iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69370

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Network Intrusion Detection System Using Artificial Intelligence

Dr. L. Malathi[1], Ms. Gayathri B[2]
[1]*Associate Professor, ECE, Sri Ramakrishna Institute of Technology, Coimbatore – 641010*
[2]*Student, ECE, Sri Ramakrishna Institute of Technology, Coimbatore – 641010*

Abstract: ***This paper focuses on the development of an Advanced Network Intrusion Detection System (ANIDS) that leverages a combination of Machine Learning Algorithms, including Recurrent Neural Networks (RNN), K- Nearest Neighbours (KNN), CatBoost and AdaBoost to enhance the accuracy and efficiency of Intrusion Detection over Wireless Network. By Employing the fusion approach, the system aims to capitalize on the strengths of each algorithm to improve overall performance in identifying malicious activities and potential threats within Network Traffic. This paper utilizes scalar encoding for effective feature representation and applies Synthetic Minority Over Sampling Technique (SMOTE) to address class imbalance in the dataset, ensuring a more robust and fairer training process. Through a comprehensive training code and processing test code, the system is designed to accurately classify normal and abnormal network behaviour, significantly reducing false positives and improving detection rates. This Innovative approach not only enhances the security of network infrastructures but also provides a scalable solution for real time monitoring and response to cybersecurity threats, thereby contributing to safer digital environments.***
Keywords: RNN, KNN, SMOTE, Python, AI, Network Intrusion

I. INTRODUCTION

In today's digital era, the increasing reliance on networks and connected devices has made cybersecurity a critical concern. With the rise in cyber threats and malicious attacks targeting network infrastructures, there is a growing need for efficient and accurate intrusion detection systems to safeguard sensitive data and ensure the integrity of communications. Traditional methods of intrusion detection often struggle with issues like false positive rates and imbalanced datasets, which hinder their ability to effectively identify and prevent attacks in real time. To address these challenges, this paper introduces an advanced network intrusion detection system that integrates multiple machine learning algorithms—RNN, KNN, CatBoost, and AdaBoost—fused together to optimize performance. By combining these algorithms, the system is designed to capture diverse patterns of normal and malicious behaviour, leading to more accurate and timely detection of intrusions. Furthermore, the paper employs scalar encoding for feature preprocessing and the Synthetic Minority Oversampling Technique (SMOTE) to balance the dataset, ensuring the model is capable of handling the complexities of network traffic data. This comprehensive approach aims to enhance both the detection accuracy and overall security of network infrastructures, offering a robust solution to modern cybersecurity challenges.

II. NETWORK INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems (IDS) play a critical role in securing network environments by identifying unauthorized or malicious activities. With the rapid growth of cyber threats, traditional detection methods often fall short of adapting to new attack patterns. As network traffic becomes more complex, IDS must evolve to detect anomalies and attacks accurately and efficiently. Machine learning techniques have gained prominence in this space, providing advanced capabilities for recognizing patterns and predicting potential security breaches. Machine learning algorithms offer robust solutions to the challenges of intrusion detection by learning from historical data and predicting threats in real-time. However, a single machine learning model may not be sufficient to handle the wide variety of network intrusions that can occur. By leveraging multiple algorithms—such as Recurrent Neural Networks (RNN), K-Nearest Neighbours (KNN), CatBoost, and AdaBoost—this paper aims to create a more reliable and accurate detection system. Each algorithm brings unique strengths, allowing for a comprehensive and multi-faceted approach to threat detection.

Combining multiple machine learning algorithms is essential to enhancing the overall accuracy and resilience of the intrusion detection system. RNNs, for instance, are well-suited for identifying patterns over time, which is critical for detecting attacks that unfold over a sequence of events. KNN offers a straightforward approach for classifying data points based on similarity, making it useful for distinguishing normal network behaviour from anomalies. CatBoost and AdaBoost, as boosting algorithms, help in improving the prediction power of weaker models, leading to higher detection rates.

One of the significant challenges in intrusion detection is the imbalanced nature of the dataset, where the majority of the network traffic is benign and only a small portion constitutes malicious activity. To address this imbalance, the synthetic minority oversampling technique (SMOTE) is used to balance the dataset, ensuring that the model does not favor normal traffic over potential threats. Additionally, data preprocessing techniques such as scaling and encoding are implemented to standardize the inputs, enhancing the overall performance of the system.

