iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.60667

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 12 Issue V May 2024- Available at www.ijraset.com

Secure Your Network: Building a Hybrid Intrusion Detection System in Java

Avneet Kaur[1], Shruti Pawar[2], Neha Jore[3], Varsha Chavan[4], Nikita Mule[5]
[1]*Professor,* [2, 3, 4, 5]*Student, Department of Computer Engineering, Dhole Patil College of Engineering, Pune- 412207, India*

Abstract: ***To protect the system from different types of intrusions, an intrusion detection system ID is required. It is essential to analyse the communication in order to classify the material as malicious or helpful. The usage of intrusion detection systems for cyber security shouldn't add to the processing time required for classification. These days, classification algorithms are utilized in conjunction with machine learning approaches to identify harmful data or intrusions. KDD cup 99 is the data set that was used in the experiment. Hybrid classification models can be used to adjust the performance of individual classification methods. This model blends rule-based algorithms with categorization techniques. An additional degree of security is provided by the combination of machine and human intelligence in classification. Precision, recall, F-Measure, and Mean Age Precision are used to validate an algorithm. The algorithm has a 92.35 percent accuracy rate. Even after merging our human-written criteria with traditional machine learning classification techniques, the model's accuracy is still considered satisfactory. However, there is still room for improvement and a more specific classification of the attack***
Keywords: Intrusion Detection, Java , Peer to Peer.

I. INTRODUCTION

Software or hardware devices known as intrusion detection systems (IDS) automate the process of tracking and evaluating network events in order to identify potentially harmful activities. Intrusion detection systems have become an essential component of most organizations' security infrastructures due to the sharp rise in the severity of network attacks. Organizations can safeguard their systems against threats posed by growing network connectivity and information system dependence by utilizing intrusion detection. The dilemma for security professionals should not be whether to utilize intrusion detection, but rather which intrusion detection features and capabilities can be deployed, given the scope and nature of contemporary network security threats.

System access by attackers is the root cause of intrusions. Authorized users of the systems who attempt to get additional rights for which they are not authorized, Authorized users who misuse the privileges entrusted to them. Numerous algorithms have been created to detect various kinds of network intrusions, but there isn't a heuristic to validate the precision of their findings. It is impossible to report the precise efficacy of a network intrusion detection system's capacity to locate malicious sources without a clear performance evaluation.

II. PROBLEM STATEMENT

Design and implement an effective Intrusion Detection System (IDS) to protect a network or system from unauthorized access, malicious activities, and potential security threats. The IDS should be capable of detecting and responding to various types of intrusions and anomalies, ensuring the confidentiality, integrity, and availability of the network or system

III. LITERATURE REVIEW

Title :User behaviour Pattern -Signature based Intrusion Detection

Author : Zakiyabanu S. Malek, Bhushan Trivedi, Axita Shah

Description :Technology advancement also increases the risk of a security. As we can have various mechanisms to ensure safety but still there have flaws. The main concerned area is user authentication. For authentication, various biometric applications are used but once authentication is done in the begging there was no guarantee that the computer system is used by the authentic user or not. The intrusion detection system (IDS) is a particular procedure that is used to identify intruders by analysing user behaviour in the system after the user logged in. Host-based IDS monitors user behaviour in the computer and identify user suspicious behaviour as an intrusion or normal behaviour.

