International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 15 Issue 02 Year 2023

IoT Protection Against Cyber Threats Based on Blockchain and Access Control: A Comprehensive Review

Nora Alwasil
Master, Department of Information Technology, College of Computer, Qassim University, Buraidah Saudi Arabia
421200339@qu.edu.sa
Salim EL Khediri*
Associate Professor, Department of Information Technology, College of Computer, Qassim University, Buraidah Saudi Arabia
S.elkhediri@qu.edu.sa

Article History

Received: 1 April 2023
Revised: 1 October 2023
Accepted: 17 October 2023

Abstract

The Internet of Things (IoT) has undeniably transformed the way we interact with the world around us. As a revolutionary technology, it seamlessly integrates into our daily routines, offering unparalleled convenience and efficiency. By embedding connectivity into everyday objects, IoT has made it possible for devices to communicate, making our lives significantly easier. This constant communication and data exchange occur everywhere, from our homes to workplaces, and even in public spaces. Unfortunately, whenever connections increase, the threat of attacks increases too. Therefore, there is a critical need for systems that provide robustness at the service level. In this paper, a basic interface to IoT devices' security architecture along with blockchain is introduced to provide scalability and authentication. This survey differs from the majority of existing reviews in that it presents a more comprehensive review of emerging research to help researchers and readers understand the state-of-the-art IoT protection against cyber threats. Additionally, different types of IoT protection against cyber threats based on blockchain and access control techniques are described in this paper. The findings demonstrate that blockchain technology offers IoT devices security along with scalability.

Keywords: Authentication, Blockchain, IoT device, IoT security

1. Introduction

Today's substantial development of technology has helped to achieve high productivity and facilitate tasks in almost every aspect of our lives.

In 1999, the term IoT was introduced to the world. It started as a simple term and continued evolving to become one of the most significant terms of the drivers of business development. IoT devices range from small wearables to platforms that develop new hardware. The Council of National Intelligence and McKinsey Global Institute stated that by 2025, everyday objects such as food packages and furniture will be part of the IoT world. [1], [2].

Unfortunately, as IoT applications have grown and become widely used, malicious intent attacks on such systems have grown as well. Therefore, security has become a critical issue in the world of IoT according to their constrained environment [3]. Lack of security can destroy entire

home systems and may have consequences on human life [4]. Thus, IoT devices require an evolution of security protection technologies to defend the system from different malicious attacks, especially from external networks.

Blockchain technology offers solutions for the one-single-point attack, a problem associated with a lot of centralized networks as well. In a blockchain network, integrity and availability are ensured by the use of blockchain technology. This makes it possible for participants on this network to write, read, and verify transactions entered into a decentralized register.

Blockchain is a chain of blocks that stores all transactions executed in the network in a public ledger after validating and verifying them [4]. The verification process in blockchain serves to find the nonce; this process is called mining. Moreover, the verification process is conducted by peers called miners to add the block to the blockchain [5]. The first miner that computes the nonce can add the block to the blockchain [6]. However, deletion and modification operations on the ledger are not allowed [7]. In other words, blockchain provides a trustless environment that divides the trust between nodes that contribute as servers in the network instead of depending on one single server. Thus, the data in the blockchain are hardly updated or altered by attackers [8].

Besides security, blockchain maintains the scalability of the IoT system when the security mechanism is placed in an advanced system that represents IoT devices and supports the whole process.

In this study, an overview of blockchain technology is given, including IoT technology and the benefits of merging these technologies together. Essential studies in the field of blockchain and IoT are explored in depth and compared.

The rest of the paper is organized as follows: Section 2 contains an overview of blockchain technology. Section 3 contains an overview of IoT systems. A review of blockchain-based IoT is presented in section 4. Previous studies are detailed in section 5. Finally, the conclusion and future work is given in section 6.

2. Overview of Blockchain Technology

Satoshi Nakamoto solved the trust issues linked to information systems when he first invented Bitcoin in 2008. Bitcoin is a cryptocurrency that has value without a need for a centralized financial entity. The blockchain network is a decentralized peer-to-peer (P2P) network of participants. The system of blockchain makes it easy to exchange digital assets and verify transactions without the need for central authority. [9], [10]

The blockchain, as the main technology of Bitcoin, is more popular. The blockchain consists of records of information called blocks. The blocks are connected to each other and secured using cryptographic algorithms [11], [12]. While generating a new block, an authentication process is conducted by network nodes. When the authentication is completed and approved, the block is added to the blockchain with a pointer that points to the previous block. This addition results in the complications of altering blocks and causing attacks on the blockchain. The basic structure of the blockchain is shown in Figure 1 [12].

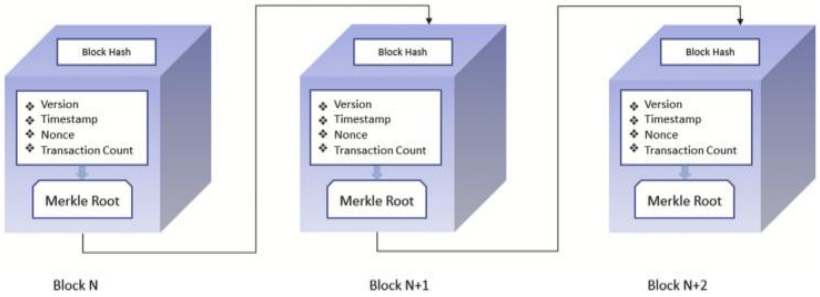

Figure 1. Basic Blockchain Structure

2.1 Blockchain Ata Structure

The transactions are recorded in a chain of blocks that make up the blockchain. Blockchain begins with its initial block called the Genesis block. Table 1 shows that there are two parts to each

block. The block header contains information such as the version of the block, previous block hash, Merkle tree root, timestamp, difficulty, and the nonce. The latter includes the transaction or any other information that ends up being stored in the Database. It includes financial data such as sales, travel records, system logs, and many others. The block body documents all inputs and outputs. The owner's private key signature signifies ownership of an asset when its input becomes the previous outlet of transactions. These are the recipient's address and any property being transmitted. The ownership attribute can only be verified by the recipient's private key; it makes the recipient alone the owner and sole user [13], [14], [15].

Table 1. Blockchain Data Structure

Field	Subfield	Size	Description
Block header	Size of block	4 bytes	Block size in bytes
	Version identifier	4 bytes	Version of block protocol
	Hash value of parent block	32 bytes	Value of the SHA256 algorithm's hash between the current block and the preceding block
	Merkle root	32 bytes	The hash value of all the transactions in the present block.
	Timestamp	4 bytes	The timestamp indicating the time of creation for the current block.
	Difficulty target	4 bytes	Difficulty target of the calculation of Proof-of-Work (PoW) in order to create the current block
	Nonce	4 bytes	In Proof of Work (PoW), a counter is employed that initiates at 0 and increments with each hash computation.
Block body	Transactions number	1-9	The quantity of transactions within this block.
	Transaction	Specified by the transactions number	Transactions that are registered in this block

2.2 Blockchain Platforms

There are various blockchain platforms. The most popular platforms are illustrated in Figure 2.

The first and most well-known blockchain platform is Bitcoin. Without a central authority or bank, Bitcoin carries out digital financial transactions. However, it does not support smart contract construction due to the limitation in the scripting language. Bitcoin utilizes the PoW consensus mechanism. Thus, it demands a lot of energy [16].

Ethereum is another popular blockchain platform that supports smart contracts using solidity language, i.e., a built-in scripting language. Therefore, Ethereum has made blockchain technology useful in various domains, not only in cryptocurrencies.

Hyperledger Fabric platform is an open-source blockchain platform. In Hyperledger Fabric, a general-purpose scripting language such as Java, Go, or Node.js simplifies smart contract creation. This has allowed for the facilitation of blockchain implementation in enterprises, as the developers do not need to learn a new scripting language for developing smart contracts. Hyperledger Fabric also supports pluggable consensus protocols to serve different industry use cases.

The multichain platform supports the creation of private blockchains. For network interaction, multichain grants a command-line interface, and by using a simple API, it extends the Bitcoin API's core functionality. Multichain supports the interaction of the network with Go, C#, Java, PHP, and Node.js through JSON-RPC API [17]. Table 2 explains the differences between blockchain platforms in detail.

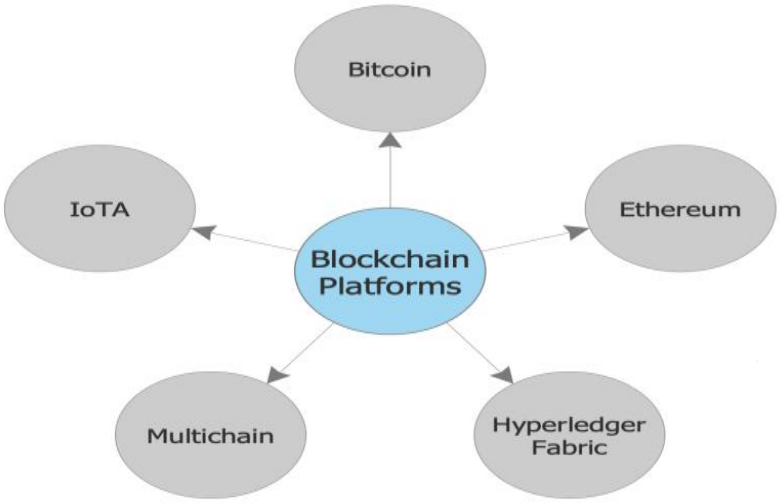

Figure 2. Blockchain Platform

Table 2. Platforms of Blockchain Comparison

Blockchain Platform	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**IoTA**	**Multichain**
Size of block	1 MB	Inconstant	Inconstant	No blocks	1GB maximum
Network permission	Permissionless	Permissioned/ Permissionless	Permissioned	Permissioned/ Permissionless	Permissioned
Time of validation	10 minutes	15-20 seconds	Fewer than Ethereum	Varies from minutes to hours.	-
Consensus mechanism	PoW	PoW, PoS	PBFT	Tip Selection Algorithm	RR
Scalability	No	No	Yes	Yes	Yes
Throughput	7 TPS	20 TPS	3000-20000 TPS	7-12 TPS	It has the capability to handle more than 2 million (TPS).
Vulnerability to attacks	51% attack	51% attack	Faulty nodes, DoS attack	34% attack	-
Cryptocurrency	Bitcoin	Ether	No native cryptocurrency	mIOTA	Multi-cryptocurrency
Smart contract	No	Yes	Yes	No support	No support
Confidentiality of data	Yes	No	Yes	No	Yes
Authentication of user	No	Digital signature	Based on certificates of enrolment	Digital signature	Login module
Energy and computational	High	High	Low	Low	Low

cost					

3. Overview of Internet of Things (IoT) Systems

The IoT is a network that links everyday physical objects, each assigned a unique, identifiable address, to enable the provision of intelligent services. In other words, it is a universal infrastructure for the community of information [18]. However, the main value of IoT is that it connects an unlimited number of devices that are heterogeneous which can be any everyday existing objects, context-aware computations, embedded intelligent sensors, smart objects, and traditional computing networks. In possession are capabilities that allow them to communicate with each other, for the reason of collecting, generating, processing, and providing information via applications and administration mechanisms that are installed in cloud data centers or networks. It makes them able to undertake sophisticated assignments and carry out their decision-making by themselves minimizing the need for human supervision. In the future, almost all objects that surround us will be linked and added to the Internet of Things [19]. The physical world and the world of information and communications technologies (ICT) will be integrated, causing a revolution in traditional networks. Communication will no longer be from person to person. Also, it will not be people accessing information. It will be machines talking to other machines on behalf of people [20].