This paper's approach aims to create a more intelligent and adaptive intrusion detection system capable of responding to a wide range of network threats. By fusing the strengths of different algorithms and employing techniques like SMOTE to balance the data, the system can detect intrusions with higher precision and lower false-positive rates. Ultimately, this leads to a more secure and resilient network infrastructure, where potential threats are identified and mitigated in real-time. Intrusion detection faces challenges due to imbalanced datasets, where most traffic is benign and only a small portion is malicious. To address this, the Synthetic Minority Oversampling Technique (SMOTE) is used to balance the dataset, preventing bias towards normal traffic. Data preprocessing methods like scaling and encoding standardize inputs, enhancing model performance.

The proposed approach develops an intelligent and adaptive intrusion detection system (IDS) that detects a wide range of threats with higher precision and fewer false positives. This is crucial as cyberattacks, including phishing, denial-of-service, malware, and zero-day exploits, are increasing. Traditional security measures like firewalls are often inadequate, making IDS essential for real-time monitoring and threat detection.

Developing an effective IDS for large-scale networks involves challenges such as handling unstructured, noisy data, managing high traffic volumes without excessive false positives, and adapting to sophisticated attacker methods. The system employs multiple machine learning algorithms: RNN for recognizing sequential patterns, KNN for classifying traffic based on historical data, and boosting algorithms like CatBoost and AdaBoost to enhance weak classifiers. This fusion results in a robust detection system capable of identifying both known and novel threats.

The system prioritizes real-time detection with optimized processing to minimize latency, ensuring immediate threat identification. It is designed to scale across different network environments, from small corporate networks to large cloud infrastructures, and adapts over time by learning from new data, maintaining effectiveness against evolving cyber threats.

III. PROBLEM STATEMENT

Despite the significance of intrusion discovery, several challenges hamper its effectiveness, especially in ultramodern network surroundings characterized by big data and imbalanced datasets. The traditional intrusion discovery styles, which are rule- grounded or hand- grounded, frequently struggle to keep pace with the fleetly evolving tactics employed by cybercriminals. These styles heavily calculate on predefined patterns or autographs of known attacks and are limited in their capability to descry preliminary unseen or zero-day attacks. Also, imbalanced datasets pose a significant problem in intrusion discovery. In numerous real-world scripts, benign network business far outweighs vicious business. As a result, intrusion discovery models trained on imbalanced datasets tend to prioritize the maturity class (normal business) and underperform in relating the nonage class (virtual business). This bias towards the maturity class can lead to false negatives, where factual intrusions go undetected, posing a serious security threat.

IV. SEVERAL COMPELLING FACTORS

The necessity for an advanced and adaptive intrusion discovery system like ML-NIDS is driven by several compelling factors

Evolving trouble Landscape The nature of network intrusions is continually evolving, with cybercriminals employing sophisticated ways to circumvent traditional discovery mechanisms. is designed to address arising pitfalls effectively by using advanced machine literacy methods.

Big Data surroundings in the age of big data, network business data has grown exponentially, making it decreasingly gruelling to reuse and assay for implicit security pitfalls. ML-NIDS is acclimatized to handle vast volumes of data efficiently, ensuring that no pitfalls go unnoticed.

Imbalanced Datasets Imbalanced datasets are a common issue in intrusion discovery, and they hamper the accurate identification of vicious business. employs ways similar as Synthetic nonage oversampling fashion (SMOTE) and Tomek-Links under slice to address the problem of imbalanced datasets. This ensures balanced representation of both normal and vicious business, reducing false negatives.

Real-time Detection Network intrusions can have severe consequences, and rapid-fire discovery is pivotal for effective response. ML-NIDS is designed to give real-time intrusion discovery, minimizing the time between trouble identification and response.

V. LITERATURE SURVEY

Title: Machine Learning Based Intrusion Detection System
Authors: Anish Halimaa A., K. Sundarakantham
Publication: 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)
Intrusion Detection Systems (IDS) monitor networks or systems for malicious activity. With increasing computer connectivity, IDS is crucial for network security. Various machine learning and statistical methods are used to enhance IDS performance. Accuracy is key to reducing false alarms and increasing detection rates. The proposed approach addresses the challenge of analyzing large network traffic data. It applies machine learning techniques like Support Vector Machine (SVM) and Naive Bayes, known for solving classification problems. The NSL-KDD dataset is used for evaluation. Results show SVM outperforms Naive Bayes in accuracy. A comparative analysis calculates the accuracy and misclassification rates of both methods.