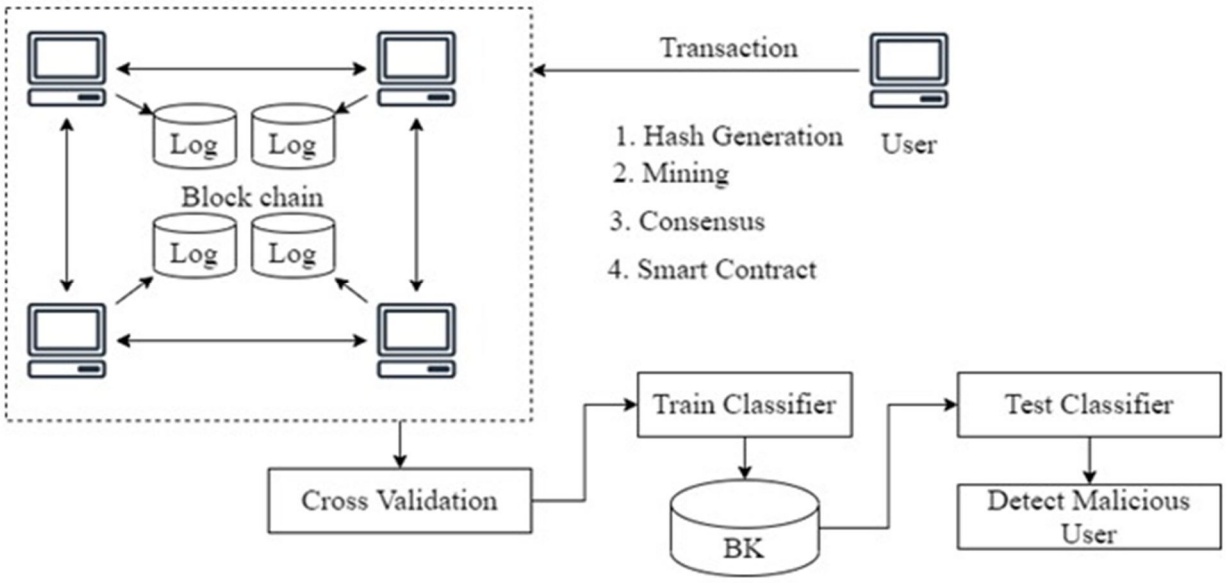
Title :A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions
Author :Osama alkadi, nour moustafa ,and benjamin turnbull
Description :This paper reviews the background and related studies in the areas of cloud systems, intrusion detection and blockchain applications against cyber-attacks. This work aims to discuss collaborative anomaly detection systems for discovering insider and outsider attacks from cloud centres, including the technologies of virtualization and containerization, along with trusting intrusion detection and cloud systems using blockchain. Moreover, the ability to detect such malicious attacks is critical for conducting necessary mitigation, at an early stage, to minimize the impact of disruption and restore cloud operations and their live migration processes.

Title :An Intrusion Detection Method for CBTC Systems Using Blockchain and LSTM
Author :Qichang Li, Junyi Zhao
Description :One of the key information security issues of CBTC systems is the data accessibility and reliability. The traditional information security methods cannot deal with data accessibility, reliability and intrusion detection problems simultaneously. In this paper, an intrusion detection method is proposed using blockchain and LSTM for CBTC systems. This method combines the advantages of distributed data sharing of blockchain, and the characteristics of high detection accuracy of LSTM neural network

IV. PROPOSED METHODOLOGY

1) *Network Security:* IDSs vigilantly monitor network traffic for suspicious activity, such as port scans, malware injections, denial-of service (DoS) attacks, and unauthorized access attempts.
2) *Host Security:* HIDSs safeguard individual systems by detecting unauthorized file changes, unusual process activity, and unauthorized access attempts.
3) *Application Security:* IDSs can detect common web attacks like SQL injection, cross site scripting (XSS), and buffer overflows.
4) *Cloud Security:* IDSs can be deployed in cloud environments to protect virtual machines, containers, and cloud storage from attacks.
5) *IoT Security:* IDSs can be deployed on IoT devices to detect attacks targeting their vulnerabilities

V. SYSTEM ARCHITECTURE



The method for an Intrusion Detection System (IDS) using Java entails continuously gathering data from network traffic and system logs. This data is then evaluated using machine learning techniques and heuristics to identify potential intrusions and anomalies. Real-time alerts are generated upon detecting suspicious activities. Blockchain technology is used to securely store security event data, ensuring unchangeable and tamper-proof records. User access controls are implemented to manage permissions for analysing and responding to incidents, while providing tools for security analysts to investigate and respond to security events using data. Compliance reports and documentation are prepared based on security incident logs to meet regulatory obligations

