iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** II **Month of publication:** February 2024

DOI: https://doi.org/10.22214/ijraset.2024.58361

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 II Feb 2024- Available at www.ijraset.com

Intrusion Detection System using Blockchain

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, Wagholi, Pune- 412207, India*

Abstract: ***This paper investigates the integration of an Intrusion Detection System (IDS) within the context of blockchain technology. The objective is to enhance the security posture of blockchain networks by detecting and mitigating potential intrusions. Through a meticulous examination of the current threat landscape and the unique challenges posed by blockchain systems, this research proposes a robust IDS framework tailored to the specific requirements of decentralized and distributed ledger environments. The study employs [specific methodology/approach] to assess the effectiveness of the proposed IDS, presenting conclusive findings that contribute to the ongoing discourse on securing blockchain ecosystems. The implications of this research extend to bolstering the resilience of blockchain networks against emerging threat.***
Keywords: Blockchain Security, Intrusion Detection System, Threat Landscape, Decentralized Ledger

I. INTRODUCTION

Blockchain technology, heralded for its decentralized and transparent nature, has emerged as a transformative force across various industries. However, the decentralized nature of blockchain networks introduces security challenges that necessitate innovative solutions. One such challenge is the inadequacy of traditional security measures in detecting and preventing intrusions in the blockchain space. The absence of a dedicated Intrusion Detection System (IDS) designed to cater to the unique characteristics of blockchain networks leaves these systems susceptible to attacks. This paper delves into the integration of an IDS within blockchain architectures, aiming to fortify the security posture of decentralized and distributed ledger systems. By providing a comprehensive examination of the existing security landscape and proposing an effective IDS framework, this research contributes to the ongoing efforts to enhance the robustness of blockchain technology in the face of evolving cyber threats

II. PROBLEM STATEMENT

The proliferation of blockchain technology has introduced novel security challenges, necessitating the development of specialized solutions. Traditional security mechanisms often fall short in safeguarding decentralized and distributed ledger systems. The inherent characteristics of blockchain, such as transparency and decentralization, create a unique attack surface that demands a tailored approach to intrusion detection. The absence of a dedicated Intrusion Detection System (IDS) specifically designed for blockchain environments poses a significant risk, leaving these systems vulnerable to various forms of attacks. This research aims to address this critical gap by formulating and evaluating an IDS framework optimized for the intricacies of blockchain technolog

III. OBJECTIVES

1) To study and analysis of various machine learning and deep learning techniques used in intrusion detection systems.
2) To design and develop a algorithm for hybrid feature selection from synthetic and real time network traffic data for unique feature selection
3) To develop a modified Recurrent Neural Network (RNN) deep learning based algorithm for intrusion detection and intrusion prevention system.
4) To explore and validate the proposed system with multiple network dataset as well as compare with existing approaches

IV. LITERATURE REVIEW

A literature survey for a smart contract system for digital certificate using blockchain would involve reviewing various research papers, articles, and projects related to smart contract system for digital certificate using blockchain Iftikhar Ahmad , Qazi Emad Ul Haq have describe a feature selection technique on the Matrix correlation. Matrix correlation calculated between the features. Selected optimal features from UNSW NB 15 dataset and proposed new model using decision tree to classify normal traffic and network threads. [1]

Osama Alkadi, Nour Moustafa have described this This paper discusses the collaborative anamaly detection system. This system can help discover insider and outsider attacks in cloud centres by analysing network behaviour and identifying anamolies that may indicates a potential attack these systems can use technologies such as virtualization and containerisation to monitor cloud resources and services and differentiate between various scenarios encountered during network behaviour analysis. [2]

Isiaka O. S, Bolaji-Adetoro D. F This paper provide a technique. In that technique IDS that uses the wireshark to capture detailed information of data packets. Imtiaz ullah , and qusay h. Mahmoud Cybersecurity is important today because of the increasing growth of the Internet of Things (IoT), which has resulted in a variety of attacks on computer systems and networks. Cyber security has become an increasingly difficult issue to manage as various IoT devices and services grow[3]

Lin Chen, Zhimin Gao, Lei Xu, Nolan Shah, Yang Lu, Weidong Shi have proposed paper in which the concept of blockchain is explained in detailed manner[5]. Blockchains main feature is decentralization in which data is not stored on single server. In these paper detailed algorithm for blockchain smart contract is explained which helps to understand the concept of smart contract very deeply. [4]

System Architecture

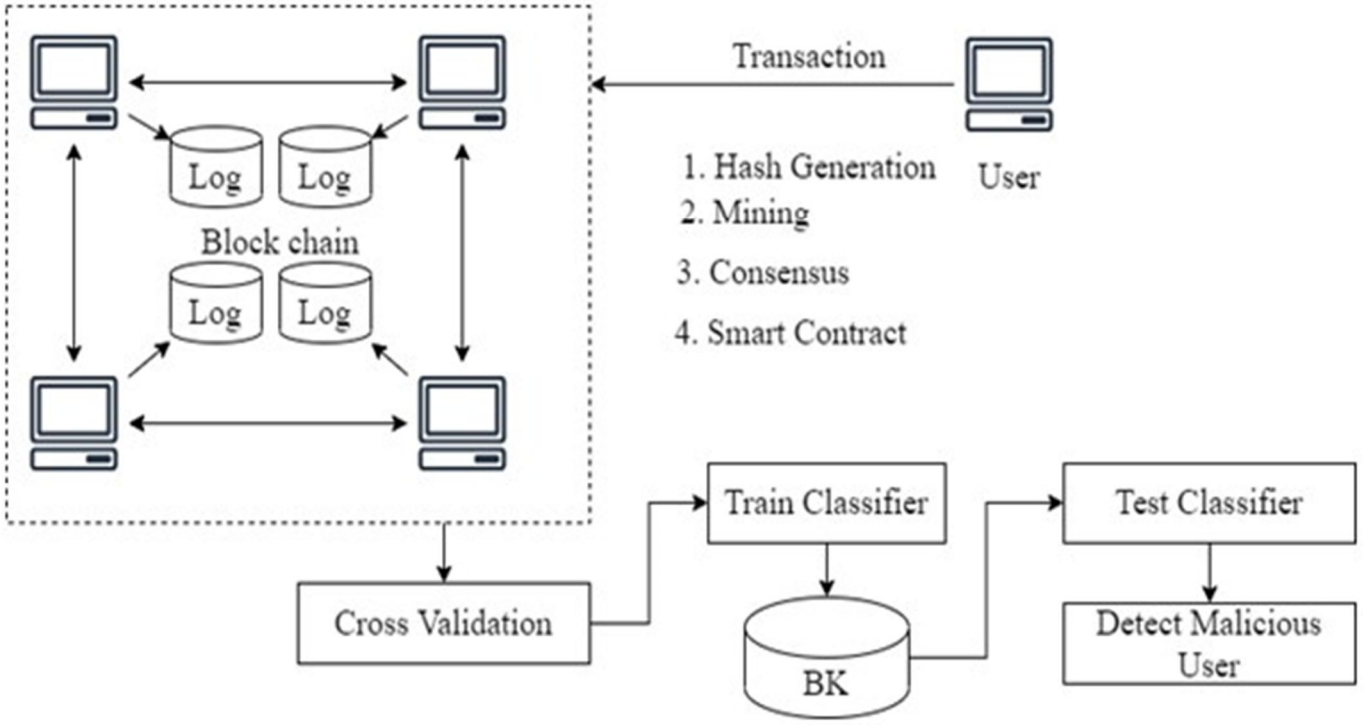


Fig.- Overview of the Proposed Architecture.

Intrusion detection system using blockchain technology typically consists of several components and follows a specific system architecture. Here's an overview of the key components and their functions:

1) *User:* The system process starts by login into the system. user are responsible for login process. After successful login user can be directed to the proposed system.
2) *Hash Generation:* Generated the hash value by using SHA 256 to become the data more secure And started mining the data
3) *Consensus:* Consensus Is the process where determine which transaction is validate and whuch are not. Called the majority and validate the labelled is validate or not
4) *Blockchain:* Blockchain technology plays an very important role in our system. It is main foundation of our project. Blockchains main feature is decentralization and immutable. Here no one can easily modify the data.
5) *BK:* BK stands for background knowledge .For bk used the RNN algorithm more secure detection
6) *Ethereum Virtual Machine (EVM):* It used to design smart contract agreement.
7) *Smart Contract:* It is piece of code where instructions are written in fixed formats. It is immutable piece of code which cannot be changed by any outsiders from network. It is deterministic.
8) *Solidity:* A solidity is language which helps you to easily develop and compile smart contracts code.It is high level language used to develop smart contracts. • Detect malicious user : Detect the user who is used malicious activity which are uploaded on blockchain.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

V. PROPOSED OUTCOMES

The proposed outcomes of IDS using blockchain is summarized as follows :

1) Provides a distributed and decentralized architecture for storing and sharing intrusion detection logs. This eliminates the single point of failure and enhances the resilience of the system against attacks.

2) Blockchain technology ensures the integrity and immutability of the intrusion detection logs. Each log entry is cryptographically linked to the previous one, creating a chain of blocks that cannot be altered or tampered with. This enables the detection of any unauthorized modifications or tampering .Attempts, making the IDS more reliable and trustworthy.

3) It secure data in network packets from the known attacks (such as phishing attack,man in the middle attack,etc) and unknown attacks

VI. CONCLUSION

In conclusion, leveraging blockchain technology within an Intrusion Detection System (IDS) Offers a robust solution for enhancing the security of digital assets and data. By integrating blockchain, The system ensures tamper-proof and transparent record-keeping of security events, providing a high Level of data integrity.

The IDS can continuously monitor network and system activities, detect Anomalies, and issue real-time alerts, improving the organization’s ability to respond to potential Security breaches promptly. Additionally, compliance reporting is streamlined with blockchain-verified Records, aiding in regulatory adherence. Overall, the use of blockchain technology strengthens the IDS's capabilities in safeguarding against intrusions and protecting sensitive information

REFERENCES

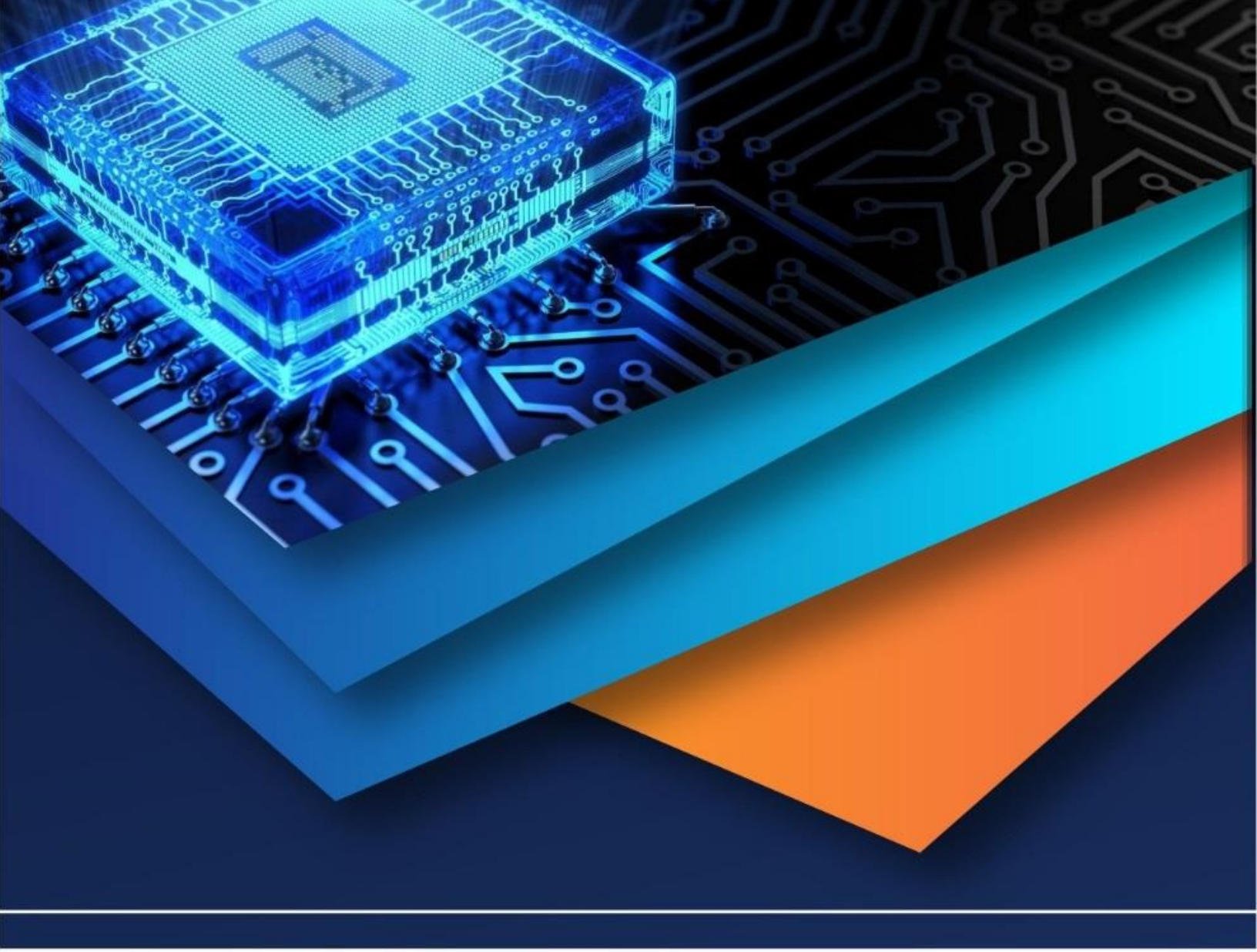
[1] User behavior Pattern -Signature based Intrusion Detection,et al.Zakiyabanu S. Malek, Bhushan Trivedi, Axita Shah,978-1-7281-6823-4/20/$31.00 c 2020 IEEE

[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 IDS 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