Title: Network Intrusion Detection
Authors: B. Mukherjee, L.T. Heberlein, K.N. Levitt
Publication: IEEE Network
Intrusion detection is a method to enhance security in existing computer systems and networks while maintaining their open operational mode. Its goal is to identify unauthorized use, misuse, and abuse by both insiders and external attackers. The growing complexity of computer networks makes intrusion detection more challenging, as increased connectivity facilitates intruder access and evasion. Intrusion Detection Systems (IDSs) operate on the premise that intruder behavior differs from legitimate users and that many unauthorized actions are detectable. IDSs typically use statistical anomaly and rule-based misuse models to detect intrusions. Various prototypes have been developed and experimentally deployed. The paper surveys both host-based and network-based IDSs. Host-based systems rely on audit trails from the host operating system, while network-based systems primarily monitor network traffic, sometimes using host audit trails as well.

Title: Intrusion Detection System using Machine Learning Techniques: A Review
Authors: Usman Shuaibu Musa, Megha Chhabra, Aniso Ali, Mandeep Kaur
Publication: 2020 International Conference on Smart Electronics and Communication (ICOSEC)
The growing use of computer networks brings challenges in maintaining network availability, integrity, and confidentiality. Intrusion Detection Systems (IDS) help monitor network traffic for unauthorized and malicious activities. Intrusion refers to the breach of security policies with malicious intent, and IDS aim to detect such activities and alert administrators.
There are two main types of detection: misuse or signature-based detection, which compares traffic against known attack signatures, and anomaly detection, which identifies deviations from normal behavior. The paper reviews various efforts to build efficient IDS using single, hybrid, and ensemble machine learning classifiers. It evaluates these systems using seven different datasets, discussing and comparing results to provide guidance for future research.

Title: Intrusion Detection: A Survey
Authors: F. Sabahi, A. Movaghar
Publication: 2008 Third International Conference on Systems and Networks Communications
The rapid expansion of computer networks has significantly impacted network security, making them vulnerable to various threats from hackers. Numerous and potentially devastating threats necessitate robust Intrusion Detection Systems (IDS) capable of identifying attacks in diverse environments. Various methods for misuse and anomaly detection have been developed, with different approaches performing better in specific environments.
This paper presents a taxonomy of IDS, classifying them based on their detection principles and operational aspects. The taxonomy is used to survey and categorize existing IDS, highlighting complementary technologies suited for different environments.

Title: Intrusion detection and prevention system: Challenges & opportunities
Authors: Uzair Bashir, Manzoor Chachoo
Publication: 2014 International Conference on Computing for Sustainable Global Development (InaCom)
The push for universal and readily available network access has revolutionized the field, yet preventing resource theft and attacks remains a challenge. This issue is critical for industries, companies, and national security as they face increasing threats like viruses and intrusions. Despite various intrusion detection and prevention systems (IDPS) deployed by organizations, many security breaches still go undetected.

This paper surveys common security breaches and explores the opportunities and challenges in the field of IDPS. It reviews the progress in intrusion detection systems, examining existing types, techniques, and architectures. The paper also outlines current research challenges and issues in enhancing IDPS effectiveness.

Title: A Review on Intrusion Detection System using Machine Learning Techniques
Authors: Usman Shuaibu Musa, Sudeshna Chakraborty, Muhammad M. Abdullahi, Tarun Maini
Publication: 2021 International Conference on Computing Communication and Intelligent Systems (ICCCIS)
Computer networks are increasingly vulnerable to cyber-attacks due to widespread internet usage. Intrusion Detection Systems (IDSs) have been developed to identify unauthorized access and attacks, ensuring network security. Various methods, including machine learning, Bayesian algorithms, meta-heuristic techniques, swarm algorithms, and Markov neural networks, have been proposed to improve IDS efficiency by identifying key features.
This paper reviews numerous research articles employing single, hybrid, and ensemble classification algorithms. It compares result metrics, shortcomings, and datasets used in IDS development. The paper also highlights future research directions for further improvement in IDS.

Title: Intelligent Intrusion Detection System Using Clustered Self-Organized Map
Authors: Muder Almi'ani, Alia Abu Ghazleh, Amer Al-Rahayfeh, Abdul Razaque
Publication: 2018 Fifth International Conference on Software Defined Systems (SDS)
The growing complexity and frequency of information security breaches demand highly flexible and accurate protection methods. Intrusion Detection Systems (IDS) play a crucial role in detecting threats before they impact network systems. Artificial neural networks have been effective in meeting the high accuracy requirements of IDS.
This paper presents an intelligent IDS using a clustered Self-Organized Map (SOM) network. The system has two stages: first, building the SOM network, followed by hierarchical agglomerative clustering using k-means on SOM neurons. The proposed system addresses sensitivity and time consumption issues, achieving 96.66% sensitivity with processing time of less than 0.08 milliseconds per connection record, demonstrated using the NSL-KDD benchmark dataset.

Title: Intrusion Detection System Using Machine Learning
Authors: Ajmeera Kiran, S. Wilson Prakash, B. Anand Kumar, Likhitha, Tammana Sameeratmaja, Ungarala Satya Surya Ram Charan
Publication: 2023 International Conference on Computer Communication and Informatics (ICCCI)
The rapid growth of internet usage has made information security increasingly critical. Designing a robust Intrusion Detection System (IDS) is essential to prevent unauthorized access by hackers and intruders. IDS monitors network or system activities for unethical behavior or policy violations and reports to a Management Station.
This study proposes using machine learning as a framework for developing a network IDS. The system detects intrusions by identifying deviations between expected and observed patterns. Experimental results show that the proposed machine learning approach enhances the effectiveness of intrusion detection.
Title: Using Deep Learning Techniques for Network Intrusion Detection
Authors: Sara Al-Emadi, Aisha Al-Mohannadi, Felwa Al-Senaid,
Publication: 2020 IEEE International Conference on Informatics IoT and Enabling Technologies (ICIoT)

Title: A survey of intrusion detection system
Authors: Loubna Dali, Ahmed Bentajer, Elmoutaoukkil Abdelmajid, Karim Abouelmehdi,Hoda Elsayed, Eladnani Fatiha, Benihssane Abderahim,
Publication: 2015 2nd World Symposium on Web Applications and Networking (WSWAN)
In this paper, we presented a survey on intrusion detection systems (IDS). First, we referred to different mechanisms of intrusion detection. Furthermore, we detailed the types of IDS. We have focused on the application IDS, specifically on the IDS Network, and the IDS in the cloud computing environment. Finally, the contribution of every single type of IDS is described.

VI. EXISTING WORK SYSTEM

In the existing intrusion detection systems (IDS), traditional methods primarily rely on rule-based or signature-based approaches, which are effective at identifying known threats but fail to detect novel or evolving attacks. These systems often depend on predefined patterns of known intrusions, making them less adaptable to new forms of cyber threats, such as zero-day attacks. Furthermore, most existing IDS solutions struggle with high false-positive rates, leading to inefficient use of resources and alert fatigue among security teams. Additionally, current systems may not effectively handle the large volumes of network traffic generated in modern infrastructures, resulting in delayed threat detection and inadequate response times. The limitations of scalability, adaptability, and accuracy in recognizing newer or more sophisticated attacks necessitate the development of more advanced and flexible detection mechanisms.

VII. PROPOSED WORK SYSTEM

The proposed system addresses the shortcomings of traditional IDS by integrating advanced machine learning algorithms, such as RNN, KNN, CatBoost, and AdaBoost, to create a more robust and adaptive intrusion detection system. By leveraging a hybrid approach that fuses these algorithms, the system can detect both known and previously unseen network intrusions with greater accuracy. Preprocessing techniques like scalar encoding and SMOTE are employed to normalize the data and balance the dataset, improving the system's performance on imbalanced data typical in network traffic. RNN is utilized for time-series analysis, identifying patterns over time, while KNN, CatBoost, and AdaBoost provide spatial pattern recognition and ensemble learning that enhance detection precision and reduce false positives. The proposed system is designed to handle large-scale, real-time data streams, making it scalable and capable of adapting to evolving cyber threats. This approach ensures a higher detection rate, faster response, and better overall network security.

VIII. METHODOLOGY

The proposed intrusion detection system utilizes a hybrid approach, combining multiple machine learning algorithms such as RNN, KNN, CatBoost, and AdaBoost to enhance detection accuracy and performance. The system begins with data processing, where raw network traffic data is cleaned and encoded using scalar encoding to ensure uniformity. To address the challenge of imbalanced data typically found in intrusion datasets, SMOTE (Synthetic Minority Oversampling Technique) is applied to balance the dataset, improving the model's ability to detect minority class intrusions. The system then applies RNN (recurrent neural network) for sequential analysis of time-dependent patterns in network traffic, identifying anomalies that develop over time. KNN (K-Nearest Neighbors) is used for spatial pattern recognition, while CatBoost and AdaBoost serve as ensemble learning models to enhance classification performance by combining predictions from multiple algorithms. The fusion of these models is achieved through a train-test split, where the hybrid system is trained on a portion of the dataset and tested on the remaining data to ensure high accuracy in real-time intrusion detection. This approach enables the system to detect both known and emerging threats with low false-positive rates, offering a more robust and scalable solution for network security.

IX. WORKING MECHANISM OF ML ALGORITHMS

The intrusion detection system leverages the power of multiple machine learning algorithms, each contributing uniquely to the detection process. The system begins with data preprocessing, where the network traffic data is first encoded using scalar encoding techniques. This step ensures that all input features, such as packet size, duration, and source/destination IP addresses, are normalized for consistent input across all algorithms. Additionally, SMOTE (Synthetic Minority Oversampling Technique) is applied to balance the dataset, addressing the issue of class imbalance by oversampling the minority class, thereby improving the system’s ability to detect rare intrusion events like network attacks.

X. TYPES OF ML ALGORITHMS FOR NETWORK DETECTION

A. RNN (Recurrent Neural Network)

The RNN is central to the system's detection of time-sequential patterns within the network traffic data. Since RNNs are capable of processing data over time, they are used to detect abnormal behaviours that evolve gradually, such as Distributed Denial of Service (DDoS) attacks or slow data leaks. The RNN processes sequences of network data, utilizing its internal memory to understand long-term dependencies between events. This allows the system to identify subtle patterns that are spread over time, improving the detection of sophisticated, time-sensitive intrusions.

B. KNN (K-Nearest Neighbours)

KNN, a non-parametric algorithm, is applied to complement the RNN by focusing on spatial pattern recognition. It works by comparing new data points to the nearest neighbors in the feature space, determining whether a given network event is classified as normal or an intrusion based on the proximity of known attack patterns. KNN is particularly effective in detecting outliers and anomalies, such as sudden spikes in network activity, which may indicate an attack. Its simplicity and effectiveness in pattern recognition make it a strong component in the system's hybrid approach.

C. CatBoost

CatBoost, a gradient boosting algorithm, enhances the system by efficiently handling categorical data without requiring extensive preprocessing. It works by iteratively building decision trees that learn from previous model errors, making it particularly useful for capturing complex relationships between different network features. CatBoost also helps in reducing overfitting and bias in the model by using its gradient-based structure, ensuring the system can generalize better across different types of network traffic.

D. AdaBoost

AdaBoost adds an additional layer of accuracy to the system. It focuses on combining weak classifiers to create a strong classifier by assigning more weight to misclassified instances in each iteration. This ensemble approach helps the system adapt to misclassified network intrusions in the training data, refining its ability to distinguish between normal network activity and various types of attacks. By boosting weak learners, AdaBoost contributes to a more balanced and robust model that can handle both common and sophisticated intrusions effectively.

E. Fusion of Algorithms

The strength of the system lies in the fusion of these diverse algorithms. After training each model on the preprocessed data, the system evaluates their combined performance during the testing phase. The predictions from each model are aggregated, leveraging their individual strengths. For example, RNN excels in temporal anomaly detection, while KNN is effective for spatial outliers, and CatBoost and AdaBoost work well in refining the overall classification accuracy. This ensemble of models helps achieve a lower false positive rate and improves the system’s ability to detect a wide range of network intrusions.