VI. LANGUAGES

A. *Hash Generation*

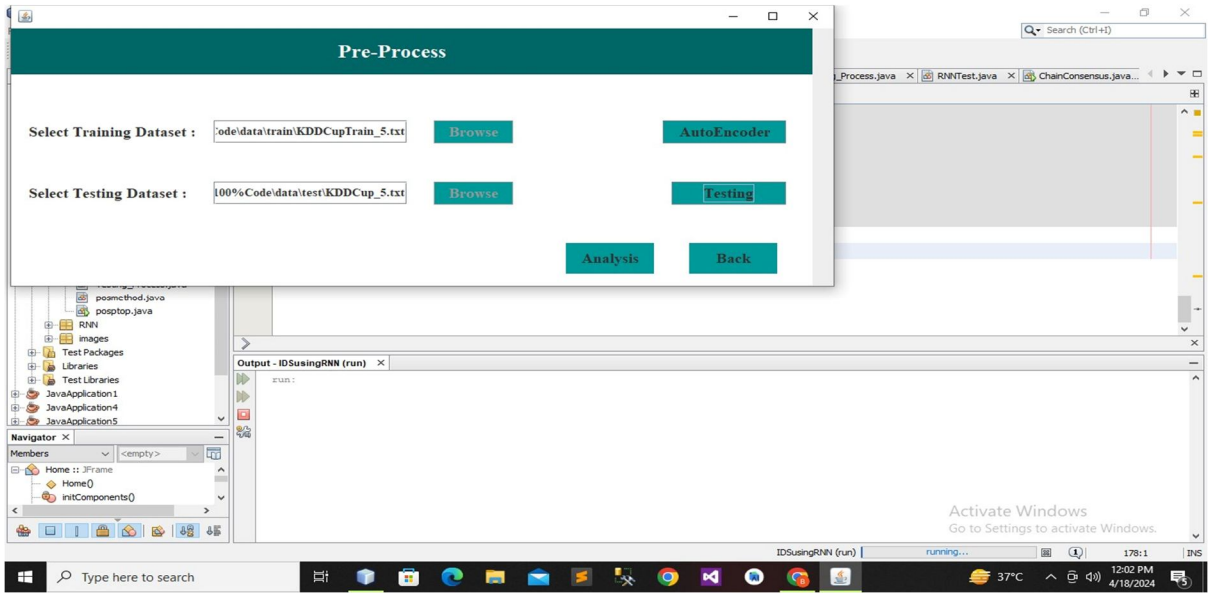
Input: data d, the Genesis block, the previous hash, Hash H was generated based on the provided data.
Step 1 : First, enter the data as d
Step 2: Utilize SHA 256 from the SHA group
Step 3: SHA256(d) is the current hash.
Step 4: Give Back the Current Hash

