International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 August 2023 **Revised:** 07 October 2023 **Accepted:** 26 October 2023*

Blockchain Technology in the Intrusion Detection Domain

Dr Issac K Varghese[1], Dr Ajith Sundaram[2], Moshe Rani[3], A Srikanth[4], Keshaboina Samatha[5]
[1]Assistant Professor, T A Pai Management Institute, Manipal Academy of Higher Education, Manipal, India
issackvarghese@gmail.com
[2]Assistant Professor (Selection Grade), Amrita School of Business, Kochi, Amrita Vishwa Vidyapeetham, India. ajithsundaram@gmail.com
[3]Assistant Professor, Department of ECE Hyderabad Institute of Technology and Management
Mail : ranim.ece@hitam.org
[4]Assistant Profesor, Department of EEE ,Institute of Aeronautical Engineering Hyderabad.
Mail : a.srikanth@iare.ac.in"
[5]Assistant professor, Department of CSE, MLR Institute of Technology,Dundigal,Hyderabad.
Mail : samathak@mlrinstitutions.ac.in

Abstract: The ability of blockchain technology to improve security and transparency across a range of industries has receivedA great deal of attention has been garnered lately in correcting the sentence.. In the domain of intrusion detection, where the identification and mitigation of cyber threats are paramount, blockchain has emerged as a promising solution. This abstract examines how blockchain is used in intrusion detection systems and emphasizes its advantages. Blockchain technology improves the security and integrity of intrusion detection systems by using a decentralized and immutable ledger. It provides an immutable audit trail, distributed consensus, and increased resilience to attacks. Moreover, blockchain fosters trust, transparency, and collaboration among stakeholders, enabling faster threat detection and response. This research can explore novel approaches to integrating blockchain into intrusion detection systems, providing stronger protection against cyber threats.Immutable Audit Trail: In the context of intrusion detection, the capacity of blockchain to produce an unalterable and transparent audit trail is of enormous value. Research in this area can focus on developing techniques to leverage the blockchain's audit trail for effective incident response, forensic investigations, and attribution of cyberattacks. We will use theweighted product model in this study, which is a research approach that gives weights to various factors and combines them to make conclusions based on their relative relevance in a weighted way. Taken as alternative is"IDS1, IDS2, IDS3, IDS4, IDS5, IDS6, IDS7, and IDS8".Detection Quality, Performance, Stability, User Interface, Profile update, ConvenienceThe By this we can see that IDS4 has 1 RANK and IDS5 has the 8th RANK.In conclusion, blockchain technology holds great potential in the intrusion detection domain. Its decentralized and immutable nature can enhance the security and reliability of intrusion detection systems by providing transparent and tamper-proof logs of network activity. Blockchain-based solutions can improve threat detection, facilitate secure information sharing among entities, and enhance the overall resilience of intrusion detection systems. As the technology continues to evolve, further research and development in integrating blockchain with intrusion detection will unlock new possibilities for combating cyber threats.

Keywords: "Detection Quality**,**blockchain technology, supply-chain management, MA-ABS,IoT networks,Blockchain technology, security, intrusion detection systems, distributed systems".

1. INTRODUCTION

The Internet of Things (IoT) has the potential to deliver fascinating services to a range of industries, including online social networking businesses, automated transportation, and smart cities [1], [2], and [3]. We have witnessed this potential in recent years. In order to meet the growing demands of these industries, IoT connects heterogeneous devices with a range of functionalities into networks that are both machine- and human-centric. The huge amount of connected devices and the required Quality-of-Services (QoS) provide issues due to the IoT devices' constrained compute, storage, and bandwidth capabilities. Blockchain technology has recently had a transformational effect on all main categories of IoT applications. This paradigm change provides a decentralized setting with trustworthy and anonymous transactions. IoT systems can benefit from integration with blockchain technology by having cheaper operational costs, decentralized resource management, and resilience to threats and attacks, among other things. As a result, by combining IoT and blockchain technology, we hope to overcome significant obstacles to the establishment of an IoT platform in the near future.Satoshi Nakamoto presented the idea of blockchain in 2008 [8], first developed for virtual currencies like Bitcoin [1]. It has received a lot of interest recently as a novel peer-to-peer (P2P) technology for distributed computing and decentralized data exchange. Due to the adoption of encryption technologies and the absence of a central control agent or centralized data storage, blockchain is impenetrable to system takeovers. Later, in 2013, state machine for transactions Ethereum is a blockchain programming language that has been made available. Blockchain technology is now being

employed in a range of industries outside of cryptocurrencies due to its distinctive and appealing qualities such transaction privacy, security, information immutability, audibility, integrity, authorization, system transparency, and fault tolerance. Several advantages can be attained by applying blockchain to intrusion detection: 1. Increased Security: Because of the decentralized design that blockchain offers, it is more difficult for attackers to compromise the entire system. The integrity and authenticity of the data are guaranteed by the cryptographical security of transactions recorded on the blockchain.2. Immutable Audit Trail: Each intrusion detection system transaction or event can be stored as a block on the blockchain. These blocks are connected in a chronological order to provide an unchangeable audit trail. As a result, it is simpler to identify and verify occurrences, which makes it more difficult for attackers to hide their footprints.3. Distributed Consensus: To confirm and accept the system's present state, blockchain employs a consensus procedure. By requiring consensus among numerous network nodes regarding the legality of transactions, this distributed consensus protects against a single point of failure.4. Trust and Transparency: Blockchain's transparency allows authorized participants within the intrusion detection network to have visibility into the system's operations. This fosters trust among stakeholders and enables more effective collaboration between different entities involved in detecting and mitigating cyber threats.5. Resilience to Attacks: Since blockchain operates in a distributed manner across multiple nodes, it becomes resilient to common attack vectors like DDoS (Distributed Denial of Service) attacks. Even if some nodes are compromised or go offline, the system as a whole remains operational.6. Collaboration and Data Sharing: Blockchain enables safe and controlled data sharing between many entities, such as organizations, security researchers, and threat intelligence providers. This collaboration enables faster threat detection and response by leveraging collective knowledge and insights.By leveraging blockchain technology, intrusion detection systems can become more robust, transparent, and resilient against cyber threats. It offers a decentralized, tamper-resistant, and transparent infrastructure that enhances the overall security posture and promotes trust among participants in the network. However, it's important to note that while blockchain brings significant benefits, it also comes with its own challenges, such as scalability and energy consumption, which need to be addressed to fully utilize its potential in the intrusion detection domain.Ethereum, introduced as a blockchain programming language in 2013, is a transaction-based state machine. Blockchain is being used in businesses outside of cryptocurrency because of its unique and appealing features such transactional privacy, security, data immutability, auditability, integrity, authorization, system transparency, and fault tolerance. The multiple benefits of Blockchain's design include the following: There is no central authority, so all participants have equal rights. There is no chance of fraud because everyone keeps identical copies of the ledger. Fraud and counterfeit can be avoided thanks to the high level security and trust of the block chain system. In addition to the financial sector, Blockchain technology has a promising future in fields including automation, voting, e-healthcare, and fraud detection (cyber security). gadgets that are Internet-connected or Internet-capable a significant network of things, machines, instances, and other things that can communicate data.The internet of things/internet of vehicles is a collection of devices connected to the internet to perform specific functions supporting the transportation industry in the context of intelligent transportation or smart cars. In the automation and transportation sectors, IoT devices have advanced so swiftly that most vehicles will soon be integrated to connect to the internet or other IoT devices. For a longer time, these services will make consumers' life more convenient and joyful. It is important to note that tiny wearableAs shown in the following graphic, practically all IoT fields can benefit from the application of blockchain technology. “Healthcare Internet of Things The use of IoT in healthcare has enabled clinical data about patients, their families, friends, and healthcare professionals to be fed into e-healthcare systems. The data is recorded in electronic medical records (EMRs) by the competent healthcare provider. To facilitate patient data movement, certain electronic health records (EHRs) have a more complex data structure than EMRs. Esposito et al. advocated the development of a distributed online database-based blockchain-based system for IoT in healthcare. When new healthcare data is produced, a new block is instantiated and distributed in a consortium blockchain format.”a private blockchain platform. Guo et al. [34] suggested the MA-ABS attribute-based signature technique, which makes use of various authorities, in order to address EHR immutability. Blockchain technology is used in the MA-ABS proposal, which can fend off attempts by corrupted authorities to engage in N-1 collusion. Furthermore, a selective predicate attack on the MA-ABS renders it unforgeable. Consequently, Liang et al.'s [35] use of the blockchain network in mobile healthcare apps helped to safeguard integrity, conduct further audits, or conduct investigations. The Internet of Things in the 5G Era 5G will make it possible for the billions of connected things in the IoT Era to live in a completely mobile and connected society [44].A blockchain-based privacy preservation and data sharing technique was proposed by Fan et al. [45] to solve privacy concerns in the 5G heterogeneous communication environments. Each new block is founded on the idea of adding blocks to the blockchain and is connected to it by its hash value. Remember that the block header contains the previous hash value."Vehicles and heterogeneous networks, such as vehicle-to-vehicle, vehicle-to-road, vehicle-to-human, and vehicle-to-sensor networks, must create intelligent communication in order to with everything-to-vehicle, a brand-new idea known as the Internet of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 August 2023 **Revised:** 07 October 2023 **Accepted:** 26 October 2023*

Vehicles (IoV) was created. However, there have been a number of recent initiatives to investigate the use of blockchain technology in the Internet of Things (IoT).

2. MATERIALS AND METHODS

Benefits of WPM in Intrusion Detection: Enhanced Evaluation and Selection: The integration of WPM with blockchain technology enables a systematic and objective evaluation of intrusion detection systems. The weighted scores generated by WPM provide a quantitative measure to compare and select the most appropriate system based on predefined criteria. This facilitates informed decision-making and ensures that the selected system aligns with specific security requirements.Transparency and Trust: Blockchain's transparency ensures that the evaluation process is visible to authorized stakeholders, enhancing trust and accountability. Each step of the decision-making process, including criteria weights, evaluation results, and the final selection, can be audited and verified by participants. This transparency fosters collaboration and promotes confidence in the chosen intrusion detection system.Tamper-Resistance and Immutability: The use of blockchain technology ensures that the evaluation results and associated metadata are stored in an immutable manner. These outcomes cannot be changed or tampered with once they are stored on the blockchain, protecting the validity and integrity of the decision-making process. This attribute is crucial in maintaining the credibility and reliability of intrusion detection system selection.

Challenges and Future Directions: Scalability: As blockchain technology expands, ensuring scalability becomes a challenge. Research is needed to develop techniques that allow the integration of massive intrusion detection systems with evaluation procedures based on blockchain. This involves addressing scalability concerns and optimizing resource consumption.Privacy: In the intrusion detectiondomain, preserving the privacy of sensitive data is critical. Future research should explore privacy-enhancing mechanisms such as zero-knowledge proofs or selective disclosure to protect confidential information during the evaluation and selection process.

Evaluation parameters: Detection Quality, Performance, Stability, User Interface, Profile update, Convenience

Detection Quality: Detection quality refers to the accuracy and reliability of a detection system in correctly identifying and classifying objects or events of interest. It is commonly used in various fields, including computer vision, machine learning, cybersecurity, and sensor technologies.

Performance: blockchain technology, performance refers to the speed, scalability, and efficiency of a blockchain network in terms of processing transactions, validating blocks, and reaching consensus. It is an important factor since it affects the blockchain system's overall usability and efficiency.

Stability: In blockchain technology, stability refers to the robustness, reliability, and resistance to disruptions or attacks of a blockchain network. It ensures that the network can maintain its integrity, consistency, and availability over time, even in the presence of various challenges or adversarial conditions.

User Interface: In blockchain technology, the user interface (UI) refers to the graphical or visual interface through which users interact with the blockchain system. It encompasses the design, layout, and functionality of the software or application that allows users to access and interact with the blockchain network.

Profile update: In blockchain technology, a profile update refers to the process of modifying or updating the personal or account information associated with a user's blockchain identity. It allows users to make changes to their profile details, such as name, contact information, preferences, or any other relevant attributes.

incidents of identity theft Attacks of this nature create false identities to impersonate authorized users in order to access and manipulate the system. Key attacks, replay attacks, impersonation attacks, and sybil attacks are the four categories into which we divide assaults. The primary attack is: In the context of a system that uses electric automobiles and recharge stations, this assault is described as follows: If an electric car's private key is stolen, the attacker might pretend to be the car and deceive others. The LNSC protocol [10] provides a defense mechanism for mutual authentication between electric vehicles and charging stations to overcome this problem. By creating hash functions with elliptic curve encryption, it does this and ensures resistance to brute force attacks.LNSC [10] creates hash algorithms with elliptic curve encryption to counteract this vulnerability. For every request, BSein [39] instead creates a new, one-time public/private key pair, which is subsequently used to encrypt the message and determine the Message Authentication Code (MAC). Thus, it is possible to find the replay onslaught. Attack on impersonation: The attacker attempts to pose as a legitimate user to engage in illegal activity. Three strategies are provided to defend against this assault, as indicated in Table II. In order to calculate hash functions, the LNSC protocol [10] suggests utilizing elliptic curve encryption. The

distributed incentive-based cooperation method provided by Wang et al. [16] ensures the user's anonymity while also protecting their privacy.The method shields users from impersonation attacks and hides their private information within a group. BSeIn [39], on the other hand, takes use of the concept of attribute-based signatures, which states that only legitimate terminals may deliver a valid signature; as a result, any attempt at impersonation will be discovered when the related authentication mechanism fails. Sybil abuse: This tactic was employed by an enemy to construct several false identities. An attacker can acquire a lot of influence inside the community by engaging in a variety of network interactions, such as raising or lowering the reputation of specific agents. By creating an immutable chain of time-ordered interactions for each agent, Trust Chain [40] addresses this problem. By using past transactions as input, it calculates the trustworthiness of agents in an online community while including Sybil-resistance. The Trust Chain makes sure that those who use community resources also give something back. In terms of manipulation-based assaults, they encompass tampering with and unauthorized access to data. This category includes four types of attacks: manipulation, overlaying, alteration, and false data injection. All of these attacks are feasible.Attack on fake data injection aims to compromise the data integrity of the control system, leading it to make poor control decisions. The metre node is a private blockchain network, claim Liang et al. [21]. 9 Additionally, the consensus technique used for node interactions is based on the execution of a distributed voting algorithm. Each node has the capacity to verify the data it has received. When there is agreement, the latter is deemed to be correct. utilize a public-key cryptosystem that is compatible with the current Bitcoin system, as stated in [41]. The plaintext transaction quantities would be covered by the homomorphic Paillier encryption method, and the encrypted transaction amounts would be verified by the commitment proof. Overlay attack: When this occurs, the attacker augments the original encrypted amount using the recipient's public key by encrypting additional data. This exploit is identified in [41] because each transaction includes a timestamp to identify its uniqueness. It is possible to identify and link several inputs from the same trader to various transactions, ensuring resilience against the overlay attack. Attack involving modification: To do this, the broadcast transaction or response message must be modified. LNSC [10] uses the idea of elliptic curve encryption to compute hash functions in order to address this problem. In contrast, BSeIN [39] makes use of both MAC and attribute signatures. When a man-in-the-middle assault occurs and the attacker poses as two separate people, they can secretly transmit and even modify the communication between these individuals, creating the illusion of direct communication while having full control over the entire conversation. To address this risk, BSeIN [39] provides secure mutual authentication. More information about LNSC can be found in [10].

Method: This document presents a brief explanation of the Weighted Product Model (WPM) in the context of blockchain technology in the intrusion detection domain. WPM is a decision-making approach that allows the evaluation and selection of intrusion detection systems based on multiple criteria. By integrating WPM with blockchain technology, a robust and transparent framework for intrusion detection can be achieved. This document discusses the key concepts of WPM, its application in the intrusion detection domain, and the benefits it offers in terms of system selection and evaluation. Additionally, it explores the potential challenges and future directions for research in this area.Intrusion detection is a critical aspect of cybersecurity, aimed at identifying and mitigating unauthorized access attempts and malicious activities within computer networks. With the advent of blockchain technology, there is an opportunity to enhance the security, transparency, and efficiency of intrusion detection systems. “The Weighted Product Model (WPM) is a multi-criteria decision-making approach that can be integrated with blockchain technology to evaluate and select the most suitable intrusion detection system based on predefined criteria.” Weighted Product Model (WPM): The Weighted Product Model is a well-established decision-making technique that allows the aggregation of multiple criteria and their respective weights to rank alternatives based on their performance. In the context of intrusion detection, various criteria such as accuracy, response time, scalability, resource consumption, and detection capabilities can be considered. By assigning weights to each criterion, WPM calculates a weighted product score for each alternative, facilitating their comparison and selection.Integrating WPM with Blockchain Technology: Blockchain technology offers a decentralized, tamper-resistant, and transparent infrastructure that aligns well with the objectives of intrusion detection systems. By integrating WPM with blockchain, the evaluation and selection process can be conducted in a secure and auditable manner. The blockchain ledger can store the criteria weights, evaluation results, and relevant metadata, ensuring the integrity and traceability of the decision-making process.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *07 October 2023* ***Accepted:*** *26 October 2023*

3. RESULTS AND DISCUSSIONS

TABLE 1. Blockchain Technology in The Intrusion Detection Domain

	Detection quality	Performance	stability	User interface	profile update	convenience
IDS1	3.060	0.730	0.820	1.640	0.820	2.760
IDS2	3.453	0.820	1.000	1.180	0.730	2.573
IDS3	1.940	1.180	0.730	1.640	0.820	2.760
IDS4	7.997	4.180	5.000	0.360	1.180	8168.393
IDS5	3.060	0.730	1.000	1.180	0.730	2.573
IDS6	3.453	0.820	0.730	1.640	0.820	2.760
IDS7	1.940	1.180	5.000	0.360	1.180	2.543
IDS8	7.997	4.180	2.820	6.270	4.180	6.817

Table 1 shows the “IDS1, IDS2, IDS3, IDS4, IDS5, IDS6, IDS7 and IDS8” recorded values for each category (Detection quality, Performance, Stability, User interface, Profile update, Convenience) within the IDS systems, we can identify the highest and lowest values.Detection quality:Highest value: IDS4 - 7.997Lowest value: IDS3 - 1.940Performance:Highest value: IDS8 - 4.180Lowest value: IDS1, IDS5, IDS6 - 0.730Stability:Highest value: IDS4, IDS7 - 5.000Lowest value: IDS3 - 0.730User interface:Highest value: IDS8 - 6.270Lowest value: IDS4 - 0.360Profile update:Highest value: IDS8 - 4.180Lowest value: IDS3 - 0.820Convenience:Highest value: IDS8 - 6.817Lowest value: IDS4 - 8168.393.

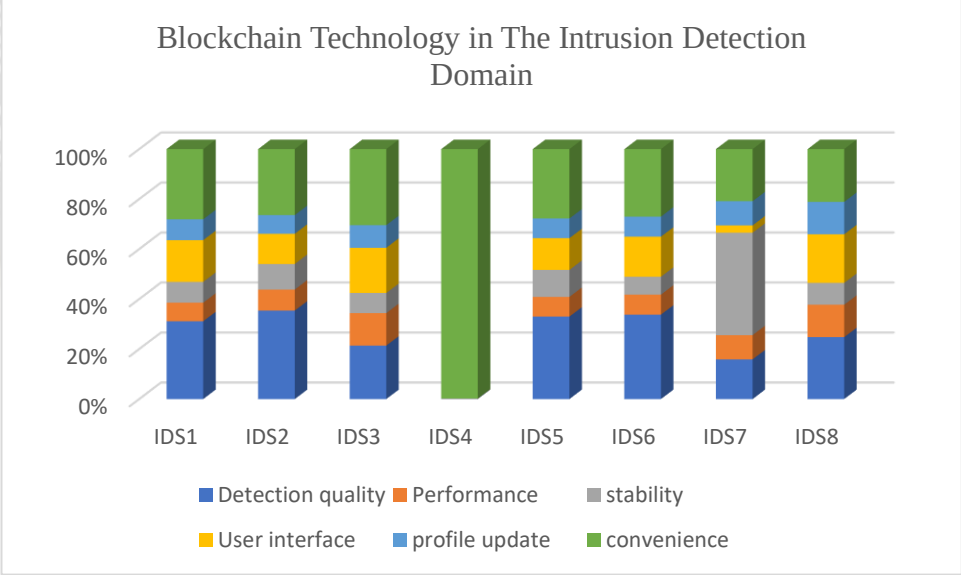

Figure 1shows the “IDS1, IDS2, IDS3, IDS4, IDS5, IDS6, IDS7and IDS8” recorded values for each category (Detection quality, Performance, Stability, User interface, Profile update, Convenience) within the IDS systems, we can identify the highest and lowest values.Detection quality:Highest value: IDS4 - 7.997Lowest value: IDS3 - 1.940 Performance:Highest value: IDS8 - 4.180Lowest value: IDS1, IDS5, IDS6 - 0.730Stability:Highest value: IDS4, IDS7 - 5.000Lowest value: IDS3 - 0.730User interface:Highest value: IDS8 - 6.270Lowest value: IDS4 - 0.360Profile update:Highest value: IDS8 - 4.180Lowest value: IDS3 - 0.820Convenience:Highest value: IDS8 - 6.817Lowest value: IDS4 - 8168.393.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *07 October 2023* ***Accepted:*** *26 October 2023*

TABLE 2. Performance value

	Performance value					
IDS1	0.38266	0.17464	0.16400	0.26156	0.19617	0.00034
IDS2	0.43185	0.19617	0.20000	0.18820	0.17464	0.00032
IDS3	0.24260	0.28230	0.14600	0.26156	0.19617	0.00034
IDS4	1.00000	1.00000	1.00000	0.05742	0.28230	1.00000
IDS5	0.38266	0.17464	0.20000	0.18820	0.17464	0.00032
IDS6	0.43185	0.19617	0.14600	0.26156	0.19617	0.00034
IDS7	0.24260	0.28230	1.00000	0.05742	0.28230	0.00031
IDS8	1.00000	1.00000	0.56400	1.00000	1.00000	0.00083

Table 2 shows performance value of alternative and evaluation parametersthe recorded values for each category (Detection quality, Performance, Stability, User interface, Profile update, Convenience) within the IDS systems, we can identify the highest and lowest values.Detection quality:Highest value: IDS4, IDS8 - 1.00000Lowest value: IDS3 - 0.24260Performance:Highest value: IDS4, IDS8 - 1.00000Lowest value: IDS1, IDS5 - 0.17464Stability:Highest value: IDS7 - 1.00000Lowest value: IDS3 - 0.14600User interface:Highest value: IDS8 - .00000Lowest value: IDS4, IDS7 - 0.05742Profile update:Highest value: IDS8 - 1.00000Lowest value: IDS1, DS3, IDS5, IDS6 - 0.00034Convenience:Highest value: IDS8 - 0.00083

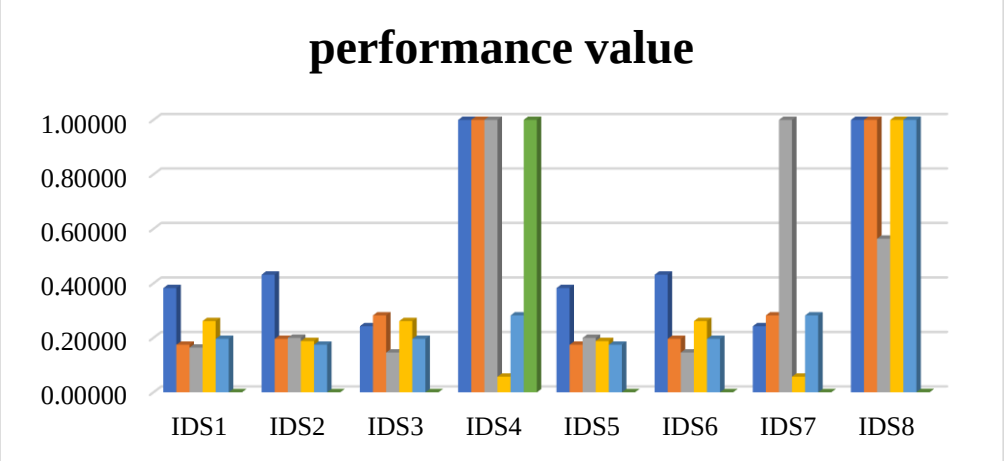

FIGURE 2.performance value

Figure 2shows performance value of alternative and evaluation parameters the recorded values for each category (Detection quality, Performance, Stability, User interface, Profile update, Convenience) within the IDS systems, we can identify the highest and lowest values. Detection quality: Highest value: IDS4, IDS8 - 1.00000 Lowest value: IDS3 - 0.24260 Performance: Highest value: IDS4, IDS8 - 1.00000 Lowest value: IDS1, IDS5 - 0.17464 Stability: Highest value: IDS7 - 1.00000 Lowest value: IDS3 - 0.14600 User interface: Highest value: IDS8 - .00000 Lowest value: IDS4, IDS7 - 0.05742 Profile update: Highest value: IDS8 - 1.00000 Lowest value: IDS1, DS3, IDS5, IDS6 - 0.00034 Convenience

TABLE 3. Weightages

	Weight					
IDS1	0.17	0.17	0.17	0.17	0.17	0.17
IDS2	0.17	0.17	0.17	0.17	0.17	0.17
IDS3	0.17	0.17	0.17	0.17	0.17	0.17
IDS4	0.17	0.17	0.17	0.17	0.17	0.17

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *07 October 2023* ***Accepted:*** *26 October 2023*

IDS5	0.17	0.17	0.17	0.17	0.17	0.17
IDS6	0.17	0.17	0.17	0.17	0.17	0.17
IDS7	0.17	0.17	0.17	0.17	0.17	0.17
IDS8	0.17	0.17	0.17	0.17	0.17	0.17

Table 3 Weight shows the informational set for the weight all same value 0.17.

TABLE 4. Weighted Normalised Decision Matrix

	Weighted normalized decision matrix					
IDS1	0.85206	0.74764	0.73984	0.79970	0.76227	0.26391
IDS2	0.86940	0.76227	0.76472	0.75701	0.74764	0.26085
IDS3	0.78974	0.80994	0.72565	0.79970	0.76227	0.26391
IDS4	1.00000	1.00000	1.00000	0.62112	0.80994	1.00000
IDS5	0.85206	0.74764	0.76472	0.75701	0.74764	0.26085
IDS6	0.86940	0.76227	0.72565	0.79970	0.76227	0.26391
IDS7	0.78974	0.80994	1.00000	0.62112	0.80994	0.26034
IDS8	1.00000	1.00000	0.90896	1.00000	1.00000	0.30684

Table 4 shows the weighted normalised decision matrix of alternative and evaluation parametershe weighted normalized decision matrix, we can identify the highest and lowest values.Detection quality:Highest value: IDS4, IDS8 - 1.00000Lowest value: IDS3 - 0.78974 Performance:Highest value: IDS4, IDS8 - 1.00000Lowest value: IDS1, IDS5 - 0.74764 Stability:Highest value: IDS7 - 1.00000Lowest value: IDS3 - 0.72565User interface:Highest value: IDS8 - 1.00000Lowest value: IDS4, IDS7 - 0.62112Profile update:Highest value: IDS8 - 1.00000Lowest value: IDS1, IDS2, IDS3, IDS5, IDS6 - 0.26085Convenience:Highest value: IDS8 - 0.30684Lowest value: IDS1, IDS2, IDS3, IDS5, IDS6 - 0.26034.

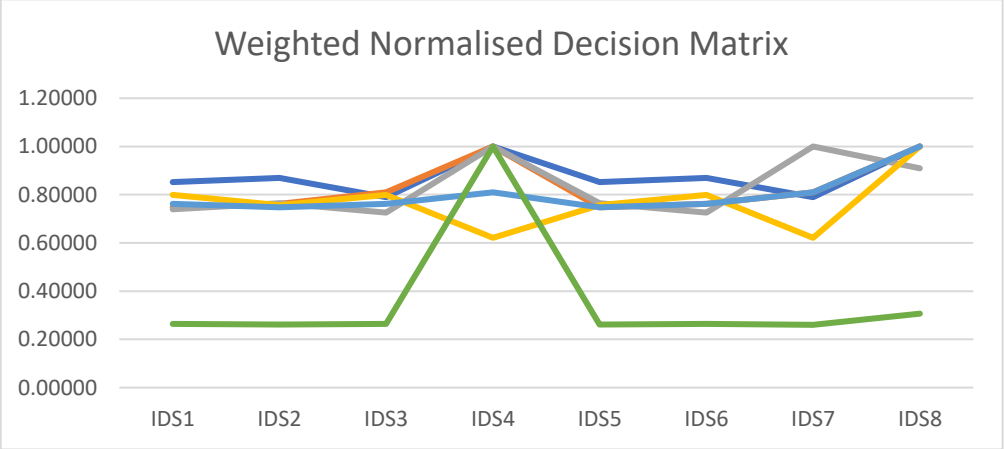

FIGURE 3. Weighted Normalised Decision Matrix

Figure 3 shows the weighted normalised decision matrix of alternative and evaluation parametershe weighted normalized decision matrix, we can identify the highest and lowest values.Detection quality:Highest value: IDS4, IDS8 - 1.00000Lowest value: IDS3 - 0.78974 Performance:Highest value: IDS4, IDS8 - 1.00000Lowest value: IDS1, IDS5 - 0.74764 Stability:Highest value: IDS7 - 1.00000Lowest value: IDS3 - 0.72565User interface:Highest value: IDS8 - 1.00000Lowest value: IDS4, IDS7 - 0.62112Profile update:Highest value: IDS8 - 1.00000Lowest value: IDS1, IDS2, IDS3, IDS5, IDS6 - 0.26085Convenience:Highest value: IDS8 - 0.30684Lowest value: IDS1, IDS2, IDS3, IDS5 and IDS6 - 0.26034.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *07 October 2023* ***Accepted:*** *26 October 2023*

TABLE 5. Preference Score & Rank

	Preference Score	RANK
IDS1	0.075823	5
IDS2	0.07482	6
IDS3	0.074672	7
IDS4	0.503064	1
IDS5	0.07192	8
IDS6	0.077366	4
IDS7	0.083772	3
IDS8	0.278903	2

Table 5 shows the Preference Score & Rankof alternative and evaluation parametersthe preference scores and ranks provided, we can identify the highest and lowest values.Highest preference score: IDS4 - 0.503064 (Ranked 1)Lowest preference score: IDS5 - 0.07192 (Ranked 8).

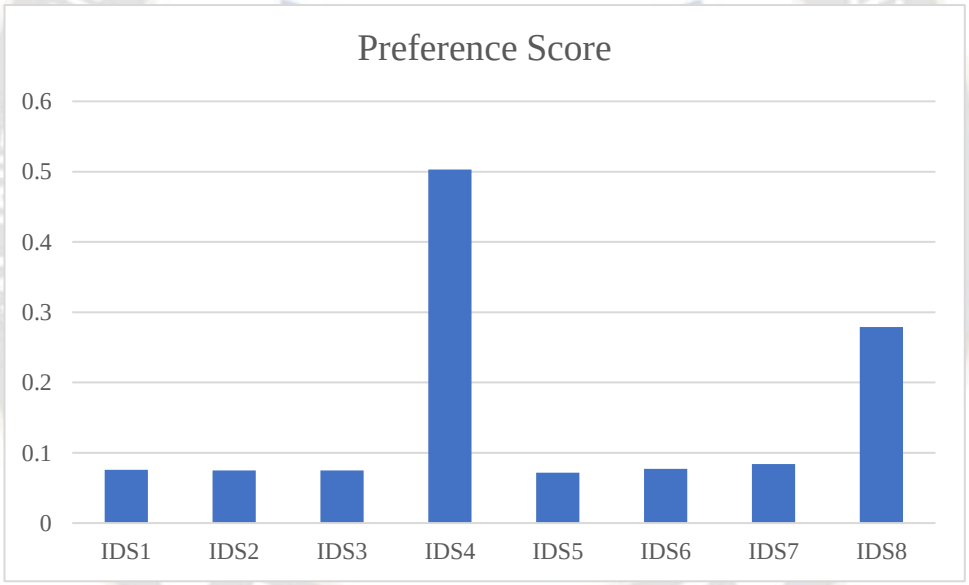

FIGURE 4. Preference Score

Figure 4shows the Preference Score &Rankof alternative and evaluation parameters the preference scores and ranks provided, we can identify the highest and lowest values. Highest preference score: IDS4 - 0.503064 (Ranked 1) Lowest preference score: IDS5 - 0.07192 (Ranked 8).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *07 October 2023* ***Accepted:*** *26 October 2023*

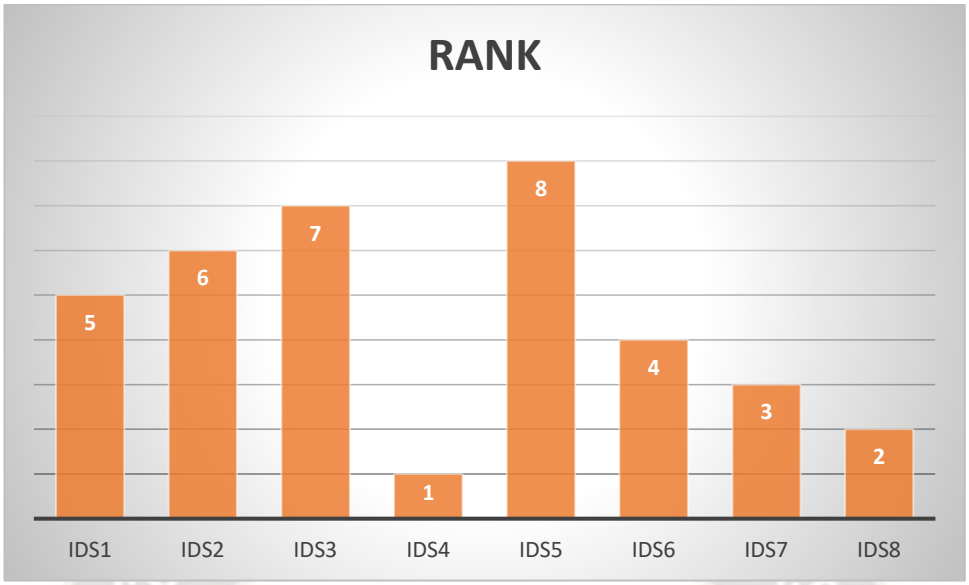

FIGURE5. Rank

Figure 5 shows "IDS1, IDS2, IDS3, IDS4, IDS5, IDS6, IDS7and IDS8"&Evaluation parameters: Detection Quality, Performance, Stability, User Interface, Profile update, Convenience.By this we can see that IDS4 has 1 RANK and IDS5 has the 8th RANK.

4. CONCLUSION

In conclusion, the utilization of blockchain technology in the intrusion detection domain presents numerous benefits and opportunities. By leveraging its decentralized and tamper-proof nature, blockchain enhances the security, transparency, and trustworthiness of intrusion detection systems. The use of blockchain technology ensures the immutability and integrity of intrusion detection data, safeguarding against unauthorized alterations or manipulations. This, in turn, enables more reliable and accurate detection of malicious activities, thereby strengthening network security. Furthermore, the distributed consensus mechanism in blockchain enhances transparency and trust in the intrusion detection process.The likelihood of false positives and false negatives is decreased through the involvement of numerous nodes in validating and verifying the data, resulting in more efficient and effective intrusion detection.In conclusion blockchain technology shows great promise for improving the security and dependability of network systems when it is integrated into intrusion detection. By leveraging its decentralized and immutable nature, blockchain offers several advantages in detecting and preventing unauthorized access.Blockchain offers a safe and unchangeable platform for storing intrusion detection data, guaranteeing the accuracy and legitimacy of the data. This helps in identifying and tracking malicious activities more effectively, as any unauthorized alterations or modifications can be easily detected.Moreover, the distributed consensus mechanism in blockchain improves the transparency and trustworthiness of intrusion detection systems. Through the participation of multiple nodes in validating and verifying the data, the likelihood of false positives and false negatives is minimized, leading to more accurate and reliable intrusion detection alerts.Furthermore, the utilization of blockchain facilitates efficient and secure information sharing among different entities involved in intrusion detection. This promotes collaboration and enables faster response times, as stakeholders can access and share relevant threat intelligence in a trust less and decentralized environment.While blockchain technology in the intrusion detection domain is still in its early stages, ongoing research and development are expected to unlock its full potential. As the technology matures, we can anticipate even more robust and sophisticated intrusion detection systems that leverage the benefits of blockchain, enhancing network security and thwarting cyber threats effectively.Additionally, blockchain technology facilitates secure and efficient information sharing among different entities within the intrusion detection ecosystem. By eliminating the need for intermediaries and providing a decentralized platform, blockchain promotes collaboration and cooperation, enabling faster response times and more comprehensive threat intelligence.Overall, the integration of blockchain technology in the intrusion detection domain holds the potential to revolutionize the protection of computer networks against unauthorized access. As this technology continues to evolve and mature, we can anticipate significant advancements in intrusion detection systems, which will further enhance network security and mitigate the risks associated with cyber threats..

REFERENCES

[1]. Krishna, A. Mohan, and Amit Kumar Tyagi. "Intrusion detection in intelligent transportation system and its applications using blockchain technology." In 2020 international conference on emerging trends in information technology and engineering (IC-ETITE), pp. 1-8. IEEE, 2020.

[2]. Ferrag, Mohamed Amine, MakhloufDerdour, Mithun Mukherjee, AbdelouahidDerhab, LeandrosMaglaras, and Helge Janicke. "Blockchain technologies for the internet of things: Research issues and challenges." IEEE Internet of Things Journal 6, no. 2 (2018): 2188-2204.

[3]. Amine Ferrag, Mohamed, MakhloufDerdour, Mithun Mukherjee, AbdelouahidDerhab, LeandrosMaglaras, and Helge Janicke. "Blockchain technologies for the internet of things: research issues and challenges." arXiv e-prints (2018): arXiv-1806.

[4]. Li, Wenjuan, Yu Wang, Jin Li, and Man Ho Au. "Towards blockchained challenge-based collaborative intrusion detection." In Applied Cryptography and Network Security Workshops: ACNS 2019 Satellite Workshops, SiMLA, Cloud S&P, AIBlock, and AIoTS, Bogota, Colombia, June 5–7, 2019, Proceedings 17, pp. 122-139. Springer International Publishing, 2019.

[5]. Hui, Hongwen, Xingshuo An, Haoyu Wang, Weijia Ju, Huixuan Yang, Hongjie Gao, and Fuhong Lin. "Survey on Blockchain for Internet of Things." J. Internet Serv. Inf. Secur. 9, no. 2 (2019): 1-30.

[6]. Signorini, Matteo, Matteo Pontecorvi, Wael Kanoun, and Roberto Di Pietro. "BAD: A blockchain anomaly detection solution." IEEE Access 8 (2020): 173481-173490.

[7]. Benaddi, Hafsa, and Khalil Ibrahimi. "A review: Collaborative intrusion detection for iot integrating the blockchain technologies." In 2020 8th International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 1-6. IEEE, 2020.

[8]. Arshad, Junaid, Muhammad Ajmal Azad, RoohiAmad, Khaled Salah, MamounAlazab, and Razi Iqbal. "A review of performance, energy and privacy of intrusion detection systems for IoT." Electronics 9, no. 4 (2020): 629.

[9]. Arshad, Junaid, Muhammad Ajmal Azad, RoohiAmad, Khaled Salah, MamounAlazab, and Razi Iqbal. "A review of performance, energy and privacy of intrusion detection systems for IoT." Electronics 9, no. 4 (2020): 629.

[10]. He, Debiao, Kim-Kwang Raymond Choo, Neeraj Kumar, and Aniello Castiglione. "IEEE access special section editorial: Research challenges and opportunities in security and privacy of blockchain technologies." IEEE Access 6 (2018): 72033-72036.

[11]. Arshad, Junaid, Muhammad Ajmal Azad, RoohiAmad, Khaled Salah, MamounAlazab, and Razi Iqbal. "A review of performance, energy and privacy of intrusion detection systems for IoT." Electronics 9, no. 4 (2020): 629.

[12]. Salman, Tara, Raj Jain, and Lav Gupta. "Probabilistic blockchains: a blockchain paradigm for collaborative decision-making." In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 457-465. IEEE, 2018.

[13]. Salman, T., R. Jain, and L. Gupta. "Probabilistic blockchains: A blockchain paradigm for collaborative decision-making. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)(pp. 457-465)." (2018).

[14]. Al-E'mari, Salam, Mohammed Anbar, Yousef Sanjalawe, Selvakumar Manickam, and IznanHasbullah. "Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges." Computer Systems Science & Engineering 40, no. 1 (2022).s

[15]. Hasbullah, Iznan. "Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges."

[16]. Shreevyas, H. M., CR Suthikshan Kumar, Pune DIAT-DRDO, Ruhin A. Shaikh, BG ACU, and IN KA. "Can Blockchain technology be the future of network intrusion detection system: A review." International Journal of Applied Engineering Research 14, no. 15 (2019): 10179-10187.

[17]. Al-E'mari, Salam, Mohammed Anbar, Yousef Sanjalawe, Selvakumar Manickam, and IznanHasbullah. "Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges." Computer Systems Science & Engineering 40, no. 1 (2022).

[18]. Meng, Weizhi, Elmar Wolfgang Tischhauser, Qingju Wang, Yu Wang, and Jinguang Han. "When intrusion detection meets blockchain technology: a review." Ieee Access 6 (2018): 10179-10188.

[19]. Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where is current research on blockchain technology?—a systematic review." PloS one 11, no. 10 (2016): e0163477.

[20]. Xie, Junfeng, Helen Tang, Tao Huang, F. Richard Yu, RenchaoXie, Jiang Liu, and Yunjie Liu. "A survey of blockchain technology applied to smart cities: Research issues and challenges." IEEE communications surveys & tutorials 21, no. 3 (2019): 2794-2830.

[21]. Mishra, Lokanath, and Vaibhav Kaushik. "Application of blockchain in dealing with sustainability issues and challenges of financial sector." Journal of Sustainable Finance & Investment (2021): 1-16.

[22]. Fernández-Caramés, Tiago M., and Paula Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things." Ieee Access 6 (2018): 32979-33001.

[23]. Zhao, Guoqing, Shaofeng Liu, Carmen Lopez, Haiyan Lu, Sebastian Elgueta, Huilan Chen, and Biljana MilevaBoshkoska. "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions." Computers in industry 109 (2019): 83-99.

[24]. Wamba, Samuel Fosso, and Maciel M. Queiroz. "Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities." International Journal of Information Management 52 (2020): 102064.

[25]. Leible, Stephan, Steffen Schlager, Moritz Schubotz, and Bela Gipp. "A review on blockchain technology and blockchain projects fostering open science." Frontiers in Blockchain (2019): 16.