By integrating these machine learning techniques, the hybrid system provides a powerful and adaptive solution to intrusion detection, offering real-time analysis and high accuracy across various types of network attacks.

XI. SOFTWARE DESCRIPTION

Python is an interpreted, high-position programming language created by Guido van Rossum and first released in 1991. It emphasizes law readability, using significant whitespace to define law blocks, which makes the language easy to understand and use. Python’s simple and elegant syntax allows it to be freshman-friendly while still furnishing important capabilities for advanced programming. It's a general-purpose language, suitable for operations similar to web development, data wisdom, artificial intelligence, robotization, and more. Python supports high-position data structures like lists, wordbooks, and sets, along with important libraries for complex data manipulation.

Python follows object-acquainted programming principles, allowing inventors to produce modular, applicable law using classes and objects. It supports heritage and system booting, which makes it easy to make on being law. Python’s dynamic typing means that the type of a variable is determined at runtime, making the law more flexible. As an interpreted language, Python executes laws line by line, which aids in debugging and provides interactive capabilities. Also, Python can integrate with other languages like C/C to enhance performance for further complex tasks.

Functions in Python are first-class objects, meaning they can be passed as arguments, returned from other functions, and assigned to variables. Python also supports lambda functions, which give a terse way to define simple, anonymous functions. With an expansive standard library and access to thousands of external libraries through PyPI, Python offers a wide range of tools for inventors. erected in modules like zilches, sys, and calculation give essential functions for tasks similar to system programming, train running, and fine operations.

Python’s class system allows for the speeding of data and functionality together. It supports heritage, making it possible to produce new classes grounded on being bones, therefore enabling law exercise. Python classes are dynamic, allowing new attributes or styles to be added indeed after the class has been defined. Python uses namespaces to collude variable names to objects and to control variable compass. The global keyword is used to modify global variables inside functions.

Python also supports the compendium of scripts into bytecode, stored in. pyc lines, for briskly lading and prosecution. By using the-O and-OO flags, Python law can be optimized by removing gratuitous debug information or docstrings, which can ameliorate performance. The Python practitioner automatically caches collected performances of modules, making posterior significances briskly.

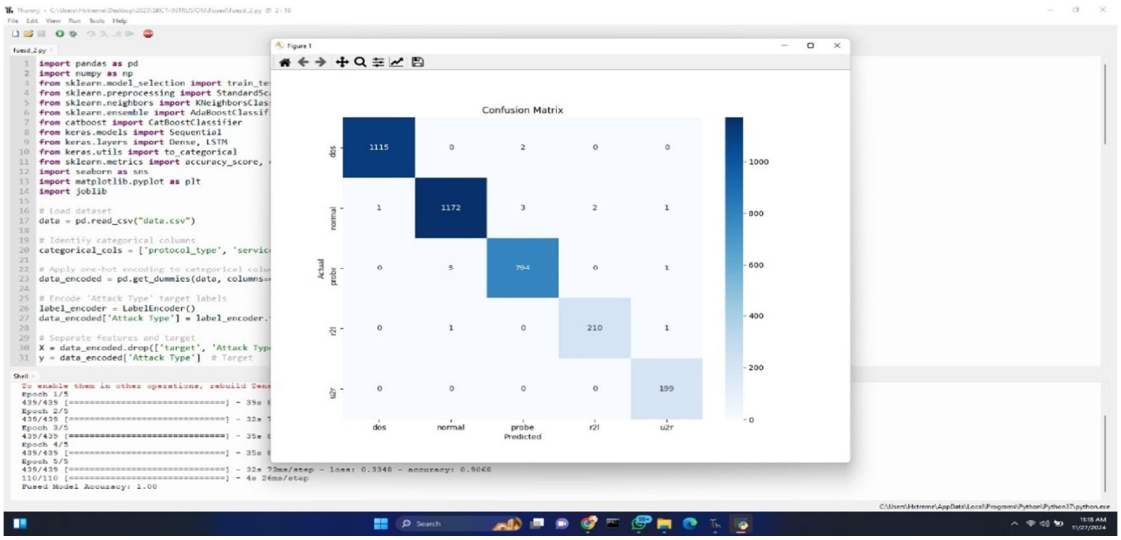
In conclusion, Python is a protean, important language ideal for rapid-fire operation development and robotization. Its combination of simplicity, readability, and robust libraries has made it a popular choice across colorful fields, from web development to machine literacy and data analysis.