However, broad connectivity is a requisite for IoT at its core. To meet this need, numerous different devices and communication protocols –from minute sensors up to rather reliable server-based systems intended in order to process data, analyze it, and deliver knowledge are required. This involves smooth inter-operation with mobile devices including routers and smart hubs, as well as human operators as controllers within the system [21].

3.1 Common Attacks in IoT Systems

IoT networks are susceptible to both internal and external network attacks. External attacks occur when a malicious actor targets the network from outside without access to its cryptographic keys. In contrast, internal attacks presuppose that the attacker has control over a trusted network entity, launching the assault from within the network itself. In this scenario, the attack originates from within the network, and it can be particularly challenging to detect as it may involve a previously trusted device turning rogue [1]. Further details about common attack scenarios against IoT networks can be found in Table 3.

Table 3. Common Attacks on IoT Systems

Attack	External/ Internal	Description
Sybil Attack	Both	This is a type of assault where an attacker impersonates the existing network nodes' identities.
DoS Attack	Both	Numerous devices attack a centralized server with a large number of malicious requests and prevent the server from responding to legitimate requests.
Intermittent Attack	Internal	This attack targets the nodes to perform benign and malicious behaviors to prevent their discovery as threats.
Spoofing Attack	Both	To access a valid user's privileges, the attacker tries to impersonate that user.
Substitution of Message Attack	Both	This attack alters a legitimate massage in transit so that the user receives it as the original message from the sender.
Message Replay Attack	Both	Fake information is added to previously delivered messages or reproduced.
Ballot-stuffing Attack	Internal	Malicious nodes are granted trust by positive

		reviews from other malicious nodes.
Bad-mouthing Attack	Internal	Bad reviews are given to certain nodes to prevent them from being served.
Good-mouthing Attack	Internal	This attack forces good reviews on malicious nodes to grant them trust.
Side-channel Attack	Both	The profile of a user's electricity consumption can be examined by an attacker to track the usage patterns of an application, and an attack could be launched based on this information.

3.2 General Limitations of IoT Systems

Due to the structural simplicity of IoT devices, hardware such as CPU and memory has limited capacities. Also, energy availability is very simple and cannot handle high-consumption operations. Moreover, it is not possible to deploy any software that requires high performance such as accessing the control system. Also, the integration of applications in the network infrastructure concentrates on obtaining functionality instead of considering security requirements when designing the application. Thus, security is almost nonexistent in IoT devices.

The transmission media is the route that creates the connection physically and transmits the data to the receiver. The usual issues relating to transmission media such as high error rate and bandwidth also exist for IoT. Every communication medium demands particular energy, network hardware, and compatible bandwidth with the medium. Thus, bandwidth improvement in IoT applications is a challenge to maintain and extend the network's lifetime [22]. The limitations of the IoT system are mentioned briefly in Figure 3.

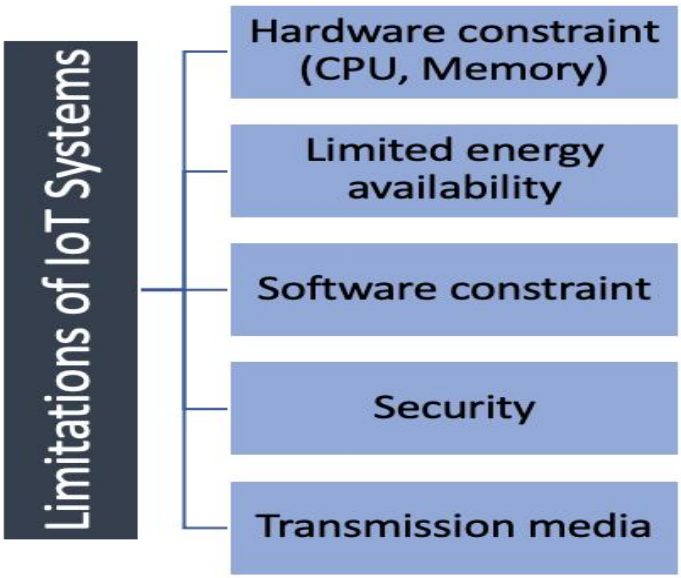

Figure 3. Blockchain Platform

4. Blockchain-based IoT Review

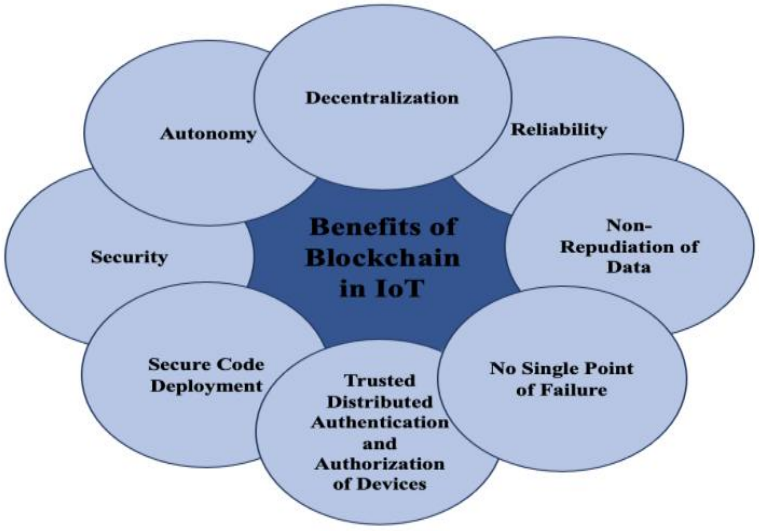

Figure 4. Benefits of Blockchain in IoT

Blockchain technology became popular after Bitcoin. There is no need for third-party security for online transactions in Bitcoin, which is a key advantage. Besides decentralization, blockchain technology grants significant features such as immutability, auditability, and transparency [23].

