VAWKUM Transactions on Computer Sciences
http://vfast.org/journals/index.php/VTCS@ 2023 ISSN(e): 2308-8168, ISSN(p): 2411-6335
Volume 11, Number 1, January-June 2023 *pp: 138-151*

A Survey on Blockchain-based Intrusion Detection Systems for IoT

Jawad Hassan[1], **Muhammad Kamran Abid**[2], **Mughees ahmad**[1], **Ali Ghulam**[3], **Muhammad Salman Fakhar**[4], **Muhammad Asif**[5]

[1]Department of Computer Science and Engineering, Air University Multan Campus, Pakistan; [2]Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan; [3]Information Technology Centre, Sindh Agriculture University, Sindh, Pakistan; [4]Directorate of IT, BZU, Multan, Punjab, Pakistan; [5]Department of CS and IT, The Isalmia University of Bahawalpur, Pakistan

Keywords: *Internet of Things, Security, Intrusion Detection Systems, Blockchain, DDoS and CyberSecurity*

Journal Info:
Submitted:
January 15, 2023
Accepted:
April 16, 2023
Published:
May 2, 2023

Abstract The Internet of Things (IoT) is a contemporary concept that unifies the Internet and physical objects across various domains, such as home automation, manufacturing, healthcare, and environmental monitoring. This integration enables users to leverage Internet-connected devices in their daily routines. Despite its numerous advantages, IoT also presents several security challenges. As the popularity of IoT continues to grow, ensuring the security of IoT networks has become a critical concern. While encryption and authentication can enhance the security of IoT networks, protecting IoT devices against cyber-attacks remains a complex task. A successful cyber-attack on an IoT system may not only result in information loss but also potentially cripple the entire system. Intrusion detection systems (IDS) are instrumental in identifying malicious activities that could compromise or disrupt network performance. Consequently, there is a pressing need for effective IDS solutions to safeguard IoT systems. Blockchain, an emerging technology, bolsters security systems to counter modern threats. In this paper, we provide an extensive review of state-of-the-art blockchain-based intrusion detection systems for IoT applications. Additionally, we present recent advancements in addressing security concerns in a tabular format. Lastly, we identify open challenges and current limitations that warrant further exploration.

***Correspondence Author Email Address:**
jawadhassan521@gmail.com; garahu@sau.edu.pk

1 Introduction

The Internet of Things (IoT) has emerged as a critical technological, social, and economic topic in recent years. This domain encompasses consumer products, durable goods, engines, vehicles, commercial and

application components, sensors, and various standardized objects, all integrated with internet connectivity and advanced analytical capabilities. These advancements promise to transform the way we work, live, and play. IoT represents an intelligent network wherein all objects are interconnected via the internet, employing agreed-upon protocols for information exchange [1]. This connectivity enables access to any object within the IoT network at any time and from any location [2]. Wirelessly connected through sophisticated and compact sensors, IoT devices do not require human intervention for interaction [3]. Unique addressing is utilized by IoT to facilitate communication between objects within a network. A wide range of applications, such as health monitoring, smart water management, and smart environments, have emerged as a result of IoT advancements [4]. IoT encompasses numerous diverse applications that bridge the physical and cyber realms, with a focus on integrating smart objects and the internet. These solutions include not only simple smart home devices but also industrial plant equipment and a myriad of other everyday items. While the objectives of various IoT applications may differ, they share several characteristics. IoT operations are based on 3 primary phases outlined below [5].

- COLLECTION PHASE
- TRANSMISSION PHASE
- PROCESSING MANAGEMENT AND UTILIZATION PHASE

1.1 Collection Phase

The collection of physical environment data is the primary purpose of the collection phase.Data gathering is made possible by incorporating multiple sensors with short-range communications technology. The devices employed in this process are often modest and a source of energy.Communication protocols and technologies have restricted data rates and short distances during this stage, with limited memory space and low power consumption, which is why these networks are known as LLNN (Low-power and Lossy Networks).

1.2 Transmission Phase

The data gathered in the transmission process, the collection stage is transmitted to applications and users. To construct a network, technologies such as Wireless Subscriber Line (DSL), WiFi, Hybrid Fiber Coaxial (HFC), and Ethernet are combined with TCP/IP protocols, connecting these items and users to this network. Using Gateways, the LLN selection phase protocols and traditional Internet protocols in this phase are combined.

1.3 Processing Management and Utilization Phase

The collected data is analyzed in this step to obtain useful physical environment information. Depending on this knowledge, these applications can make decisions and can control the physical objects of the physical environment.

Middle-ware is used in this stage to promote the integration and communication between various multi-platform apps and physical things. There are some characteristics of the Internet of Things given below.

1.3.1 Confidentiality

When a sender sends a message to a receiver, an attacker or malicious user can easily intercept that message, so that the confidential data can be leaked and an attacker can also modify the content. [6]. So that security is needed for a message to pass in IoT.

1.3.2 Integrity

The sent mail should be the same as it is sent from the sender to the recipient, it shouldn't be altered during communication of the message. Integrity ensures that mail has now no longer been altered through unauthorized communication during the time of transmission [8].

1.3.3 Availability

Data and all the resources of the system should be available whenever they are required [8]. Attackers will launch a DOS attack to flood the resource bandwidth to damage availability. Data and resource availability may be affected by attacks such as DOS attacks, black holes, flooding, and jamming attacks, etc.

1.3.4 Authenticity

Authentic offers identifying proof [9]. Clients who are communicating with one another must be able to recognise one another. The verification process, which prohibits unauthorised users from utilising the network, serves as evidence of this [10].

1.3.5 Non- Repudiation

Non-repudiation is a property that guarantees that after sending and receiving the message, the sender and recipient will not reject or deny it [11].

1.3.6 Data Freshness

This is the property that ensures that the data is updated or recent whenever it is needed. It ensures that an adversary does not replay any old messages [12].

The three main layers of the architecture of the IoT system are shown in Figure 1.

1.3.7 Perception Layer

This layer is the basic or main IoT layer. All types of data of the IoT environment are collected and observed in this layer. RFID, Sound sensors, camera, temperature sensors, GPS, etc. can be used to collect the information [13]. The layer of sensation consists of two parts. 1. The perception node: This is used to control data. 2. The perception network: This is used to submit the controller data [14].

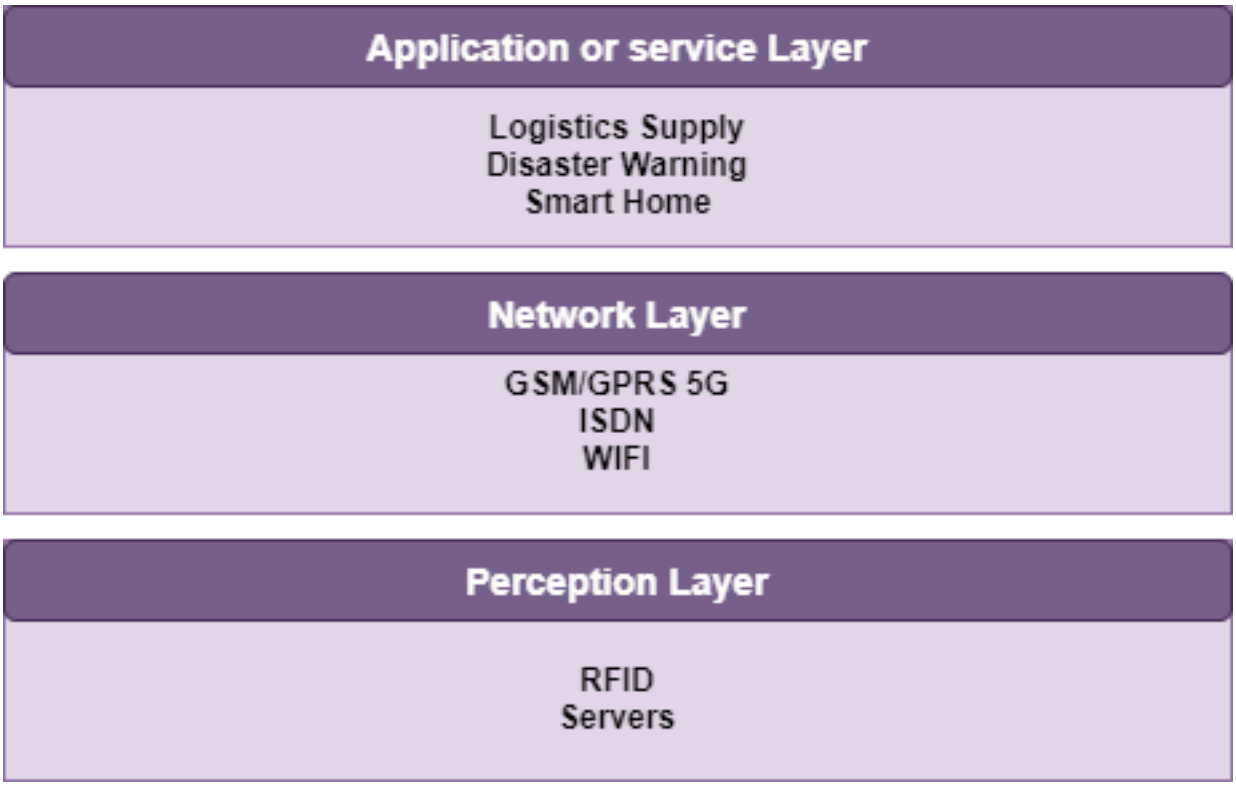

Figure 1. Layers of IoT.