A. Thonny IDE

Thonny is a lightweight, small Integrated Development Environment (IDE) designed for simplicity and speed. It requires minimal dependencies and is independent of specific desktop environments like KDE or GNOME. It primarily relies on the GTK2 toolkit and requires GTK2 runtime libraries to run. Thonny can be compiled using a simple process involving commands like. /Configure, Make, and Make install. It has been successfully tested on various Linux distributions and FreeBSD, as well as on Microsoft Windows. Thonny automatically loads files from the previous session on startup, and users can control the number of recent files stored. The IDE allows multiple instances but ensures that only the first one loads previous session files. It includes a terminal widget, provided by the libvte.so library, which can be disabled if necessary. This terminal supports basic clipboard functionality and behaves like a regular terminal. Thonny's project settings allow users to configure Make and Run commands to work within the current project, overriding default settings. The terminal path can be configured to use any Bourne-compatible shell, and users can run their scripts directly in the terminal window. Basic printing support is available, but printed files lack syntax highlighting. Thonny is a versatile IDE for Python development, offering a clean and straightforward interface for beginners and advanced users alike.

XII. RESULT ANALYSIS

The training module for given project has been compiled and using these Operations we make Artificial intelligence to study about the date interruption and type of Intrusion occurred using machine learning algorithms. The Partial Output has been shown below.



