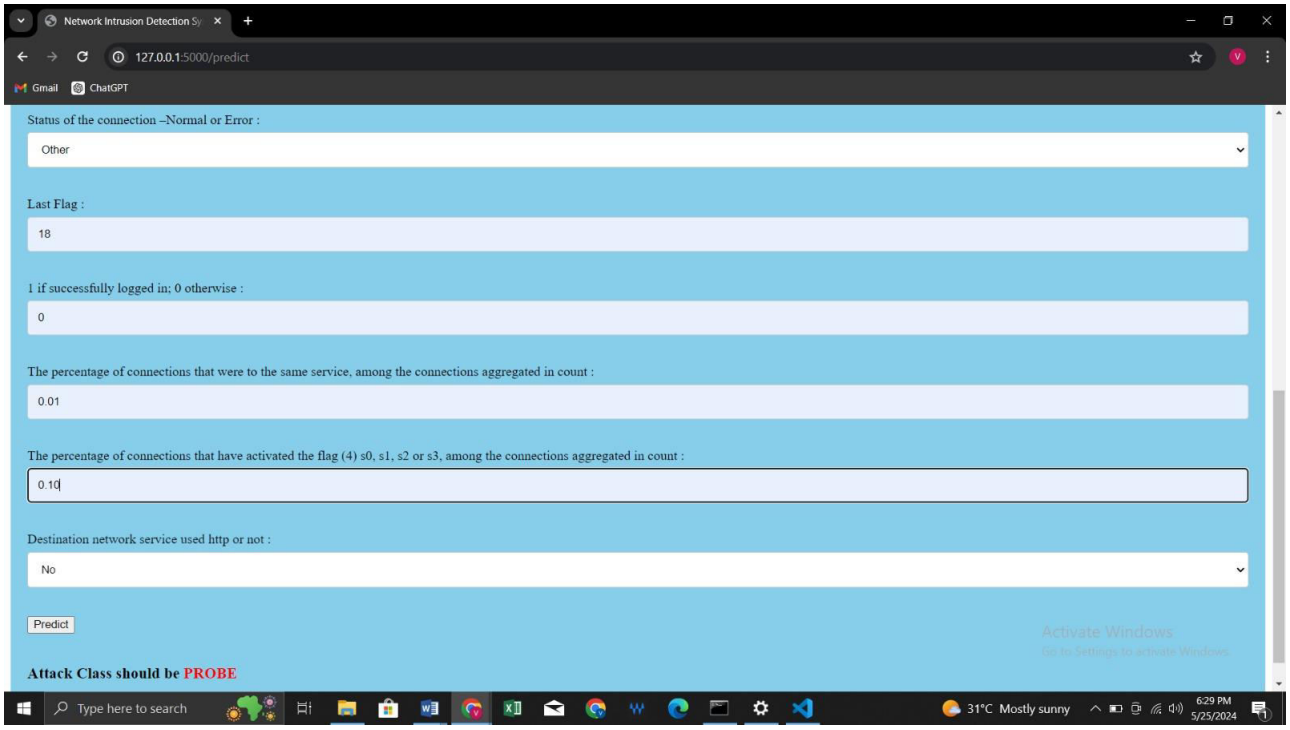


Fig. 4 As we see our model predicted based on the given parameter. Attack should be probe.

V. CONCLUSION

In this research paper, a new Network Intrusion Detection System (NIDS) based on an ensemble learning framework is introduced, focusing on real-time identification of network traffic from instantaneous flows. The system includes a bi-phase algorithm that initially screens network packets quickly and then performs a detailed analysis of identified malicious traffic.The effectiveness of the selected features is evaluated using key metrics: accuracy, precision, recall, and F1-score.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205291 |

The study confirms the superior performance of the bi-phase algorithm in terms of accuracy compared to existing methods, while also achieving an efficient balance between detection time and rate. Real-time implementation on a test-bed demonstrates the feasibility and effectiveness of the proposed technique in accurately classifying network packets.

The proposed model could also be extended to create a dynamic framework for cybersecurity, enhancing capabilities through integration with unsupervised approaches.

REFERENCES

[1] Ratul Chowdhury, Shibaprasad Sen, Arpan Goswami, Shankhadeep Purkait, Banani Saha, An implementation of bi-phase network intrusion detection system by using real-time traffic analysis, Expert Systems with Applications, Volume 224, 2023, 119831, ISSN 0957-4174

[2] Md. Alamin Talukder, Khondokar Fida Hasan, Md. Manowarul Islam, Md. Ashraf Uddin, Arnisha Akhter, Mohammand Abu Yousuf, Fares Alharbi, Mohammad Ali Moni, A dependable hybrid machine learning model for network intrusion detection, Journal of Information Security and Applications, Volume 72, 2023, 103405, ISSN 2214-2126

[3] Pengzhou Cheng, Mu Han, Gongshen Liu, DESC-IDS: Towards an efficient real-time automotive intrusion detection system based on deep evolving stream clustering, Future Generation Computer Systems, Volume 140, 2023, Pages 266-281, ISSN 0167-739XYassin M. Y. Hasan and Lina J. Karam, "Morphological Text Extraction from Images", IEEE Transactions On Image Processing, vol. 9, No. 11, 2000

[4] Joseph R. Rose, Matthew Swann, Konstantinos P. Grammatikakis, Ioannis Koufos, Gueltoum Bendiab, Stavros Shiaeles, Nicholas Kolokotronis, "IDERES: Intrusion detection and response system using machine learning and attack graphs," Journal of Systems Architecture, Volume 131, 2022, 102722, ISSN 1383-7621

[5] S.Bhuvaneswari, T.S.Subashini, "Automatic Detection and Inpainting of Text Images", International Journal of Computer Applications (0975 – 8887) Volume 61– No.7, 2013

[6] L. Gupta and S. Ma, ``Gesture-based interaction and communication: Automated classification of hand gesture contours," \textit{IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)}, vol. 31, no. 1, pp. 114-120, 2001.

[7] S. Mitra and T. Acharya, ``Gesture recognition: A survey," \textit{IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)}, vol. 37, no. 3, 2007.Uday Modha, Preeti Dave, " Image Inpainting-Automatic Detection and Removal of Text From Images", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue 2, 2012

K. M. Lim, A. W. C. Tan, and S. C. Tan, ``Block-based histogram of optical flow for isolated network intrusion detection system," \textit{Journal of Visual Communication and Image Representation}, vol. 40, pp. 538-545, 2016

[8] Pengzhou Cheng, Mu Han, Gongshen Liu, DESC-IDS: Towards an efficient realtime automotive intrusion detection system based on deep evolving stream clustering, Future Generation Computer Systems, Volume 140, 2023, Pages 266-281, ISSN

0167-739X, https://doi.org/10.1016/j.future.2022.10.020 .

[9] Pengzhou Cheng, Mu Han, Gongshen Liu, DESC-IDS: Towards an efficient realtime automotive intrusion detection system based on deep evolving stream clustering, Future Generation Computer Systems, Volume 140, 2023, Pages 266-281, ISSN

0167-739X, https://doi.org/10.1016/j.future.2022.10.020

[10] Monika Vishwakarma, Nishtha Kesswani, DIDS: A Deep Neural Network basedrealtime Intrusion detection system for IoT, Decision Analytics Journal, Volume5, 2022,

100142, ISSN 2772-6622, https://doi.org/10.1016/j.dajour.2022.100142.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details