Introducing blockchain to IoT has brought considerable advantages to IoT systems. Decentralization of data is a significant characteristic, as are security, reliability, non-repudiation of data, and autonomy. Also, due to the decentralized environment of blockchain, there is no single point of failure. Moreover, blockchain implements secure code deployment and device-distributed authentication and authorization [24]. On a related note, there are three main criteria concerned with identity and accessibility in blockchain, namely public (less authorized), private (authorized), and consortium [25]. Figure 4 illustrates the major benefits of blockchain in IoT.

However, handling big data on the blockchain is one of the big challenges of applying blockchain technology to IoT. Also, the regulation of blockchain in IoT represents a challenge, because there are no clear laws on blockchain. Moreover, IoT devices frequently produce data which makes the concurrency of data a big challenge. The limited throughput is also a big issue in blockchain due to the complexity of cryptographic security protocols and consensus mechanisms. [26] .Furthermore, blockchain requires high computational power which is difficult for IoT to implement.

Scalability is the most critical challenge for providers of blockchain. The issue of scalability needs to be solved in order to merge IoT and blockchain. [27], [1].

In blockchain, the consensus mechanism is essential for adding blocks to the chain. The state of blockchain relies on the protocol that generates approval through independent entities. The consensus mechanism ensures high system availability and security for IoT systems including various entities.

The consensus mechanism is utilized in a decentralized (P2P) network. There is no need for a central authority to validate and store the transactions. Instead, various nodes are connected to each other in a P2P manner. Once a transaction is initiated between two nodes, a validation for the transaction needs to be performed by the rest of the nodes via a type of confirmation or voting for an agreement between the nodes. Consensus algorithm is the method used for the validation process. There are diverse types of consensus algorithms, with each algorithm varying in its performance, level of security, and reliability [17].

Table 4. Different Types of Consensus Mechanisms

Consensus Mechanism	**Example**	**Blockchain Type**	**Energy Saving**	**Scalabi -lity**	**Mining**	**Mechanis -m**	**Transaction Rate**
Proof of Work (PoW)	Bitcoin, Ethereum , NameCoi n	Permissionl ess	Low	Bad	Based on computing a mathematica l problem	Based on proof	Poor
Proof of Stake (PoS)	Ethereum , Nxt	Permission ed/ Permissionl ess	Medium	Good	The higher the stakes of the verifier, the higher the chances for creating a new block	Based on the number of tokens/ coins Locked assets	Excellent
Delegated Proof of Stake (DPoS)	Bitshares, Monax	Permissionl ess	Medium	Excelle nt	Using a random selection as the basis.	Based on voting	Excellent
Practical Byzantine Fault Tolerance (PBFT) and Variants	Hyperled ger Fabric	Permission ed	High	Fair	Based on random selection	Based on voting	Excellent
Proof of Authority (PoA)	Ethereum Microsoft Azure	Permission ed/ Permissionl ess	High	Excelle nt	The identity of the validator proceeds the role of the stake	Based on reputation	Excellent
Proof of Elapsed Time (PoET)	Coin desk, Hyperled ger sawtooth	Permission ed	High	Good	Based on election	Based on lottery	Fair
Round Robin (RR)	Multichai n, Tendermi nt	Permission ed	High	Poor	Based on pseudo- random selection	Based on voting	Excellent

5. Previous Work

At present, the significant increase of cyberattacks is resulting in a high level of damage to individuals and public properties such as network damage and the stealing of critical data. IoT

systems are resource-constrained devices that have limited memories and capacities. Therefore, the possibility of attack increases.

There is a high demand for secure IoT systems. Fortunately, blockchain technology has many advantages in securing IoT systems.

This section reviews the essential studies of recent years. The studies are chosen based on their solution to security and scalability problems in blockchain-based IoT systems. Figure 5 shows a summary of the most significant previous studies.

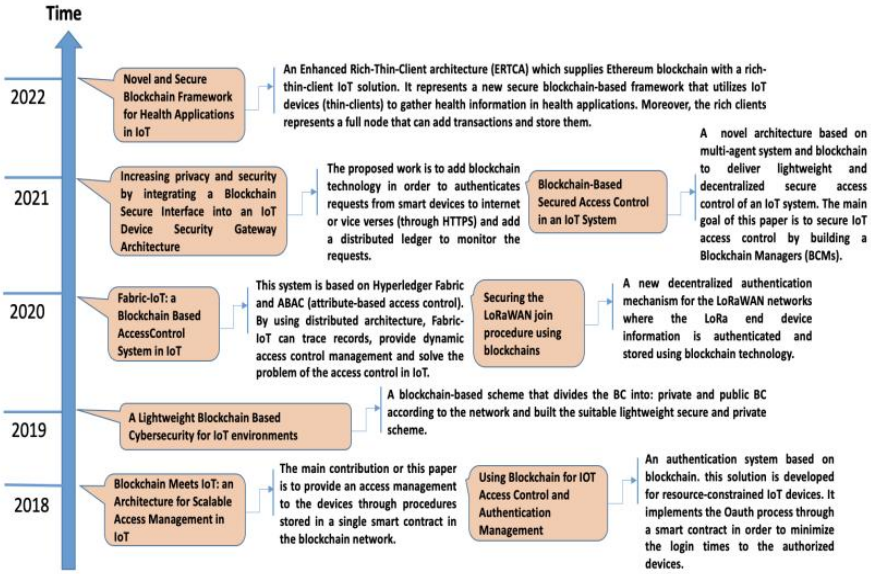

Figure 5. Recent Essential Works

Fotohi et al. focused on authenticating devices and performing hash on blocks before transmitting them over a network [27]. The operation is conducted in stages. Figure 6 displays the process of the method.

During the authentication phase, the registration algorithm of the IoT device is the first step. To perform system-level tasks, the first step is to register the device by the CA. In this step, the device is given a unique number by VCC. After that, the CA is allowed to send keys of encryption to the device. The device is currently VCC-authenticated. Moreover, as part of the verification procedure, certificates of the devices are kept by the VCC for future use.

During the registration process, in response to the device registration request, the signature and primary cases of encryption are created and stored by CA. Once a device is connected to VCC, a legitimate ID is registered and then used in subsequent transactions.