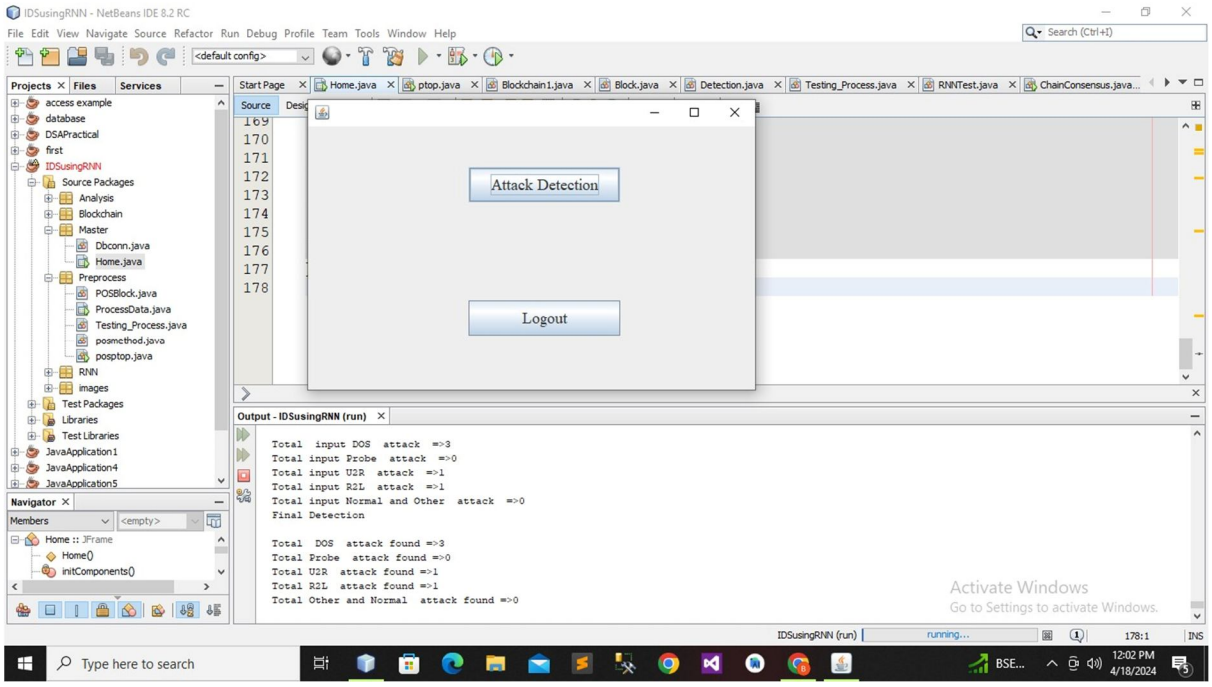
B. *Peer to Peer Algorithm*

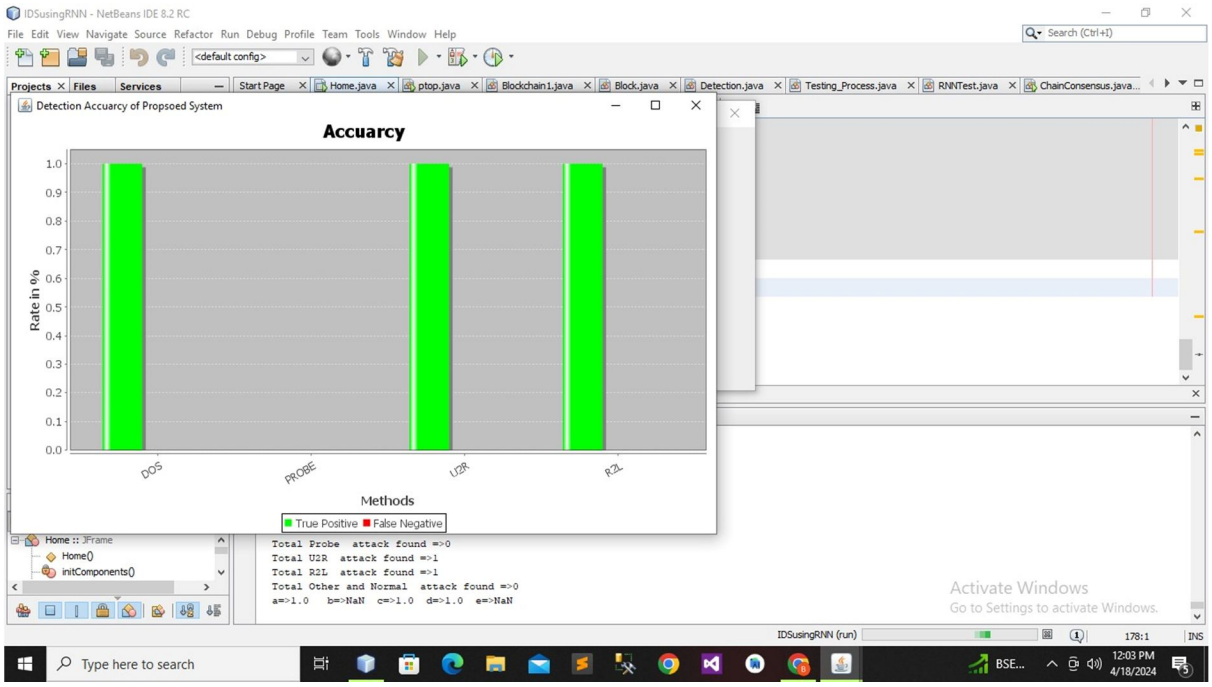
Peer-to-peer networks let millions of users connect directly, organize into groups, and work together to develop file systems, virtual supercomputers, and search engines that were all established by users. In contrast to the client-server approach, which involves communication to and from a central server, this network arrangement model is different. Though most people still consider P2P services to be at least internet-based, they have evolved beyond being solely internet services today. Peer-to-peer services encompass a variety of activities, from straightforward purchasing and selling to those that fall under the umbrella of the sharing economy. Peer-to-peer services bring people together to collaborate on projects, exchange information, or communicate without the need for direct middlemen. Some of them even operate without any paid transactions from the users. P2P services of this type can be run as non-profit, free services, or make money by selling user data or placing advertisements on their users' screens.

1) Open-source SoftwareAnyone can see and/or edit the software's code. Open-source software crowdsources the development, editing, and quality control of software among authors and users in an effort to do away with the need for a central publisher/editor.
2) Filesharing Files haring is the exchange of software files and media between uploaders and downloaders. Filesharing services offer security and file scanning in addition to peerto-peer networking. They may also provide users the option to anonymously evade intellectual property restrictions or alternatively may provide enforcement for intellectual property.

VII. RESULT







VIII. CONCLUSION & FUTURE SCOPE

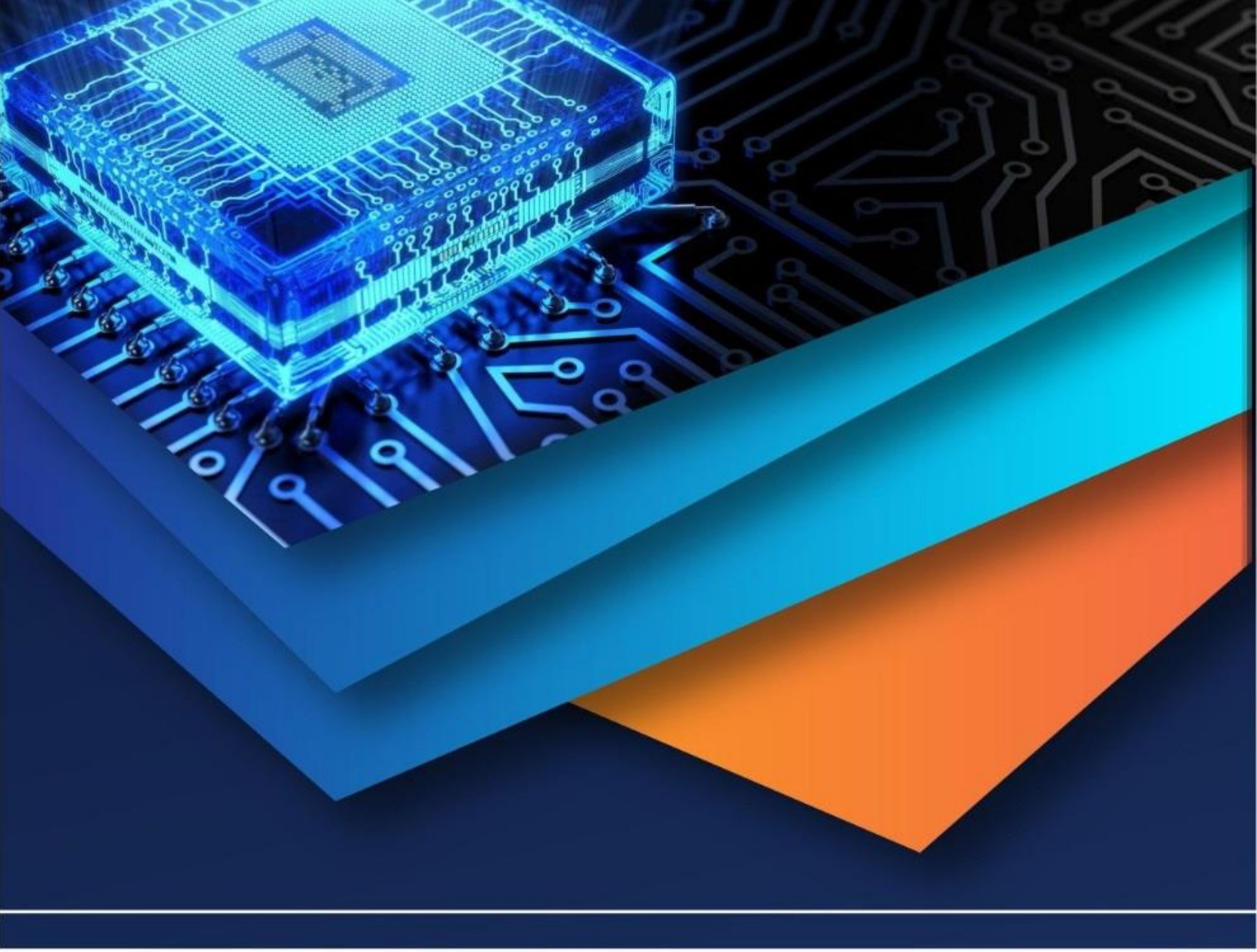
The entire IDS is written in Java. Thus, the present system is platform neutral, however it has been tested solely on Windows XP. It can be deployed and tested on many other machines which operate on other Operating systems and which satisfy the needs and pre-requisites for the IDS system. The log used by the current IDS system is only good for the current session; it does not retain data from previous sessions. By improving the log's ability to store information about previous sessions, this feature can be expanded. Techniques relating to the following next works could be added to the system to improve it

The current system does not use any methods to extract knowledge from the information included in the log entries; it only shows the log information. By using data mining techniques to examine the information in the log records, the system can be expanded and potentially improve decision-making efficiency. Only known attacks are detected by the current system.

This can be further enhanced by adding intelligence so that it can learn new intrusion patterns and analyse the increasing volume of traffic in order to acquire knowledge on its own. In our future work, we will also compare the performance of the proposed network intrusion detection with already existing intrusion detection systems based upon the methodology developed. We will also combine the proposed intrusion detection system and the Java-based cryptosystem using a dynamic Huffman coding and encryption methods we developed in . So doing, the security is reinforced to avoid intruder to discover plaintext data

REFERENCES

[1] User behaviour Pattern -Signature based Intrusion Detection al.Zakiyabanu S. Malek, Bhushan Trivedi, Axita Shah,978-1-7281- 6823-4/20/$31.00 c 2020 IEEE
[2] A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions, et al.Osama alkadi, nour moustafa ,and benjamin turnbull, 2020 IEEE
[3] An Intrusion Detection Method for CBTC Systems Using Blockchain and LSTM, et al. Qichang Li, Junyi Zhao, 979-8-3503-1080- 1/23/$31.00 ©2023 IEEE
[4] Design and Development of RNN Anomaly Detection Model for IoT Networks, et al.Imtiaz ullah , and qusay h. Mahmoud,2022 IEEE
[5] BIDS: Blockchain Based Intrusion Detection System for Electoral Process , et al.Salefu Ngbede Odaudu, Umoh J. Imeh, Umar Abubakar, 2020 IEE



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY