Volume 11, Issue 1, January 2024 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

A Survey on Intrusion Detection System using Blockchain Technology

Jyotsna Vitthalrao Kadam
M.E. Research Scholar
Computer Science and Engineering
Trinity College of Engineering and Research,
Pune, Maharashtra, India.
Email: jyotsna.v.jadhav@gmail.com

Sneha Somshankar Tirth
Assistant Professor
Computer Engineering Department,
Trinity College of Engineering and Research,
Pune, Maharashtra, India.
Email: snehatirth.tcoer@kjei.edu.in

Sai Yogesh Takwale
Assistant Professor
Computer Engineering Department,
Trinity College of Engineering and Research,
Pune, Maharashtra, India.
Email: saitakawale.tcoer@kjei.edu.in

Geetika Narang
Head of the Department
Computer Engineering Department,
Trinity College of Engineering and Research,
Pune, Maharashtra, India.
Email: hodcomp.tcoer@kjei.edu.in

Abstract

Cybersecurity threats continue to evolve, demanding innovative solutions to safeguard sensitive digital assets. "Intrusion Detection Systems" (IDS) play a crucial role in identifying and mitigating these threats. Traditional IDS, while effective, often face challenges related to data integrity, tamper resistance, and centralized points of failure. This research proposes an advanced Intrusion Detection System leveraging Blockchain Technology, a decentralized and secure framework. Blockchain technology, renowned for its immutability, transparency, and cryptographic security, offers a promising solution to the limitations of conventional IDS. By integrating blockchain, the IDS achieves unparalleled data integrity through immutable, tamper-proof records of network activities. This research explores the architectural design and implementation of a blockchain-based IDS, detailing the incorporation of smart contracts for automated threat response mechanisms this research contribute significantly to the field of cybersecurity by presenting As organizations worldwide face escalating cyber threats, the implementation of this Blockchain-based IDS offers a resilient defense mechanism, ensuring the protection of critical digital assets in an increasingly complex and interconnected digital landscape.

Keywords:— *Blockchain, Cybersecurity, Cyber Threats*

I. Introduction

Intrusion Detection System (IDS) is a security mechanism that monitors network traffic and system activities to identify and prevent unauthorized access, misuse, or any other malicious activities. It plays a crucial role in ensuring the security and integrity of computer systems and networks. Blockchain technology, on the other hand, is a decentralized and immutable ledger that records transactions across multiple computers. It is known for its transparency, security, and resistance to tampering. By combining IDS with blockchain technology, we can enhance the effectiveness and reliability of intrusion detection systems. The integration of blockchain technology into IDS brings several advantages. Firstly, it 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. Secondly, 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. Furthermore, the use of blockchain technology enables secure and private sharing of intrusion detection information between different organizations or entities. By using smart contracts, access to specific logs or information can be controlled and authenticated, ensuring that only authorized parties can access and utilize the data. Additionally, blockchain technology can incentivize network participants to contribute their intrusion detection data by rewarding them with tokens or other forms of digital assets. This promotes a collaborative and cooperative environment for sharing threat intelligence, leading to a more comprehensive and effective IDS.

II. Related Work

Technology Innovation progression likewise expands the gamble of a security. As we can have different components to guarantee security yet there have blemishes. The really concerned region is client confirmation. Have based IDS screens client conduct in the PC and distinguish client dubious way of behaving as an interruption or typical way of behaving. This paper examines how a specialist framework distinguishes interruptions involving a bunch of rules as an example perceived motor. We propose a PIDE (Example Based Interruption Recognition) model, which is confirmed recently executed SBID (Measurable Based Interruption Identification) model. Explore results demonstrate that reconciliation of SBID and PBID approach gives a broad framework to identify interruption (Zakiyabanu S. Malek, BhushanTrivedi, Axita Shah)

This paper surveys the foundation and related examinations in the space of cloud frameworks, interruption recognition and blockchain applications against digital assaults. This work means to talk about cooperative oddity location frameworks for finding insider and untouchable assaults from cloud focuses, including the advances of virtualisation and containerisation, alongside believing interruption discovery and cloud frameworks utilizing blockchain. In addition, the capacity to identify such malevolent assaults is basic for directing important alleviation, at a beginning phase, to limit the effect of disturbance and reestablish cloud tasks and their live movement processes. This paper presents an outline of cloud engineering and classifies likely cutting edge security occasions in view of their event at various cloud arrangement models. Network Interruption Identification Frameworks (NIDS) in the cloud, including sorts of order and normal discovery draws near, are additionally depicted. Cooperative NIDSs for cloud-based blockchain applications are additionally made sense of to exhibit how blockchain can address difficulties connected with information protection and trust the executives. A rundown of the examination difficulties and future exploration headings in these fields is likewise made sense of.(Osama alkadi, nourmoustafa , and benjaminturnbull et al.)