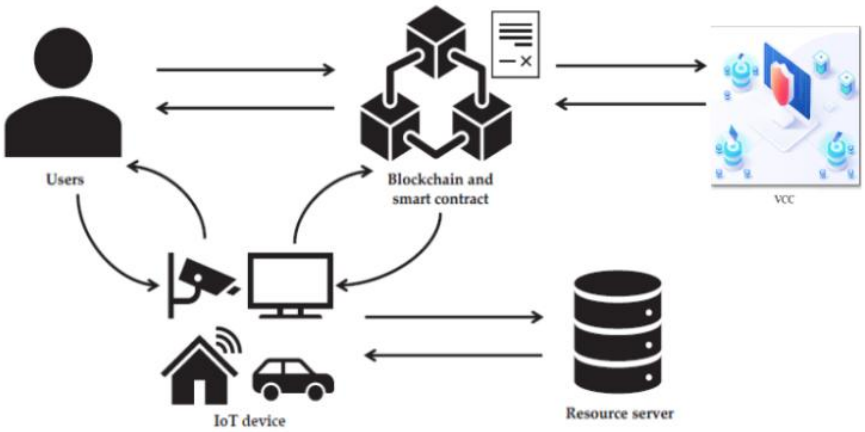

Figure 6. Authentication and Block Transmission Architecture in the CBcA Method [28]

Šarac Marko et al. focused on proposing a custom home server (hub) that functions on any platform and enables the connection of all smart devices to it [28].

The solution is based on several points. First, the connection to smart devices could be wired or wireless. Also, the connection between smart devices and home servers is wired. The communication through smart devices cannot be direct from/to the Internet; the server stands in the middle of the connection. Moreover, blockchain technology is added to the system and the network is decentralized. Also, a distributed ledger is added to detect all requests. Finally, for more security, blockchain performs authentication.

In Figure 7, the logic of blockchain is involved in the home server. Once the incoming data is parsed, the blockchain performs validation of data. Following their generation, blocks are added to the distributed ledger.

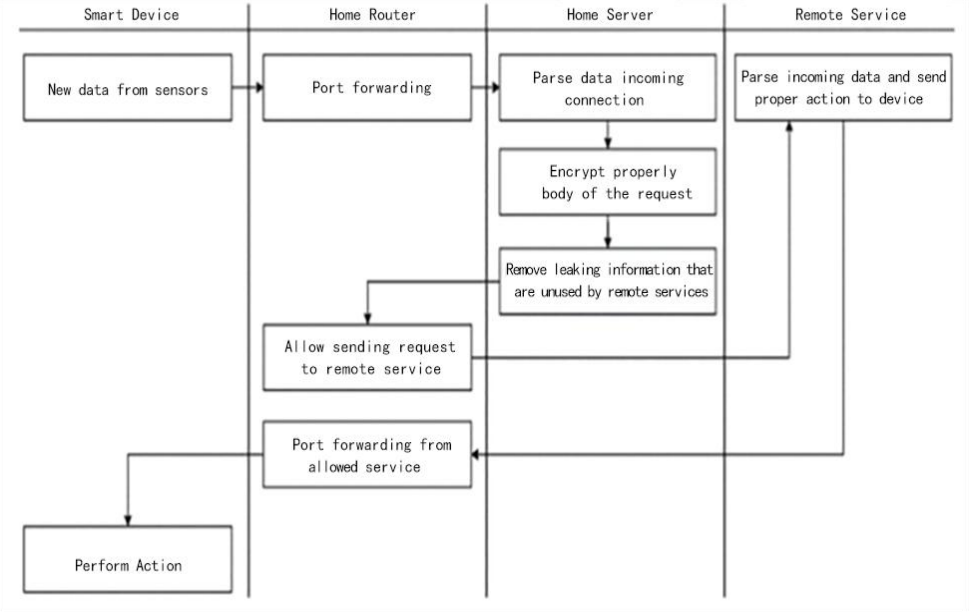

Figure 7. Activity Diagram of the Solution [29]

Li et al. proposed a system that improves the security of IoT systems in many ways [30]. In a multi-node network, whenever a new device is added, the blockchain must be updated with the identity data of the devices. Device IDs, public keys, and other information are hashed and kept in the ledger of the blockchain. The blockchain network is made up of many devices, each of which is a node. Moreover, the consensus mechanism makes sure that all nodes are storing the same data.

The system consists of three steps. First, registration of all devices in the blockchain should be completed before authentication. When a device requests network access, authentication is performed using the registration data stored in the blockchain. Beyond authentication, to spot intrusion behavior, the integrity of the device's important information hash is verified. The system model is illustrated in Figure 8.

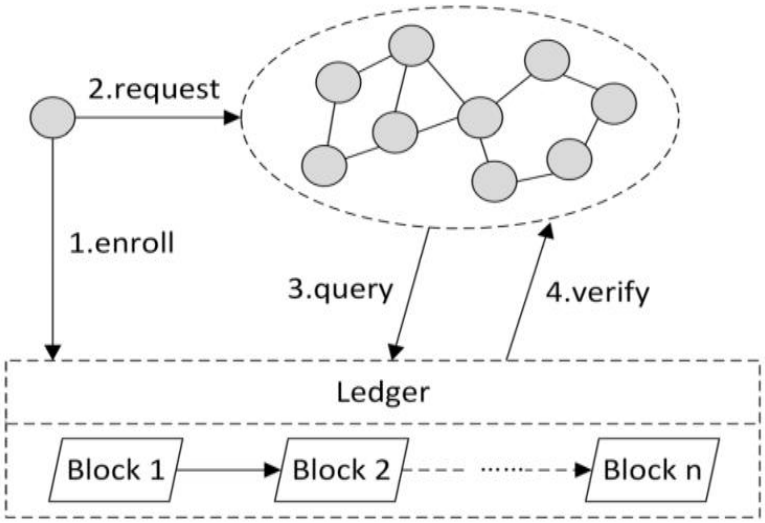

Figure 8. System Model [29]

Abdulkader et al.(2019) chose a secure lightweight blockchain for securing IoT environments from cyberattacks [31] . There are three main components of the architecture: manager of edge block (EBM), manager of aggregation block (ABM), and manager of cloud block (CBM). To store generated data, transactions, and blocks of IoT devices, the EBM is made up of SH appliances (IoT devices) and devices of local storage (LSD). Considering that it manages all storage and computation on behalf of IoT devices on a system with sophisticated computing and multicore resources, the EBM is regarded as a central manager among IoT devices in a local wireless network that manages all local transactions and blocks. Moreover, data transfer between devices is managed by EBM. It additionally collects a group of transactions into a block, verifies the block, and adds to a local blockchain the new block. Generally, a very important contribution EBM performs is the ensuring of cybersecurity in the proposed model by verifying and attaching devices, transactions, and blocks. Here, the researchers distinguish between the flow of data and the flow of transactions in order to mitigate traffic latency.

Novo (2018) proposed a fully distributed access control system based on blockchain technology for a secure IoT devices environment [32],[33]. Smart contracts store access control details. It is important to note that only these two components, IOT and the management hub nodes withstanding, are part of the mentioned infrastructure. Therefore, it handles issues associated with an increasing number of transactions in a single block. It is important, especially because many IoT devices do not have the ability to keep blockchain data, that they are limited in essence. Therefore, in this architecture, the management hub is a new node that represents IoT devices rather than adding them to the blockchain. This node requests from the blockchain the information of access control. Moreover, a single smart contract is included in this solution to determine which operations are permitted in the system of access control. Furthermore, managers are entities that provide the access control policy for the system by communicating with the smart contract.

Figure 9 illustrates the System's Architectural design. These include six elements of the architecture – a wireless sensor network, manager, agents, smart contact, a blockchain network, as well as a management hubs.

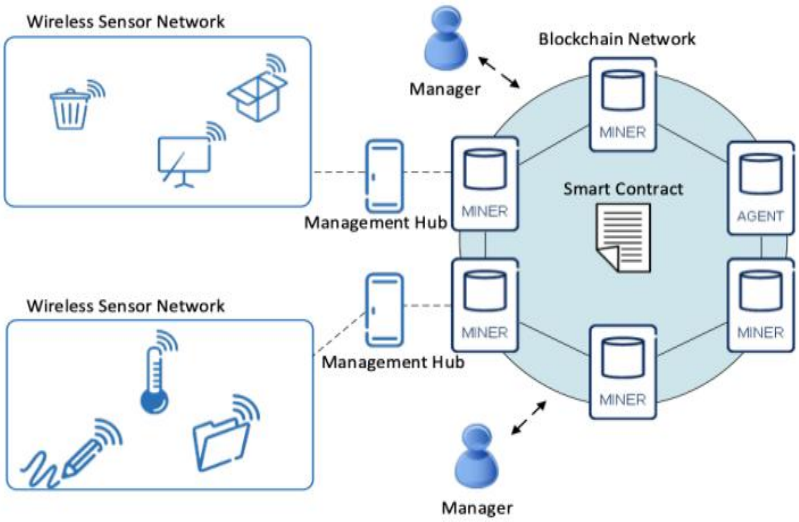

Figure 9. Decentralized Access Control System [34]

Ourad et al. proposed an authentication and secure communication system which is based on blockchain [35] . This solution is developed for resource-constrained IoT devices. The solution implements the open authorization (OAuth) process through a smart contract in order to reduce login times. The login process is done once, and all the authorized devices are controlled instead of registering each IoT device separately. Moreover, to make the IoT devices self-profiting, the smart contract could be run by them. Furthermore, the solution provides a one-time authentication. To verify the user's ID, the user authenticates the smart contract. After that, the smart contract determines whether the user can access the resource or not. Any preferred method, including SHH or HTTPS, could be used to connect to the IoT devices after user authorization.

Zhang et al. suggested an attribute-based access control (ABAC) scheme to provide authorized access for devices of IoT using the blockchain to transmit the access information securely and grant reliable credentials[36]. Moreover, a verifiable collaboration mechanism was created to prevent any malicious actions and restrict additional authorization for a specific group. Also, to perform computations and communicate with the blockchain, authority nodes (ANs) were created. In general, the system consists of five components: The access tree, IoT devices, the consortium blockchain network, chain code with the public ledger, and the authority node. There are authority nodes and common nodes in the blockchain network. Related participants in the blockchain will copy and record the information from the public ledger. Each IoT device is assigned a group ID and an IP address to identify it as a member of that group. The IoT devices have the ability to communicate with any device in any group. It is well known that most IoT devices are resource-constrained. Therefore, the IoT devices were separated from the blockchain, and authority nodes were introduced in the system to act on behalf of IoT devices. Each authority node in the system has the chain code deployed on it.

Danish et al. designed a decentralized LoRaWAN join procedure framework [37] .For LoRaWAN networks, this work introduces a distributed novel authentication method in which blockchain technology is used to authenticate and store LoRa end device data. As illustrated in Figure 10, the framework consists of gateways and LoRa end devices, a join server, an agent network server (ANS), a blockchain network, and a smart contract. At the gateway, LoRa end devices interact with the network server to complete tasks. "LoRa End Devices". The locomotion network server will get data from the LoRa end device by the gateway through TCP/IP connections. This model has an unsecured gateway. In addition, Lora end devices do not belong to the blockchain network. Hence, these functions are possible at low power consumption. The server of the network joins the conversation through IP connections to create the application and network session keys with which it feeds the network server and applications. The join server has the main purpose of storing and restoring the user's authentication information from the blockchain network.