1.3.8 Network Transportation Layer

The transport layer is another name for this. This layer is capable of transferring data from the higher towards bottom layers [13]. The data or data may also be transmitted over the internet through this layer. So the various heterogeneous networks can be combined in this layer [14].

1.3.9 Application (Service) Layer

The service layer is another name for this layer. In addition to giving end users a user interface (UI), this is utilised to transform information into valuable data. This layer's main problem is the secure exchange of information with other users so that no malicious user or unauthorized user can read or alter this information [13].

2 Attacks on Internet of Things

In this section, we'll discuss cyber-attacks that can occur on IoT applications. These attacks may be internal and also external attacks. In external attacks, the attacker is usually not part of the internal network but instead uses some compromised or malicious insider node to initiate the attack.

2.1 Sinkhole Attack

A malicious or compromised node attracts all the traffic towards itself in this attack. To draw all surrounding connections to send their packets to the malicious node, this malicious node shows that its cost of routing is negligible. For attacking the network an attacker introduces the false node inside the network [15].

2.2 Wormhole Attack

In Wormhole Attack, an opposing node formed an electronic canyon between ends. An opposing node, between actual nodes, serves as a forwarding node. Typically, the malicious nodes announce they could be away from one hop from the base station. In this attack, it can also convince by relaying packets they might be familiar with these nodes [14, 15].

2.3 Selective Forwareded Attack

The node which is devious starts behaving as a normal node and drops selective packets in this attack [6].However, in the Various attacks, the rogue node discarded all of the transmissions instead of just a few.

2.4 Sybil Attack

The node has more than one identity in this Sybil attack. The routing protocol, cooperation strategies, and prevention set of rules get attacked with the help of a malicious node [15].

2.5 Hello Flood Attack

The routing protocol emits a hello message on a sensor network to signal its presence to its neighboring nodes. In addition, a node that gets the hello message can anticipate that the node source is in its range and that node source is added to its list of neighbors [16].

2.6 Denial of Service (DOS) Attack

This is the most common attack that can occur on IoT. It normally damages the availability of resources. When an attack starts, authorized users no longer have access to data and services. When this kind of attack is initiated from different nodes this is called a DDOS attack. Network resources, CPU time, bandwidth, etc. can be affected by this kind of attack.

3 Intrusion Detection System

Intrusion detection is the method of identifying malicious acts that are carried out against the network systems by an attacker or intruder. These acts are called intrusions; they are aimed at obtaining unauthorized network access. There are two kinds of intruders internal and external, internal intruders are those intruders who are part of a network and they attempt to gain access to the privileges of legitimate users to misuse non-authorized privileges. External intruders attempt to obtain unauthorized access to device information outside the targeted system or network [17, 18]. IDS consists of sensors, a reporting system, and an analysis engine. Sensors can be placed in different positions or places in a network depending on the requirements of a network. They collect data from the host or network, data include packet headers, traffic statistics, service requests, file-system changes, and operating system calls. This information is collected by the sensors and then sent to the analysis engine to look over the data gathered to identify ongoing intrusions. The reporting mechanism produces a warning on a network when a malicious user intrudes the system. Intrusion is unauthorized or malicious traffic to sensitive nodes that are hazardous. IDS is a program system and many applications. IDS can look at and check machines and user behavior, find signatures of popular attacks, and interpret malicious network activity. IDS aims to look at the networks and also network's nodes, it detects various intrusions in the network, if there is any intrusion it also warns the nodes about this intrusion. The IDS usually plays an important role as an alarm or observer of a network it can prevent the system from the attack before an attack. It can come across each inner and outside assault. Internal assaults are released through compromised nodes that are related to the community while outside assaults are released through 1/3 events that are initiated outside of the network. IDS come across the packets in a network and decide whether or not they're intruders or legitimate users. IDS usually consists of three components Monitoring, Analysis, and detection, Alarm [19]. There are mainly two kinds of IDS Host-based IDS and Network-based IDS.

3.1 Host-Based IDS

Host-based IDS are designed specifically for hosts and they scan logs and audit records to detect the intrusion or malicious behavior. Host-based IDS usually protects the critical nodes or hosts from all types of malicious users whether they are insider or outsider intruders. Host-based IDS are very beneficial because they provide detailed information and decrease false alarm rates. Host-based IDS are less complex than network-based IDS. This reduced the efficiency of the system and it relied heavily on the host's log data and its capability to monitor [20, 21].

3.2 Network-Based IDS

As all the IoT are usually connected to a network so for IoT devices network-based IDS detect any kind of intrusion. For detecting intrusions, network-based IDS are used to identify suspicious activity and data flow in the network. Network-based IDS does not alter the configuration of the host, and it also does not affect the network effectiveness.Additionally, even if the network IDS stops working, the business process is unaffected. However, Network-based IDS has one drawback: rather than inspecting other network segments, it only checks the segment's direct connection. It is also very tough to understand the sessions which are anonymized in network-based IDS [22]. There are so many approaches for IDS in the Internet of Things. Some of them are described in this section [45].

3.2.1 Signature Based Approaches

In this approach, IDS detect based on signatures stored in IDS internal databases by matching these signatures. After matching some device or network behaviors with stored patterns/signatures, an alarm is generated. But this method is not used to detect new attacks [34, 35].

3.2.2 Fule-based Approaches

Chen Jun [36] suggested an IDS-based event processing system that solves the issue of IDS real-time in the IoT network. In their approach, they used Event Processing Model (EPM) to design the IDS. It is a rules-

based IDS Rule Pattern Repository that is stored and takes Epser's SQL and EPL for reference. It requires less processing time than conventional IDS for this technique.

3.2.3 Anomaly based Approaches

Anomaly-based methods are the most common method, it depends on the identification of malicious patterns and by the comparison of patterns of traffic. The advantage is that new and unknown intrusions can be detected by using this approach. But the main disadvantage of this approach is that it results in high false-positive rates.

3.2.4 Hierarchical Energy Efficient Based Approaches

Samir Athmani [37] WSN recommends a new approach, the hierarchical power IDS implemented in the NS2 network simulator for the detection of black hole attacks. In this approach, the base station and sensor node at a time replace the previous control packet. The number of node IDs and packets sent to the cluster header is found in any control packet. To detect black hole attacks, the base station works in monitor mode. Less energy is used, from this point of view, to suggest interference. They do not guarantee that the proposed approach will be capable of detecting all kinds of black hole attacks, but it will mitigate these attacks.

3.2.5 Specification-Based Approaches

This approach is a collection of rules and thresholds to determine how a part of the network should function, such as nodes, protocols, and routing tables. When network activity detracts from expected behavior or unique rules are established, the intrusion is detected. The rules are manually specified by human experts in specification-based approaches [**?**]. Manually defined specifications help in lowering the false-positive rates in comparison to anomaly-based detection [34, 44]. These systems don't need to be trained but can begin working after manually defining the rules.

3.2.6 Hybrid Approaches

Hybrid approaches combine signature-based approach, anomaly-based approach, and specification-based detection which helps in maximizing the efficiency of intrusion detection for IoT devices. The hybrid approach can combine any of the above-mentioned techniques to detect intrusion in an IoT network. This approach has the advantage of minimizing the limitations of an approach when combined with other approaches, but on the other hand, this will require more resources to work properly and efficiently particularly when so many protocols operate entirely on the IoT network for the detection of intrusion in the system. IDS requires more resources for working efficiently.

4 Blockchain Based Intrusion Detection Systems in IoT

Li et al. presented a block-chain information protection model based on IDS Technology on the Internet of Things in this paper. For the defense of block-chain information security, they apply IDS technology and they also evaluate detection technology which is usually based on different models. Similarly, they also analyze the combination of things and block-chain. As the Internet of Things continues to expand and it is difficult to deploy they first deploy Internet of Things as subject, the ecological system was then connected to the industry and eventually developed. For the implementation of artificial intelligence, block-chain is used, and intelligent contracts are automated, sophisticated, and complicated. Improving and implementing the block-chain age has had a critical influence around the world, and more and more accomplishments have been made [21]. A block-chain, multi-agent system, and machine learning-based intrusion detection system were suggested by the authors in[22].

In this paper, they have discussed in detail the work mode of each model component and its function. Thanks to the versatility of multi-agent systems, these new IDS are usually used in IoT environments in different dimensions. To ensure that the system is safer from information falsification, leakage of information, and other blockchain risks, all acts by communicators are documented. A multi-agent strengthening

algorithm is used in their system to continuously improve their efficiency. The results of their experiments demonstrate the usability of this SESS device at various IoT network levels. This system detects and reacts to attacks in real-time because the detection time is 0.18 s. The timing is documented through the initialization and loading of data models, time, and detection. This timing can also be entirely different on several occasions like hardware, various server properties, reminders, etc. Similarly, these calculations aim to ensure that the suggested version can be carried out in an area with high-speed stays. The results from such experiments can then be used to determine the status of the multi-agent enhancement process. In this article, neural network implementations will also be discussed. Experiments show that deep learning algorithms operate more efficiently in the same IoT network than conventional approaches. This system may be distributed to various remote host systems using blockchain technology since the blockchain allows ACL communication more secure and smart contract modular communication between the agents. The use of the NSL-KDD data set in experiments indicates an unreasonable detailed detection of an intrusion at the IoT-environment transport layer for DNN. The total output of the DNN version in the isolation of anomalies from standard devices is higher than that of various methods, which involve decision-making bodies. This demonstrates the ability to use IoT computer IDS deep learning algorithms. The tests show a high overall machine efficiency in different situations, including networks of varying complexity and attacks. The study will concentrate on multi-agent technology, blockchains, and neural networks to provide an IoT model for an intrusion detection system. In their future work, they defined the improvement of the modules of their system to allow every agent to operate well together [22]. An IDS technique based on a distributed evaluation of the confidence score was introduced by Ambili et al. It demonstrates that it is not easy to evade IDS if IDS uses blockchain history to verify the trust values. The transaction of the manipulated confidence score does not recognize this method. Furthermore, 51% attack in a consensus-based on evidence-of-work, whereby a plurality will take ownership of the blockchain. As a consequence of the collapse of the system of consensus, there are other assaults. In the current work, the out-of-band wormhole has not been considered, because it is beyond the network [23].

Putra et al formulate a decentralized IoT CIDS scheme based on blockchain technology. They have an accountable trust mechanism that encourages rewards and punishments and scalable storage of data on intrusion through the exchange of bloom filters. They introduce a modular design proof in a local trial site for typical attacks in IoT networking and the associated overhead. It tests the feasibility of this proof of theory. In this post, they have used intruders' adaptive blockchain behavior, from which they can evaluate their intrusion behavior. The crucial component of intrusion analysis is power consumption. This proposed framework is referred to as LVRS with a different layer.Three layers—a positive layer, a negative layer, and a propagating layer—are present in the paper that employs energy usage. The number of processing is the first stage, contour functions are used in the second step, and then a linear quad architecture is used for data transfer. LVRS improves the method for identification further in the next step. Based on preaching data generated via a transaction total power consumption, LVRS analyzes user behaviors. The paper introduces a special voter rule which helps to analyze the network for intrusion scanning.Blockers are enforced and data is analysed through breakpoints using the simulation's 100 window size. A total of five hundred magazines are evaluated based on throwback and strength. The gasses and power usage vary substantially by more than 30% [34].

In this system, Li et al advocated the use of blockchains centred on signature-based identification and the creation of CBSigIDS, a standardised framework for cooperative blockchain signature-based IDSs that will aid in the sharing and evolutionary construction of a reliable data store. Their research shows that under hostile circumstances (such as flooding attacks), CBSigIDS can boost the strength and efficiency of signature-based detection because signatures are transferred in a verifiable manner. Their proposed system is an early research study in this field, which demonstrates how to use blockchains to boost the efficiency of IDSs based on collective signatures. Future work includes creating a stable IDS system for anomalous detection across the blockchain and designing a robust mechanism to protect IDS nodes from advanced internal attacks [25].

Authors in [26] proposed the distributed community-detected blockchain detection model based on the Propose-Select-Adjust (PSA) paradigm. This PSA algorithm works asymptomatically and also refers to the study of the data in the sub-network to define structural entropy communities. Results of their studies

show how the algorithm operates efficiently and detects group structures within complex Bitcoin trust networks successfully. It draws many assailants to itself due to the independent capacity of blockchain. These assaults bypass the IDS. Inspired by the rapid improvement and development of blockchain, the authors have suggested a CIDN architecture that takes advantage of the advantages provided by a blockchain. In its structure, the knots shape a consortium chain that enhances the functioning and robustness of CIDNs that are based on the task.

The results show that their system improves the strength and stability of CIDNs in managing trust by recognizing advanced malicious nodes and aggregating alarms, detecting invasive information, and reducing error rates [28]. Their framework was tested both under random toxicity and SOOA attacks. The author suggested a CIDS model based on blockchain technology for a signature invasion detection system. The use of CIDS-based blockchain helps address existing issues of CIDS, including confidentiality and consensus-building, and facilitates the exchange of signatures, formation between hosts and CIDS, improving the efficiency and performance of IDS . In[29] response to current concerns of conventional IDS, Alexopoulos et al. [30] suggested a blockchain-based CIDS.

In response to current concerns of conventional IDS, Alexopoulos et al. [30] suggested aCIDS that is based on blockchain. Blockchain technology is used to improve or improve the management of the trust among IDS nodes. They have used raw alerts that can be replicated among a CIDN's nodes by IDS nodes as a transaction in the blockchain technology. After that, all these nodes begin to enforce a consensus protocol to ensure that the transaction is validated. All these operations guarantee the temperature resistance of the alerts produced and stored in the blockchain. The authors of this paper have introduced a new blockchain-based CID approach without any trusted or central third-party intervention for the detection of distributed intrusion in MMG systems. This system guarantees the accuracy and non-reputability of IDS outcomes in the micro-grid during the process of distributed data transmission. In all three ways, this paper is novel.

Firstly, this is a modern CID approach for MMG systems, which incorporates consensus and rewards in the blockchain. Secondly, by developing a multi-pattern proposal generation process, the FNR of intrusion detection is reduced. Third, one richest member's defect prevails through the implementation of an improved DPoS algorithm [31].While the recent major contributions in this area of study is shown in the Table 1.

5 Challenges and Limitations

Blockchains Intrusion detection and blockchains complement one another. By using blockchain technology, When considering CIDS, the performance of IDS can be improved, especially in terms of data exchange and trust measurement. However, it can also be useful to identify meddling in blockchain transactions.This is close to the detection of fraud in credit card systems. Pham and Lee [41] developed a framework for the detection of an anomaly as a proxy for the detection of suspicious customers or incidents. On the other side, though, there are certain difficulties and problems. Intrusion detection has long been investigated, but in real-world implementations, there are still many issues that will probably affect detection performance [42].

5.1 Overhead Traffic with limited Handling Capability

Detection of these overhead packets will considerably reduce the efficiency of a detection system in an area where heavy network traffic is present. Many network packets must be dropped if traffic reaches the maximum IDS processing power. The calculation burden, for example, is linear in the size of the payload package [43].

5.2 Limited Signature Coverage

The capacity to detect cryptography detections depends greatly on the signatures that are currently in use. As a result, the effectiveness of the deployed signatures' quantity and constancy determines how well they

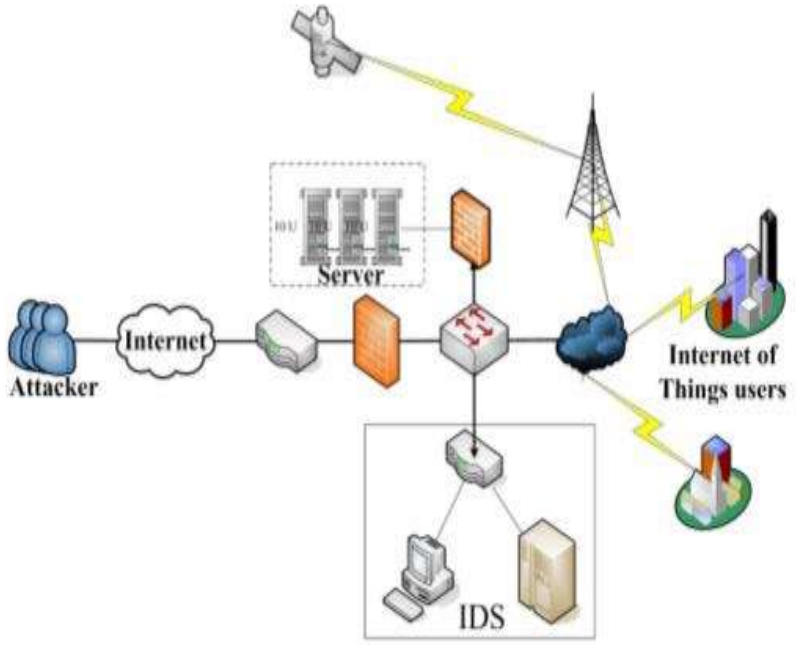

Figure 2. Blockchain-based IDS

Table 1. Recent Contributions

Year	Reference	Approach	Outcome
2020	[22]	Multi-agent Block-chain based IDS and Deep Learning	This new IDS is can be used in IoT environments in different dimensions. To ensure that the system is safer from many threats.
2020	[23]	Block-chain IDS based on Trust Score	This Intrusion detection system based on trust score evaluated in a distributed way make infringement difficult.
2019	[24]	Block-chain-based CIDS	This framework provides accountable trust establishment, which promotes incentives and penalties, and scalable intrusion information storage by exchanging bloom filters.
2019	[25]	Collaborative Block-chain based CBSigIDS	CBSigIDS can enhance the robustness and effectiveness of signature-based detection under adversarial scenarios (e.g., flooding attacks) because signatures are shared in a verifiable way
2018	[26]	Propose-Select-Adjust (PSA) based distributed community detection model for block-chain	PSA algorithm performs efficiently and is successful in detecting community structures within dynamic Bitcoin trust networks.
2019	[28]	Propose-Select-Adjust framework (PSA) based distributed community detection model for block-chain	It enhances the robustness of CIDNs in trust management by detection of advanced malicious nodes, and alarm aggregation.
2019	[29]	Block-chain-based CIDN	This block-chain-based CIDS enhances and improves the efficiency and performance of IDS.
2019	[30]	Block-chain -based Signature-based IDS	This IDS improved the management of the trust among IDS nodes
2019	[31]	Block-chain -based CIDS for Micro-grid	The FNR of intrusion detection is reduced
2020	[46]	RDTIDS for IoT	It increases the accuracy, detection rate, false alarm rate, and time overhead as compared to existing schemes

may be detected.But signatures frequently have limitations and cannot offer complete protection from all known threats and weaknesses.

5.3 Inaccurate Profile Establishment

Due to the unpredictable nature of traffic, it is difficult to create an exact normal profile for anomaly-based detection. More precisely, to create a profile, an anomaly-based IDS also leverages machine learning techniques. In practice, however, training data, especially labeled attack data, is very small, resulting in an inaccurate classifier for machine learning.

5.4 Massive False Alerts

Effective IDS can produce accurate warnings to notify security administrators of information about all forms of network irregularities or intrusions. False alarms, nonetheless, constitute a severe IDS detection issue. Wrong profiles and underdeveloped signatures may be the key explanation for false alarms, potentially leading to a decrease in IDS output and an increase in the workload of safety analysts. Blockchain software is emerging, but as seen in Figure 4, it still has some problems that are still unresolved.

5.5 Energy and Cost

Model needs capability is a concern with the use of the blockchain [44]. If we take Bitcoin mining as an example, it needs a high amount of power to calculate and validate investments. In [20] Wang and Liu discovered that firstly, the computing energy was applied to single miners, but it continues to increase as the network has grown.

5.6 Security and Privacy

Blockchain technology is vulnerable to many attacks because it attracts many cyber-criminals and different types of attacks such as DOS can occur on the blockchain. Blockchain implementations need smart transactions which need to be connected to established identities, creating some shared ledger data protection and privacy issues.

5.7 Latency and Complexity

Blockchain-based transactions require many hours to complete until all of the parties have updated the ledger because of the distributed nature of blockchain. This can cause the opening of a hole for attackers and it will also create much uncertainty for transaction participants.

6 Awareness and Adoption

Many people are still unaware of the usage of blockchain technology. Lack of awareness and adoption will define future development of blockchain.

6.1 Organization and Size

As Organizations are of different sizes, some are so big that if they use the blockchains and standards this will lead to the degradation of the performance blockchains would potentially be less usable than current systems.

6.2 Regulations and Management

There are no such general requirements for completing block-chain transactions, so for better performance, the Bitcoin block-chain does not obey current regulations. But according to the rules, block-chain implementations are anticipated to work.

7 Conclusions and Future Work

In this paper, we surveyed the blockchain based intrusion detection systems to ensure the security of IoT applications. The use of IoT is increasing day by day, but it has posed so many concerns along with the growth of IoT. We mentioned several attacks that can occur on IoT devices and we also presented different approaches to intrusion detection based on blockchain that can be used to mitigate those attacks. However, there are still certain difficulties and restrictions with various IDS methods. Since blockchain-based IDS needs more computing power, memory, and bandwidth for intrusion detection, these are open challenges which need to be addressed.

Author Contributions

Jawad Hassan: Conceptualization, Methodology and Software implementation, **M**uhammad Kamran Abid: Software implementation, Data curation, **M**ughees Ahmad work has been Validation and Writing- **A**li Ghulam has wrote the Original draft preparation and Visualization, Investigation then **M**uhammad Salman Fakhar and **M**uhammad Asif: Writing- Reviewing and Editing in the paper.

Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest. It is also declare that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

Author Information

ORCID:
Ali Ghulam: 0000-0001-5166-2213

References

[1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," IEEE Internet Things J., vol. 1, no. 4, pp. 349–359, 2014.

[2] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," IEEE Internet Things J., vol. 1, no. 4, pp. 349–359, 2014.

[3] S. Li, L. D. Xu, and S. Zhao, The internet of things: a survey", vol. 17. Springer Information Systems Frontiers, 2015.

[4] P. G. S. Sreeram and C. M. R. Sivappagari, "Development of Industrial Intrusion Detection and Monitoring Using Internet of Things"," International Journal of Technical Research and Applications, 2015.

[5] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Comput. Commun., vol. 54, pp. 1–31, 2014.

[6] M. Patel and A. Aggarwal, "Security attacks in wireless sensor networks: A survey"," in 2013 International Conference on Intelligent Systems and Signal Processing, 2013.

[7] L. Clemmer, "Information Security Concepts: Authenticity." ,2020.

[8] Brighthub.com. [Online]. Available: http://www.brighthub.com/computing/smb-. [Accessed: 16-Feb-2023].

[9] "Review on Network Security and Cryptography"," International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1, pp. 1–11, 2015.

[10] V. Mrs, D. Umadevi Chezhian, and M. Ramar2, "Security Requirements in Mobile Ad Hoc Networks," International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 2, pp. 45–49, 2012.

[11] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in 2015 IEEE World Congress on Services, 2015.

[12] S. Nabil Ali Alrajeh and B. Khan, "Intrusion Detection Systems in Wireless Sensor Networks: A Review"," International Journal of Distributed Sensor Networks, vol. 2013, 2013.

[13] X. Jia, Q. Feng, T. Fan, and Q. Lei, RFID technology and its applications in Internet of Things (IoT)", 2nd International Conference on Consumer Electron- ics, Communications and Networks (CECNet). 2012.

[14] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Springer journal of Mobile Communication, Computation and Information," vol. 20, pp. 2481–2501, 2014.

[15] C. Okan and O. Koray, "Survey of Intrusion Detection Systems in Wireless Sensor Networks," in 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015.

[16] R. Abdur Rahaman Sardar, M. Ranjan Sahoo, and S. Singh, "Jamuna Kanta Singh, and Koushik Majumder, "Intelligent Intrusion Detection System in Wireless Sensor Network," in Proc. Of the 3rd Int. Conf. on Front. Of Intell. Comput. (FICTA), vol. 2, Springer, 2014.

[17] J. Vacca, "A survey of intrusion detection and prevention systems," in Information Management Computer Security, vol. 18, Q. Qassim and C. Wills, Eds. Morgan Kaufmann, 2010, pp. 277–290.

[18] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," Inf. Manage. Comput. Secur., vol. 18, no. 4, pp. 277–290, 2010.

[19] P. Zegzhda and S. Kort, "Host-based intrusion detection system: Model and design features," in Communications in Computer and Information Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 340–345.

[20] S. S. Chakravarthi and S. Veluru, "A review on intrusion detection techniques and intrusion detection systems in MANETs," in 2014 International Conference on Computational Intelligence and Communication Networks, 2014.

[21] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "RETRACTED ARTICLE: Information security model of block chain based on intrusion sensing in the IoT environment," Cluster Comput., vol. 22, no. S1, pp. 451–468, 2019.

[22] C. Liang et al., "Intrusion detection system for the Internet of Things based on blockchain and multi-agent systems," Electronics (Basel), vol. 9, no. 7, p. 1120, 2020.

[23] K. N. Ambili and J. Jose, "Trust based intrusion detection system to detect insider attacks in IoT systems," in Lecture Notes in Electrical Engineering, Singapore: Springer Singapore, 2020, pp. 631–638.

[24] F. I. Conference and R. S. Papers, Big Data , Machine Learning , and Applications. 2019.

[25] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," Future Gener. Comput. Syst., vol. 96, pp. 481–489, 2019.

[26] Y. Chen and J. Liu, "Distributed community detection over blockchain networks based on structural entropy," in Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, 2019.

[27] S. Kim, B. Kim, and H. J. Kim, "Intrusion detection and mitigation system using blockchain analysis for bitcoin exchange," in Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things, 2018.

[28] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Poster abstract: Towards scalable and trustworthy decentralized collaborative intrusion detection system for IoT," in 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI), 2020.

[29] D. Laufenberg, L. Li, H. Shahriar, and M. Han, "An architecture for blockchain-enabled collaborative signature-based intrusion detection system," in Proceedings of the 20th Annual SIG Conference on Information Technology Education, 2019.

[30] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivanko, and M. Muhlhauser, "'Towards blockchain-based collaborative intrusion detection systems," in Proc. Int. Conf. Critical Inf. Infrastruct. Secur, 2017, pp. 1–12.

[31] B. Hu, C. Zhou, Y.-C. Tian, Y. Qin, and X. Junping, "A collaborative intrusion detection approach using blockchain for multimicrogrid systems," IEEE Trans. Syst. Man Cybern. Syst., vol. 49, no. 8, pp. 1720–1730, 2019.

[32] Salman, T., Zolanvari, M., Erbad, A., Jain, R., Samaka, M., Security services using blockchains. IEEE Commun. Surv. Tutor. 21(1), 850–880.

[33] 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.

[34] J. Vacca, Computer and information security handbook. Amsterdam: Morgan Kaufmann, 2013.

[35] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.

[36] C. Jun and C. Chi, "Design of Complex Event-Processing IDS in Internet of Things"," in Sixth International Conference on Measuring Technology and Mechatronics Automation, 2014.

[37] S. Athmani, D. E. Boubiche, and A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," in 2013 World Congress on Computer and Information Technology (WCCIT), 2013.

[38] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for CyberPhysical Systems," ACM Computing Surveys (CSUR), vol. 46, no. 4, 2014.

[39] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, and L. Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks," in 2014 IEEE International Conference on Communications (ICC), 2014.

[40] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Commun. Surv. Tutor., vol. 16, no. 1, pp. 266–282, 2014.

[41] W. W. Are, "arxiv.org e-Print archive," arXiv.

[42] W. Meng, W. Li, and L.-F. Kwok, "'EFM: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism,.'" Comput. Secur., vol. 43, pp. 189–204,.

[43] E. Ben-Sassonetal, "Zerocash: Decentralized anonymous payments from bitcoin," in Proc. IEEE Symp. Secur. Privacy (SP), Berkeley, CA, USA, 2014, pp. 459–474.

[44] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review,'. 'PLoS ONE, vol. 11, no. 10, p. e0163477, 2016.

[45] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," J. Netw. Comput. Appl., vol. 84, pp. 25–37, 2017.

[46] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks," Future Internet, vol. 12, no. 3, p. 44, 2020.