One of the key data security issues of CBTC frameworks is the information openness and dependability. The conventional data security strategies can't manage information availability, dependability and interruption location issues at the same time. In this paper, an interruption location technique is proposed utilizing blockchain and LSTM for CBTC frameworks. This strategy joins the benefits of circulated information sharing of blockchain, and the qualities of high location exactness of LSTM brain organization. The boundaries of the LSTM brain network model and the hash worth of the discovery cautions are exemplified as exchanges and transferred to the blockchain, every one of the exchanges can be shared and affirmed by the blockchain hubs. Reproductions are done with genuine CBTC information and the outcomes show the adequacy of our proposed technique. (Qichang Li, Junyi Zhao et.al)

The rise of innovation inside casting a ballot framework stays a welcome improvement as a result of the solace and speed it offer, but stays powerless against digital assault and has neglected to convey a trusted and solid framework. Hence, blockchain innovation in this paper is proposed at political decision result grouping stages to guarantee that outcome counted stays unaltered from the lower examination edge to the last phase of assemblage and declaration. In this paper, we look at the impact of innovation on appointive framework, e-casting a ballot framework its upsides and downsides, which shapes the reason for undertaking this work and the blockchain innovation and its use of political decision result gathering. (SalefuNgbedeOdaudu, Umoh J. Imeh, Umar Abubakar et. al.)

III. Methodology

Requirements Gathering: "Identify the specific requirements and objectives of the intrusion detection system, including the types of attacks to be detected, the network and system components to be monitored, the desired level of scalability, and the expected performance metrics".

System Design: Design the architecture and components of the intrusion detection system. This includes defining the network and system sensors, the data collection and analysis mechanisms, the blockchain framework, and the integration points between the IDS and the blockchain.

Blockchain Selection: Select the appropriate blockchain platform or framework that best suits the requirements of the intrusion detection system. Consider factors such as "scalability", "security", "consensus mechanism", "interoperability", and "developer community support".

Smart Contract Development: Design and develop smart contracts that define the rules, logic, and behavior of the intrusion detection system on the blockchain. This includes defining the data structures for storing intrusion detection logs, the access control mechanisms, the reward and incentive mechanisms, and the integration with other components of the IDS.

Integration and Implementation: Integrate the intrusion detection system components with the blockchain framework. This includes developing the necessary interfaces, APIs, and data flows between the IDS sensors, data collectors, analyzers, and the blockchain network. Implement the necessary data encryption, hashing, and digital signature mechanisms to ensure the "integrity" and "security" of the " intrusion detection logs".

Testing and Evaluation: Conduct thorough testing and evaluation of the "Intrusion Detection System" using realistic attack scenarios and data sets. Evaluate the system's performance, accuracy, scalability, and resilience against different types of attacks. Make necessary adjustments and optimizations based on the test results.

Deployment and Maintenance: Deploy the intrusion detection system in a production environment and monitor its performance and effectiveness. Regularly update and maintain the system to address new threats, vulnerabilities, and system requirements. Monitor the blockchain network for any potential security risks or performance issues.

Continuous Improvement: Continuously improve the intrusion detection system by incorporating feedback from users, security experts, and stakeholders. Stay updated with the latest advancements in blockchain technology and intrusion detection techniques to enhance the system's capabilities and effectiveness.

IV. Literature Survey

Sr. No.	Paper title	Publication Year	Method	Advantages	Limitations
1	Network intrusion detection system using Machine learning with data preprocessing and Feature extraction	2022	Machine Learning	Analyze large volumes of data and identify patterns that might be difficult for human operators to discern.	Machine learning models heavily depend on the quality of the training data
2	Network intrusion detection system: A systematic study of Machine learning and deep learning approaches	2022	Deep Learning	Analyze vast amounts of data and recognize complex patterns, leading to high accuracy in detecting network intrusions.	The quality of training data is paramount.
3	Research Trends in Network-Based Intrusion Detection Systems: A Review	2021	Machine Learning	The ability of intrusion detection systems to “identify novel and complex attacks”.	As intrusion detection systems analyze “network data, privacy concerns arise”, especially in sensitive environments.
4	Building Multiclass Classification Baselines for Anomaly-based Network Intrusion Detection Systems	2020	Deep Learning	Detect novel and previously unseen attacks, providing early warnings about potential security breaches before specific attack patterns are identified.	Types of network intrusions might be rare, leading to imbalanced datasets..
5	Comparing the Performance of Adaptive Boosted Classifiers In Anomaly based Intrusion Detection System for Networks	2019	Machine Learning	Anomaly-based detection systems excel at identifying previously unseen or unknown threats.	Real-world intrusion datasets are often imbalanced, with certain types of attacks being rare.
6	Network Traffic Analysis and Intrusion Detection using Packet Sniffer	2019	Machine Learning	Packet sniffers provide real-time monitoring of network traffic, allowing immediate detection of any suspicious or unauthorized activities.	Packet sniffers capture all data packets, potentially including sensitive information.
7	Research of Intrusion Detection Method Based on IL-FSVM	2019	Machine Learning	Achieve high accuracy in identifying and classifying intrusions, reducing the number of false positives and false negatives.	Machine learning-based systems require large and representative datasets for training, which can be challenging to obtain, especially for detecting rare or novel attacks.
8	An Exhaustive Research on the Application of Intrusion Detection Technology in Computer Network Security in Sensor Networks	2021	Machine Learning	Intrusion detection systems (IDS) in sensor networks can identify malicious activities at an early stage, preventing potential security breaches before they cause significant damage.	Sensor nodes often have limited processing power, memory, and energy.
9	Mapreducebased intelligent model for intrusion detection using Machine learning technique	2022	Machine Learning	Map reduce frameworks, like Apache Hadoop, provide a scalable infrastructure for processing large volumes of data across distributed clusters.	Handling sensitive network data in a distributed environment raises concerns about data security and privacy.
10	A Reliable Network Intrusion Detection Approach Using Decision Tree with Enhanced Data Quality	2021	Machine Learning	Decision trees are known for their ability to handle complex data patterns, leading to accurate intrusion detection.	Decision trees, especially deep ones, are prone to “overfitting, especially when the training data is noisy or contains outliers”.

V. Objectives

This paper is aimed to study and analysis of various machine learning and deep learning techniques used in “Intrusion Detection Systems”. To design and develop a algorithm for hybrid feature selection from synthetic and real time network traffic data for unique feature selection.

VI. Results

Data Analysis Analyze the collected data using various intrusion detection techniques, such as “signature-based detection”, “anomaly detection”, and “behavior-based detection”. Apply machine learning algorithms and statistical analysis to identify patterns and anomalies indicative of malicious activities. Intrusion Detection Logs Generate intrusion detection logs that record the detected threats, alerts, and other relevant information. Each log entry should include details such as the timestamp, source IP address, destination IP address, type of attack, severity level, and any additional contextual information. Blockchain Integration: Integrate the intrusion detection system with a blockchain framework, such as Ethereum or Hyperledger Fabric. Utilize the blockchain's distributed ledger to store and share the intrusion detection logs in a decentralized and tamper-proof manner.

Smart Contracts: Develop smart contracts that define the rules and logic for storing, accessing, and analyzing the intrusion detection logs on the blockchain. Implement access control mechanisms to ensure that only authorized entities can access and contribute to the logs. Data Encryption and Hashing: Apply cryptographic techniques to encrypt and hash the intrusion detection logs before storing them on the blockchain. This ensures the confidentiality and integrity of the logs and prevents unauthorized access or tampering. Reward and Incentive Mechanisms: Implement reward and incentive mechanisms to encourage network participants to contribute their intrusion detection data. This could involve rewarding participants with tokens or other digital assets for sharing valuable threat intelligence.

Collaborative Threat Intelligence: Enable secure and private sharing of intrusion detection information between different organizations or entities. Utilize smart contracts to control and authenticate access to specific logs or information, ensuring that only authorized parties can access and utilize the data. Monitoring and Analysis: Continuously monitor the blockchain network forany suspicious activities or anomalies. Analyze the blockchain data to identify any unauthorized modifications or tampering attempts on the intrusion detection logs. System Maintenance and Updates: “Regularly update and maintain the intrusion detection system to address new threats, vulnerabilities, and system requirements”. Stay updated with the latest advancements in blockchain technology and intrusion detection techniques to enhance the system's capabilities and effectiveness.

VII. Conclusion

Designing an “Intrusion Detection System “(IDS) using Blockchain Technology is a significant step toward enhancing cybersecurity measures. By leveraging the decentralized and secure nature of blockchain, this system offers unique advantages in detecting and mitigating various types of cyber threats. an Intrusion Detection System utilizing blockchain technology represents a promising approach to bolstering cybersecurity. However, it is essential to address the challenges effectively and stay updated with the rapidly evolving blockchain landscape. As the technology matures and becomes more widely adopted, overcoming these challenges will become more manageable, paving the way for a more secure digital future.

REFERENCES:

[1] A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions, etal. Osamaalkadi, nourmoustafa, and benjaminturnbull, 2020 IEEE

[2] 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

[3] BIDS: Blockchain Based Intrusion Detection System for Electoral Process, et al. Salefu Ngbede Odaudu, Umoh J. Imeh, Umar Abubakar, 2020 IEEE

[4] Research of Intrusion Detection Method Based on IL-FSVM, etal Zhengzhou University, Zhen Zhou, 2019, IEEE

[5] Research Trends in Network Intrusion Detection System:A Review, etal Satish Kumar, Sunanda Gupta , Sakshi Arora.2021, IEEE

[6] Network Traffic Analysis and Intrusion Detection using Packet Sniffer, etal Mohammed Abdul Qadeer, Mohammad Zahid, Arshad Iqbal, Misbahur Rahman Siddiqui.2023.IEEE

[7] Building Multiclass Classification Baselines for Anomaly-based Network Intrusion Detection System, etal Ajay Shah, Sophine Clachar, Manfired Minimair, Davis Cook, 2020, IEEE

[8] Comparing the Performance of Adaptive Boosted Classifier in Anomaly based Intrusion Detection System for Networks. Etal S. Sivnatham, R. Abirami, R. Gowsalya , 2019, IEEE

[9] Network Intrusion Detection System Using Machine Learning with Data Preprocessing and Feature Extraction, etal Manvith Pallepati, Soujenya Voggu, Rithesh Masula, Manisai Konjarla, 2022, IJRASET

[10] Salim Shaikh, B.Suresh Kumar, Geetika Narang "Diagnosis of Vector Machine Learning. Techniques", International Journal of Intelligent System and Applications in Engineering, ISSN:2147-67992.

[11] Salim Shaikh, B.Suresh Geetika Narang, "Several categories of the classification and recommendation Models for Dengue Disease: A Review", at the 5th International Conference on Intelligent Sustainable System (ICISS 2022), also as Lecture notes in Sringer's Network and System book series (LNNS, Volume - 458).

[12] Salim Shaikh, B. Suresh Kumar, Geetika Narang "Recommender system for health care analysis using machine learning technique: a review", Theoretical Issues in Ergonomics Science, Taylor and Francies, 22nd April 2022.https://doi.org/10.1080/1463922X.2022.2061078

[13] Ruwaida Shaikh, Vedant Bhogawade, Aditi Gangadhar, Chaitali Jadhav, Geetika Narang, "Blockchain based Electronic Vaccination Record Storing System", Advanced Computing and Communication System-IEEE-

ICACCS 2022, 25th and 26th March 2022 Shri Eshwar College of Engineering

[14] M.A.Abid, Z.Dehghan, T.Shinde and G.Narang, "Machine Learning based approaches for Identification and Prediction of diverse Mental Health Conditions," 2023 IEEE International Conference on Contemorary Computing and Communications (InC4), Bangalore, India, 2023.pp.1-5,doi:10.1109/InC457730.2023.10263141."

[15] T.Nakhawa, A.Nadaph, G.Narang, "Digital image water making based on visual secrete sharing scheme," 2022 8th International Conference on Advanced Computing and Communication System (ICACCS), Coimbatore, India, 2022, pp.336-341.

* * * * *