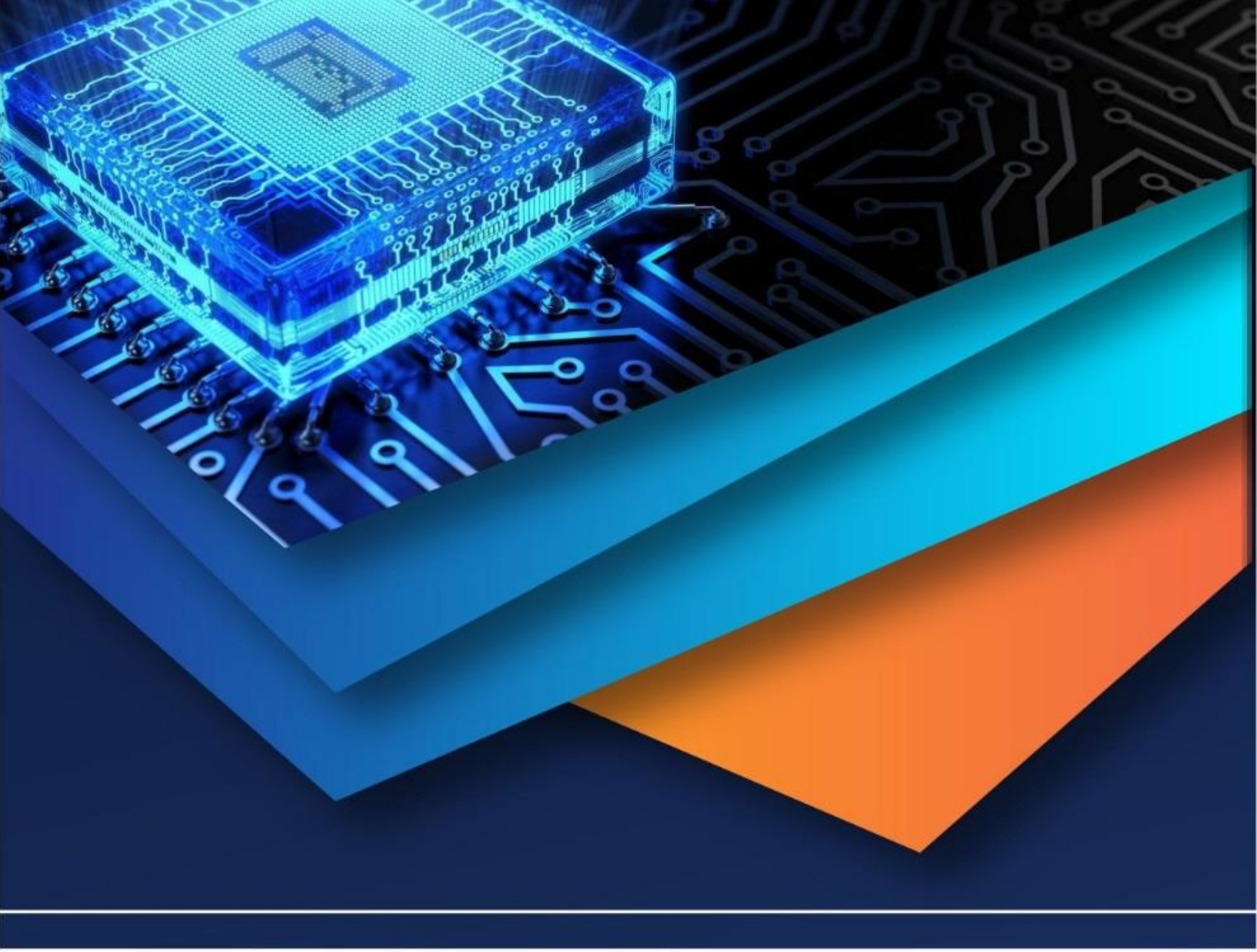
XIII. CONCLUSION AND FUTURE WORK

The intrusion discovery system developed in this design offers a robust,multi-faceted approach to relating and mollifying network pitfalls. By integrating intermittent Neural Networks (RNN), K- Nearest Neighbors (KNN), CatBoost, and AdaBoost into a single frame, the system combines the strengths of temporal pattern recognition, spatial anomaly discovery, and ensemble literacy. This mongrel system not only improves discovery delicacy but also minimizes false cons, icing dependable network security. The use of scalar encoding and SMOTE for data preprocessing enhances the model's capability to handle imbalanced datasets, making it more effective in relating rare but critical attacks. With this comprehensive approach, the design provides a scalable and adaptive result for real- time network intrusion discovery, perfecting overall security and adaptability in ultramodern network surroundings.

The stoner with little training can get the needed report. The software executes successfully by fulfilling the objects of the design. farther extensions to this system can be made required with minor variations.

REFERENCES

[1] Anish Halimaa A.,K. Sundarakantham,"Machine Learning Based Intrusion Detection System",2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)
[2] B. Mukherjee,L.T. Heberlein,K.N. Levitt,"Network intrusion detection",IEEE Network
[3] Usman Shuaibu Musa,Megha Chhabra,Aniso Ali,Mandeep Kaur,"Intrusion Detection System using Machine Learning Techniques: A Review",2020 International Conference on Smart Electronics and Communication (ICOSEC)
[4] F. Sabahi,A. Movaghar,"Intrusion Detection: A Survey",2008 Third International Conference on Systems and Networks Communications
[5] Uzair Bashir,Manzoor Chachoo,"Intrusion detection and prevention system: Challenges & opportunities",2014 International Conference on Computing for Sustainable Global Development (INDIACom)
[6] Usman Shuaibu Musa, Sudeshna Chakraborty,Muhammad M. Abdullahi,Tarun Maini,"A Review on Intrusion Detection System using Machine Learning Techniques",2021 International Conference on Computing Communication and Intelligent Systems (ICCCIS)
[7] Muder Almi'ani,Alia Abu Ghazleh,Amer Al-Rahayfeh,Abdul Razaque,"Intelligent intrusion detection system using clustered self-organized map",2018 Fifth International Conference on Software Defined Systems (SDS)
[8] Ajmeera Kiran,S. Wilson Prakash,B Anand Kumar,Likhitha,Tammana Sameeratmaja,Ungarala Satya Surya Ram Charan,"Intrusion Detection System Using Machine Learning",2023 International Conference on Computer Communication and Informatics (ICCCI)
[9] Sara Al-Emadi,Aisha Al-Mohannadi,Felwa Al-Senaid,"Using Deep Learning Techniques for Network Intrusion Detection",2020 IEEE International Conference on Informatics IoT and Enabling Technologies (ICIoT)
[10] Loubna Dali, Ahmed Bentajer, Elmoutaoukkil Abdelmajid,Karim Abouelmehdi,Hoda Elsayed,Eladnani Fatiha,Benihssane Abderahim,"A survey of intrusion detection system",2015 2nd World Symposium on Web Applications and Networking (WSWAN)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY