Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 5, April : 2024

INTRUSION DETECTION SYSTEM USING BLOCKCHAIN TECHNOLOGY

Prof. Jyotsna Kadam ,Research Scholar , Dept. Of Computer Engineering, Trinity College of Engineering and Research, Savitribai Phule Pune University, Pune.
Prof. Sneha Tirth, Assistant Professor, Dept. Of Computer Engineering , Trinity College of Engineering and Research, Savitribai Phule Pune University, Pune.
Prof. Sai Takwale ,Assistant Professor, Dept. Of Computer Engineering , Trinity College of Engineering and Research, Savitribai Phule Pune University, Pune.
Dr. Geetika Narang ,HOD Computer Engineering Department ,Trinity College of Engineering and Research, Savitribai Phule Pune University, Pune.

Abstract
Networks must be protected from harmful activity and illegal access by using intrusion detection systems, or IDS. But centralization, single points of failure, and manipulation susceptibility are problems for classic intrusion detection systems. These drawbacks can be addressed by blockchain technology, which provides transparent and safe record-keeping within a decentralized, unchangeable structure. An original method of IDS using Blockchain technology is presented in this study. Enhancing the security and dependability of intrusion detection systems is our goal by fusing Blockchain with IDS features. Through the safe recording and real-time validation of network events, the proposed system will make use of Blockchain's distributed ledger capabilities, facilitating the effective identification of unusual activity and possible security weaknesses. The suggested intrusion detection system (IDS) can automate threat detection and response procedures while maintaining data integrity and confidentiality by utilizing smart contracts and consensus methods. Moreover, the decentralized character of Blockchain guarantees resilience to attacks and augments the credibility of reported incursions. The suggested IDS employing Blockchain technology is examined in this study along with its design concepts, architecture, and implementation considerations. For improved cybersecurity, we also go over the possible advantages, difficulties, and future possibilities of using Blockchain technology into intrusion detection systems.
Keywords- Intrusion Detection System (IDS), Blockchain Technology, Security Enhancement

I. INTRODUCTION

In recent years, with the proliferation of interconnected systems and the exponential growth of data, ensuring the security of digital assets has become paramount. Traditional security measures, while effective to some extent, are often challenged by the sophistication of modern cyber threats. Intrusion Detection Systems (IDS) have long been a cornerstone of cybersecurity, serving as the frontline defense against unauthorized access and malicious activities within networks. However, the landscape of cybersecurity is evolving rapidly, necessitating innovative solutions to combat emerging threats. Blockchain technology, originally developed as the underlying framework for cryptocurrencies like Bitcoin, has garnered significant attention for its potential applications beyond the realm of finance. One such application is in bolstering the capabilities of IDS through decentralization and immutable record-keeping. The integration of blockchain technology with IDS introduces a paradigm shift in how security incidents are detected and mitigated. By leveraging the decentralized nature of blockchain networks, the detection process becomes more robust and resistant to tampering or manipulation. Furthermore, the use of smart contracts enables automated responses to detected threats, streamlining incident response procedures and minimizing human intervention. This study examines the relationship between intrusion detection and blockchain technology in an effort to give readers a thorough grasp of the advantages and disadvantages of this novel strategy. Through a detailed examination of existing literature and case studies, the efficacy of blockchain-based IDS solutions in enhancing network security is evaluated. Additionally, practical considerations such as scalability, interoperability, and regulatory compliance are addressed to facilitate the adoption of this transformative technology in real-world cybersecurity environments.

II. LITERATURE SURVEY

As technology advances, so does the possibility of a security breach. Despite the fact that we have a number of safety measures, they are not perfect. User authentication is the primary area of concern. Different biometric applications are used for authentication; nevertheless, even when authentication is completed, there is no assurance that the computer system is being used by the authorized user. The intrusion detection system (IDS) is a specific process that examines user behavior in the system once a user logs in to find intruders. Host-based intrusion detection systems keep an eye on user activity on the computer and recognize unusual or suspicious behavior from other users. In this work, the use of a set of rules as a pattern recognition engine by an expert system to identify intrusions is discussed. Based on a previously implemented SBID (Statistical Based Intrusion Detection) model, we propose a PIDE (Pattern Based Intrusion Detection) model that has been verified. According to the results of the experiment, integrating the PBID and SBID approaches creates a comprehensive system for detecting intrusion[1].

This paper examines the history and relevant research in the fields of blockchain applications, intrusion detection, and cloud systems defense against cyberattacks. In addition to discussing blockchain-based cloud system trustworthy and intrusion detection, this work seeks to explore collaborative anomaly detection systems for identifying insider and outsider attacks from cloud centers, including virtualization and containerization technologies. Furthermore, early detection of these malicious assaults is essential for carrying out the appropriate mitigation to lessen the impact of disruption and resume cloud activities and their live migration procedures. This document provides a summary of cloud architecture and classifies possible cutting-edge security events according to how they manifest at various cloud deployment patterns. The article also discusses popular detection techniques and classification types for Network Intrusion Detection Systems (NIDS) in cloud environments. To show how blockchain can address issues with data privacy and trust management, collaborative NIDSs for cloud-based blockchain applications are also described. Future research directions in these domains are also discussed, along with a review of the research problems [2](Osama alkadi, nour moustafa ,and benjamin turnbull, (2020)).

The dependability and accessibility of the data is one of the main information security concerns of CBTC systems. Conventional information security techniques are unable to address issues with intrusion detection, data accessibility, and reliability all at once. This study proposes an LSTM and blockchain-based intrusion detection technique for CBTC systems. This technique combines the benefits of distributed blockchain data sharing with the high detection accuracy of LSTM neural networks. The blockchain allows for the sharing and confirmation of all transactions, including the hash value of the detection alerts and the parameters of the LSTM neural network model. We run simulations using real CBTC data, and the outcomes show how effective our suggested approach[3].

Cybersecurity has become increasingly important in today's world because of the Internet of Things' (IoT) widespread use and the multiple attacks it has generated on computer systems and networks. Cybersecurity has grown increasingly difficult to manage as a result of the spread of IoT devices and services. Deep learning algorithms have made it possible to identify malicious traffic, which is now a critical component of network intrusion detection systems (IDS). Deep learning algorithms have been studied as a potential avenue for network intrusion detection. Recurrent neural networks (RNNs) have many applications. First, this study proposes a novel deep learning model for detecting anomalies in Internet of Things networks by utilizing a recurrent neural network. The Gated Recurrent Unit (GRU), BiL STM, and Long Short Term Memory (LSTM) are some of the implementation techniques. Convolutional Neural Networks (CNNs) are particularly helpful for feature learning because they can evaluate input features without losing important information. Next, a hybrid deep learning model was proposed using recurrent and convolutional neural networks. It was eventually possible to propose a

lightweight deep learning model for binary classification using methods based on LSTM, BiLSTM, and GRU.The proposed models are validated using BoT-IoT, IoT-NI, IoT-23, NSLKDD, and other deep learning models.MQTTset and IoT-DS2 datasets. Comparing the proposed binary and multiclass classification model to other deep learning implementations, it showed good recall, accuracy, precision, and F1 score[4].

Voter fraud and theft are intentional acts that are primarily committed at all electoral stages by fabricating, either electronically or manually, the true vote total. Although technology has made voting easier and faster, it is nevertheless a good development despite its susceptibility to cyberattacks and lack of a dependable and trustworthy system. As a result, blockchain technology is suggested in this article at various levels of the election result collation process to guarantee that the results counted remain consistent from the lower collation edge to the announcement and collation stage. In this paper, we examine the influence of technology on electoral system, e-voting system its pros and cons, which forms the basis for undertaking this work and the blockchain technology and its application of election result collation[5].

III. PROPOSED METHODOLOGY

The proposed methodology integrates Blockchain technology into Intrusion Detection Systems (IDS) to enhance network security. Blockchain nodes are deployed across the network to create a decentralized ledger of security events. Smart contracts automate response actions to detected threats, while cryptographic techniques ensure data integrity and confidentiality. Machine learning algorithms analyze historical data to improve threat detection, and interoperability standards enable collaborative threat response. This approach aims to leverage Blockchain's security features to fortify IDS, creating a more resilient defense against cyber threats.

A.APPLICATION

Blockchain-powered intrusion detection systems (IDS) have a wide range of uses in various sectors. In the financial industry, they safeguard transactions by keeping an eye out for manipulation or illegal access. They are used by healthcare systems to safeguard patient records from illegal changes or data breaches. In a similar vein, supply chain networks use blockchain-based IDS to guarantee the veracity and integrity of transactional data and product information, stopping fraud and fake items. These applications improve security, transparency, and trust in digital environments by integrating Blockchain with IDS. They do this by tackling growing cyber threats and guaranteeing the integrity of crucial data and processes.

B. SYSTEM ARCHITECTURE

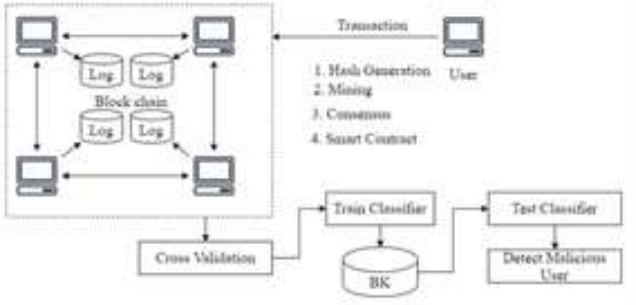

Fig1.System Architecture

C.ALGORITHM

SHA Algorithm :

SHA algorithm stands for Secure Hash Algorithm, which is a cryptographic hash function used in many security applications. Its ability to convert input data into a fixed-size hash output makes it useful

for creating digital signatures and validating data integrity.Strictly speaking, the Secure Hash Algorithm, or SHA algorithm, is one widely used hash function in cryptography. A fixed-size hash result, typically shown as a string of letters and numbers, is produced after a message is received as input. One of SHA's main objectives is to ensure data security. Frequently used applications include digital signatures, password storage, and data verification.

Algorithm 1: The Peer Verification Protocol
Input : User Transaction TID, User IP address,
Output : If a connection is valid, enable the IP address or the current query.
Step 1 : User-generated queries for any transaction—DDL, DML, or DCL
Step 2 : Get current IP address
If (connection(IP) equals(true))
Flag true
Else
Flag false
End for
Step 4 : if (Flag == true) Peer to Peer Verification valid
Else
Peer to Peer Verification Invalid
End if
End for

Algorithm 2:Hash Generation
Input : The previous hash, the genesis block,
Output : Hash H created based on the provided data
Step 1 : Input data as d
Step 2 : Apply SHA 256 from SHA family
Step 3 : Current Hash= SHA256(d)
Step 4 : Return Current Hash

Algorithm 3: Mining Algorithm for valid hash creation
Input : Hash Validation Policy P[], Current Hash Values hash Val
Output : Valid hash
Step 1 : System generate the hash Val for i th transaction using Algorithm 1
Step 2 : if (hash Val. valid with P[])
Flag =1
Else
Flag=0
Step 3 : Return valid hash when flag=1

Algorithm 4: Recover Block Chain Data
Input : User Transaction query, Current Node Chain CNode[chain], Old NodesChain [Nodeid]
Output: Run the current query and recover if any chains are invalid.
Step 1: The user creates a query for any transaction, DDL, DML, or DCL.
Step 2: Retrieve the server's current blockchain, Cchain ← Cnode[Chain].
Step 3: In NodeChain, read I using Foreach. If (!.equals Cchain(NodeChain[i])
Flag 1
Else Continue Commit query
Step 5 : if (Flag == 1)

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 5, April : 2024

Count = SimilaryN odesBlockchian()
Step6 : Calculatethemajorityofserver
Recoverinvalidblockchainfromspecif icnode
Step7 : EndifEndforEndfor

D.ACCURACY

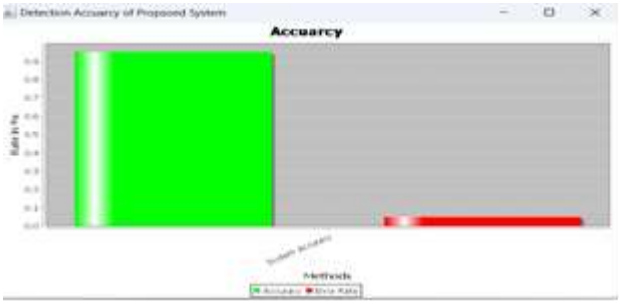

Fig 2.Graph of Accuracy

Accuracy :95%
Calculated by formula :True Positives(TP)/Total no. of records

IV EXPERIMENTAL ANALYSIS

This study aims to assess how well Blockchain Technology performs in the experimental examination of Intrusion Detection System (IDS). Extensive experimentation and testing is conducted to analyze the system's performance parameters, which include detection accuracy, false positive rate, detection duration, and resource utilization, under various network conditions and attack scenarios. Monitoring network traffic and identifying intrusions with an intrusion detection system (IDS) allows an experimental setup to be implemented in a real network design or simulated network environment. A network is subjected to a range of attacks, such as denial-of-service attacks, malware infections, and unauthorized access attempts, in order to assess an intrusion detection system's (IDS) response and threat neutralization capabilities. A number of parameters, including the number of nodes in the blockchain network, block size, transaction throughput, and consensus process, are changed during the experimental inquiry to enhance the performance and scalability of the IDS. The degree to which the system can withstand attacks such as node compromise or tampering with blockchain records is another way to assess its overall robustness and security posture. The analysis's trial findings provide useful details on how well the IDS employ blockchain technology to locate and thwart intrusions. Ultimately, these findings reinforce the security posture of modern computer networks against new cyberattacks and encourage ongoing advancements in intrusion detection technology.

V.EXPERIMENTAL RESULT

Fig. 3 Registration Page

Fig. 7Attacks Detected

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 5, April : 2024

Fig..4 Login Page

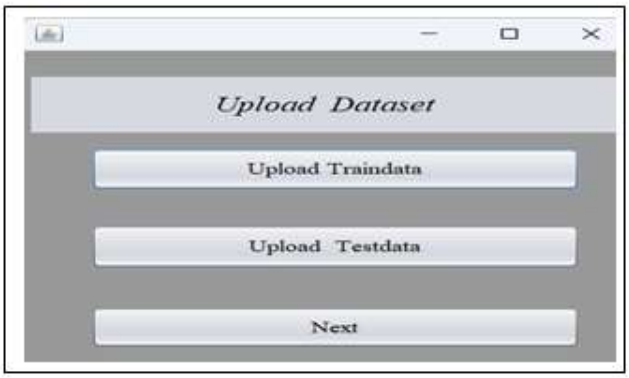

Fig. 5 Upload Dataset

Fig.6 Output

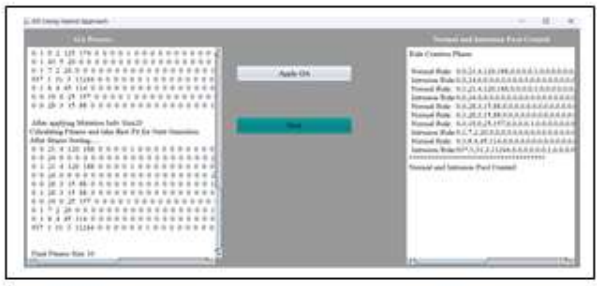

Fig. 8 Rules Created by GA

Fig. 9 Rules Created by AutoEncoder

Fig.10 Resulted Blockchain

V.CONCLUSION AND FUTURE SCOPE

In conclusion, integrating blockchain technology with an intrusion detection system (IDS) is a powerful technique to enhance the security of data and digital assets. The technology provides high levels of data integrity by leveraging blockchain, which ensures transparent and tamper-proof record-keeping of security incidents. The IDS's ability to continuously monitor network and system activity, identify anomalies, and send out real-time notifications improves the organization's ability to respond rapidly to potential security breaches. Blockchain-verified records also facilitate compliance reporting, which aids in regulatory compliance. Overall, the use of blockchain technology strengthens the IDS's ability to protect sensitive data and prevent assaults.

Blockchain-based intrusion detection systems (IDS) have a promising future ahead. This area of innovation aims to improve scalability, interoperability, and threat detection capabilities. It is envisaged that advancements in features for regulatory compliance and privacy preservation would address evolving cybersecurity challenges. Initiatives to develop decentralized governance models across industries will promote accountability, transparency, and cyberattack protection. Overall,

Blockchain-based intrusion detection systems have a lot to offer in terms of boosting cybersecurity defenses, fostering confidence in digital environments, and maintaining the security and integrity of sensitive data across a variety of sectors.

VI REFERENCES

[1] User behavior Pattern -Signature based Intrusion Detection,et 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 IEEE
[6] S. Malek, Zakiyabanu & Trivedi, Bhushan & Shah, Axita. (2019). User Behavior-Based Intrusion Detection Using Statistical Techniques: Second International Conference, ICAICR 2018, Shimla, India, July 14± 15, 2018, Revised Selected Papers, Part II. 10.1007/978-981-13-3143-5_39
[7] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, ‘‘A deep learning approach for network intrusion detection system,’’ in Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (Formerly BIONETICS), 2016, pp. 21–26.
[8] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivánkó, and M. Mühlhäuser, ‘‘Towards blockchain-based collaborative intrusion detection systems,’’ in Proc. Int. Conf. Crit. Inf. Infrastruct. Secur. Cham, Switzerland: Springer, 2017, pp. 107–118.
[9] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ‘‘When intrusion detection meets blockchain technology: A review,’’ IEEE Access, vol. 6, pp. 10179–10188, 2018.
[10] Song Y, Bu B, Zhu L. A novel intrusion detection model using a fusion of network and device states for communication-based train control systems[J]. Electronics, 2020, 9(1): 181.
[11] Yin B, Bu B, Gao B, et al. A Hybrid Intrusion Detection Method using Improved Stacking Ensemble Algorithm and False Positive Elimination Strategy for CBTC[C]//2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2022: 4253-4258.
[12] Tang T A, Mhamdi L, McLernon D, et al. Deep recurrent neural network for intrusion detection in sdn-based networks[C]//2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018: 202-206.
[13] Imrana Y, Xiang Y, Ali L, et al. A bidirectional LSTM deep learning approach for intrusion detection[J]. Expert Systems with Applications, 2021, 185: 115524.
[14] Boukhalfa A, Abdellaoui A, Hmina N, et al. LSTM deep learning method for network intrusion detection system[J]. International Journal of Electrical and Computer Engineering, 2020, 10(3): 3315.
[15] Ahsan M, Nygard K E. Convolutional Neural Networks with LSTM for Intrusion Detection[C]//CATA. 2020, 69: 69-79.
[16] Saveetha D, Maragatham G. Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning[J]. Pattern Recognition Letters, 2022, 153: 24-28.
[17] S. Tsimenidis, T. Lagkas, and K. Rantos, ‘‘Deep learning in IoT intrusion detection,’’ J. Netw. Syst. Manage., vol. 30, no. 1, pp. 1–40, Jan. 2022, doi: 10.1007/s10922-021-09621-9.
[18] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, ‘‘A bidirectional LSTM deep learning approach for intrusion detection,’’ Expert Syst. Appl.,vol. 185, Dec. 2021, Art. no. 115524, doi: 10.1016/j.eswa.2021.115524.
[19] Q. Wang, W. Zhao, and J. Ren, ‘‘Intrusion detection algorithm based on image enhanced convolutional neural network,’’ J. Intell. Fuzzy Syst., vol. 41, no. 1, pp. 2183–2194, Aug. 2021, doi: 10.3233/JIFS-210863.

[20] B. Susilo and R. F. Sari, ‘‘Intrusion detection in IoT networks using deep learning algorithm,’’ Information, vol. 11, no. 5, p. 279, May 2020, doi: 10.3390/info11050279.
[21] Cham, Switzerland: Springer, 2017, pp. 107–118.
[22] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ‘‘When intruion detection meets blockchain technology: A review,’’ IEEE Access, vol. 6, pp. 10179–10188, 2018.
[23] Song Y, Bu B, Zhu L. A novel intrusion detection model using a fusion of network and device states for communication-based train control systems[J]. Electronics, 2020, 9(1): 181.
[24] Yin B, Bu B, Gao B, et al. A Hybrid Intrusion Detection Method using Improved Stacking Ensemble Algorithm and False Positive Elimination Strategy for CBTC[C]//2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2022: 4253-4258.
[25] Tang T A, Mhamdi L, McLernon D, et al. Deep recurrent neural network for intrusion detection in sdn-based networks[C]//2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018: 202-206.
[26] Imrana Y, Xiang Y, Ali L, et al. A bidirectional LSTM deep learning approach for intrusion detection[J]. Expert Systems with Applications, 2021, 185: 115524.
[27] Boukhalfa A, Abdellaoui A, Hmina N, et al. LSTM deep learning method for network intrusion detection system[J]. International Journal of Electrical and Computer Engineering, 2020, 10(3): 3315.
[28] Ahsan M, Nygard K E. Convolutional Neural Networks with LSTM for Intrusion Detection[C]//CATA. 2020, 69: 69-79.
[29] Saveetha D, Maragatham G. Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning[J]. Pattern Recognition Letters, 2022, 153: 24-28.
[30] S. Tsimenidis, T. Lagkas, and K. Rantos, ‘‘Deep learning in IoT intrusion detection,’’ J. Netw. Syst. Manage., vol. 30, no. 1, pp. 1–40, Jan. 2022, doi: 10.1007/s10922-021-09621-9.
[31] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, ‘‘A bidirectional LSTM deep learning approach for intrusion detection,’’ Expert Syst. Appl.,vol. 185, Dec. 2021, Art. no. 115524, doi: 10.1016/j.eswa.2021.115524.
[32] Q. Wang, W. Zhao, and J. Ren, ‘‘Intrusion detection algorithm based on image enhanced convolutional neural network,’’ J. Intell. Fuzzy Syst., vol. 41, no. 1, pp. 2183–2194, Aug. 2021, doi: 10.3233/JIFS-210863.
[33] B. Susilo and R. F. Sari, ‘‘Intrusion detection in IoT networks using deep learning algorithm,’’ Information, vol. 11, no. 5, p. 279, May 2020, doi: 10.3390/info11050279.