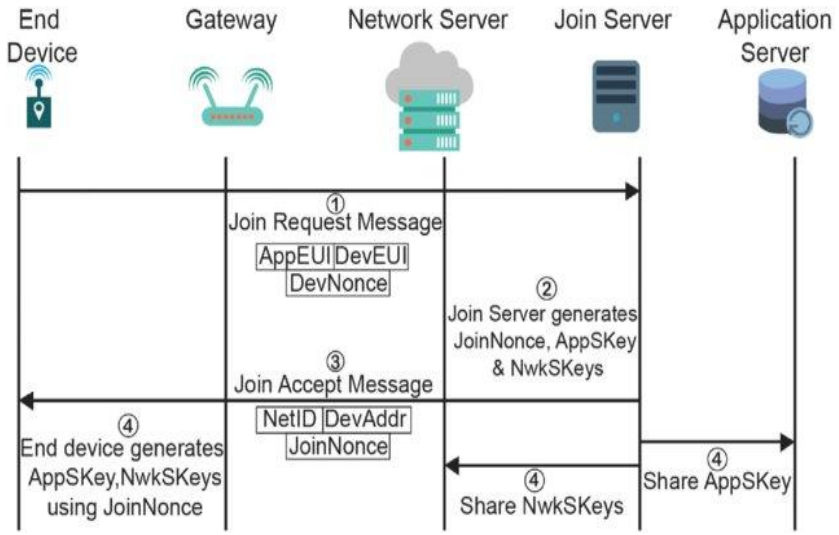

Figure 10. The Improved Architecture for the LoRaWAN Join Procedure

Bataineh et al.(2019) developed an Enhanced Rich-Thin-Clients Architecture (ERTCA), which supplies a rich-thin-client IoT solution for the Ethereum blockchain [38, 39]. The user interface and gathering of information are the thin client's responsibility. The thin clients are considered resource-constrained IoT devices. The thin clients, the rich clients, and the full blockchain nodes could be devices that are personal computers or equal to them. In this work, there are two levels of thin clients. The second-level thin client does not interact with the system; it is only used to collect data from the real world. It could be sensors databases or people. A GUI is supported by both rich and thin clients to simplify the process for users. The rich client is different from the thin client in that it has a full blockchain node that stores all of the blockchain's transaction records. Also, it is able to register transactions to the blockchain. Rich clients consist of the Ethereum blockchain node. The system is decentralized, and the rich clients represent a P2P network. Therefore, other rich clients can handle the failure and rescue the linked thin clients if the rich client is exposed to any type of failure. Figure 11 illustrates the architecture of the ERTCA system. In this health system, the rich client represents the surgery management system (SMS).

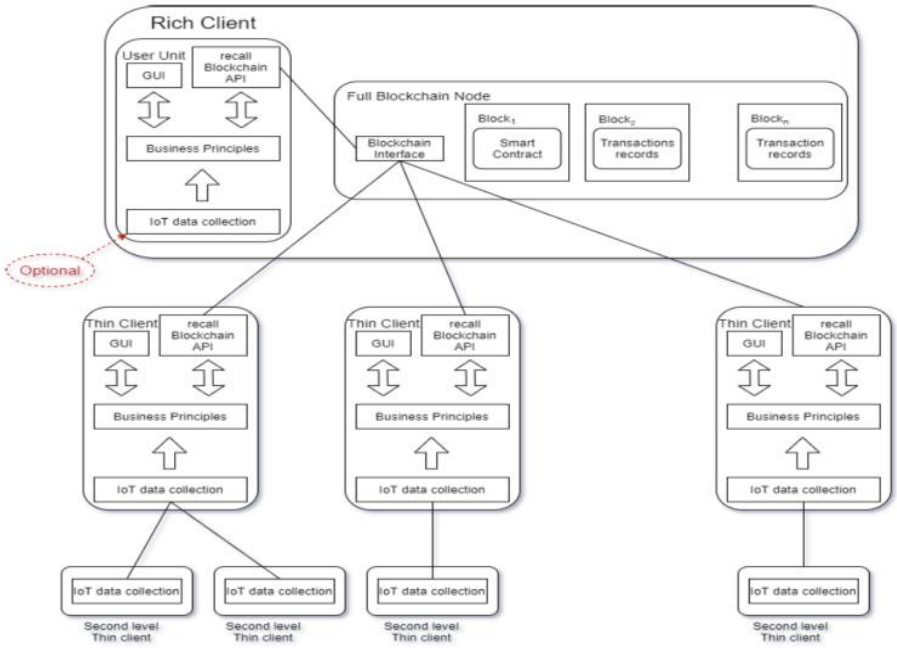

Figure 11. The Enhanced Rich-Thin-Clients Architecture (ERTCA) Architecture

To sum up, an enhanced rich-thin-clients architecture can improve a system's health functions, including users' comfort, advanced data visualization, information safeguarding, and the support of remote control and medicine. Such technologies can support hospitals with their evolving needs of scalability, interoperability, and embracing Internet-of-Things devices in changing healthcare contexts.

6. Conclusion and Future Work

This paper provides an overview of blockchain technology, IoT technology, and the benefits of merging these technologies together. The blockchain is a decentralized robust technology that provides many benefits such as security and scalability when integrated with other technologies. The integration of blockchain with IoT resource-constrained systems has brought big advantages to IoT devices. Moreover, previous studies of adding blockchain to IoT systems were reviewed based on different techniques and approaches in order to enhance security and avoid malicious behaviors by providing a decentralized system. Security has been addressed in IoT systems in different mechanisms. IoT devices have limited computing resources and storage. Therefore, most studies distinguish between the system of blockchain and the IoT devices to make the system reliable and secure.

With this growth in IOT, it is necessary for more research in scalable blockchain solutions that will be able to cater to more transaction and data volumes in the future. The development of smart consensus protocols and blockchain designs suited for IoT devices will be important.

7. Acknowledgement

The authors gratefully acknowledge Qassim University, represented by the Deanship of "Scientific Research, on the financial support for this research under the number (COC-2022-1-3-J-31771) during the academic year 1444 AH / 2022 AD".

References

[1] E.A. Shammar, A.T. Zahary and A.A. Al-Shargabi, "A survey of IoT and blockchain integration: Security perspective," *IEEE Access*, vol. 9, pp. 156114-156150, November 2021.

[2] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, "CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques," *In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) ,* pp. 1-6, july 2019.

[3] B.K. Mohanta, D. Jena, U. Satapathy and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p.100227, May 2020.

[4] F. Alkhudhayr, S. Alfarraj, B. Aljameeli and S. Elkhdiri, "Information security: A review of information security issues and techniques," *In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS),* pp. 1-6, 2019.

[5] R. Al Mogbil, M. Al Asqah and S. El Khediri, "Iot: Security challenges and issues of smart homes/cities," *In 2020 International Conference on Computing and Information Technology (ICCIT) ,* pp. 1-6, 2020.

[6] G. Alqarawi, B. Alkhalifah, N. Alharbi and S. El Khediri, "Internet-of-things security and vulnerabilities: case study," *Journal of Applied Security Research*, pp. 1-17, Feb. 2022

[7] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6-14, Jul. 2018.

[8] A.A. Monrat, O. Schelén and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134-117151, 2019.

[9] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: research and applications*, vol. 3, no. 2, p. 100067, Feb. 2022.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," *In 2017 IEEE international congress on big data (BigData congress) ,* pp. 557-564, 2017.

[11]T. Aste, P. Tasca and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18-28, 2017.

[12]A. Litke, D. Anagnostopoulos and T. Varvarigou, "Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment," *Logistics*, vol. 3, no. 1, p. 5, 2019.

[13]T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE transactions on knowledge and data engineering*, vol. 30, no. 7, pp. 1366-1385, Jul 2018.

[14]S. Saxena, B. Bhushan and M.A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," *Journal of Network and Computer Applications*, vol. 181, p. 103050, Mar 2021.

[15]X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," *In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) ,* pp. 468-477, 2017.

[16]A. Panarello, N. Tapas, G. Merlino, F. Longo and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.

[17]G. Kaur, and C. Gandhi, "Scalability in blockchain: Challenges and solutions," *In Handbook of Research on Blockchain Technology,* pp. 373-406, 2020.

[18]T.T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: a systematic review and healthcare examples," *Journal of the American Medical Informatics Association*, vol. 26, no. 5, pp. 462-478, Mar 2019.

[19]M. Dabbagh, K.K.R. Choo, A. Beheshti, M. Tahir and N.S. Safa, "A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities," *Computers & Security*, vol. 100, p. 102078, Jan 2021.

[20]F. Alfaleh and S. Elkhediri, "Efficient Security Solutions for IoT Devices," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, 2021.

[21]S.H. Alrasheed, S.A. Adubaykhi, and S. El Khediri, "Cloud Computing Security and Challenges: Issues, Threats, and Solutions," *In 2022 5th Conference on Cloud and Internet of Things (CIoT) ,* pp. 166-172, 2022.

[22]F. Khodadadi, A.V. Dastjerdi and R. Buyya, "Internet of things: an overview," *Internet of things*, pp.3-27, 2016.

[23]L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-Castellanos, A. Alissa and M. Abdulsalam, "A concise review on Internet of Things (IoT)-problems, challenges and opportunities," *In 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP) ,* pp. 1-6, 2018.

[24]M. Kouhizadeh and J. Sarkis, "Blockchain practices, potentials, and perspectives in greening supply chains," *Sustainability*, vol. 10, no. 10, p. 3652, 2018.

[25]A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173-190, 2018.

[26]S. Singh, A.S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," *IEEE Access*, vol. 9, pp. 13938-13959, 2021.

[27]Fotohi, R., & Aliee, F. S. (2021). "Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT," *Computer Networks*, vol. 197, p. 108331, Oct. 2021.

[28]M. Šarac, N.Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture," *Energy Reports*, Aug. 2021.

[29]L. Vishwakarma and D. Das, "SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain," *Journal of Parallel and Distributed Computing*, vol. 154, pp. 94-105, Aug 2021.

[30] Li, D., Peng, W., Deng, W., & Gai, F. " A blockchain-based authentication and security mechanism for IoT," *In 2018 27th International Conference on Computer Communication and Networks (ICCCN),* pp. 1-6 .July 2018.

[31] O. Abdulkader, A.M. Bamhdi, V. Thayananthan, F. Elbouraey, and B. Al-Ghamdi, "A lightweight blockchain based cybersecurity for IoT environments," *In 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom),* pp. 139-144, 2019.

[32] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE internet of things journal*, vol. 5, no. 2, pp. 1184-1195, Apr. 2018.

[33] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassam, K. Alsubhi and M. Yamin, "Blockchain-based secured access control in an IoT system," *Applied Sciences*, vol. 11, no. 4, p. 1772, 2021.

[34] A. Ouaddah, H. Mousannif, A. Abou Elkalam and A.A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237-262, 2017.

[35] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IOT access control and authentication management," *In Lecture Notes in Computer Science* , vol. 10972 , pp. 150-164, 2018.

[36] Zhang, Y., Li, B., Liu, B., Wu, J., Wang, Y., & Yang, X. (2020). "An attribute-based collaborative access control scheme using blockchain for IoT devices," *Electronics*, vol. 9, no. 2, p. 285, Feb. 2020.

[37] Danish, S. M., Lestas, M., Qureshi, H. K., Zhang, K., Asif, W., & Rajarajan, M. ."Securing the LoRaWAN join procedure using blockchains," *Cluster Computing*, vol. 23, no. 3, pp. 2123-2138. 2020.

[38] M.R. Bataineh, W. Mardini, Y.M. Khamayseh, and M.M.B. Yassein, "Novel and secure blockchain framework for health applications in IoT ," *IEEE Access*, vol. 10, pp. 14914-14926, 2022.

[39] M. Al-Enazi and S. El Khediri, "Advanced Classification Techniques for Improving Networks' Intrusion Detection System Efficiency," *Journal of Applied Security Research*, vol. 17, no. 2, pp. 257-273, 2022.