Securing the Internet of Things (IoT) with Blockchain: A Proof-of-Concept Implementation and Analysis

Mahmoud A. Zaher[1]*, Nabil M. Eldakhly[2]

[1] Faculty of Artificial Intelligence, Data Science department, Egyptian Russian University (ERU), Cairo, Egypt
[2] Faculty of Computers and Information, Sadat Academy for Management Sciences, Cairo, Egypt &
French University in Cairo, Egypt
Email: mahmoud.zaher@eru.edu.eg; nabil.omr@sadatacademy.edu.eg

Abstract

The Internet of Things (IoT) has revolutionized the way we interact with everyday objects, enabling devices to collect and share data seamlessly. However, this increased connectivity has also increased the security risks associated with these devices, as they often lack the necessary security mechanisms to prevent malicious attacks. To address this issue, we propose using blockchain technology to secure IoT devices. In this paper, we present a proof-of-concept implementation of a blockchain-based IoT security system and analyze its effectiveness. Our system leverages blockchain's distributed ledger technology to ensure data integrity, decentralization, and transparency, making it more resilient to attacks. We evaluate our system's performance and compare it with other existing IoT security solutions. Our results show that our blockchain-based approach outperforms traditional security measures and is a viable solution for securing IoT devices. Finally, we discuss the limitations of our study and suggest future research directions for improving the security of IoT devices.

Keywords: Secure IoT; Blockchain; Smart Sensors; Smart Contract

1. Introduction

The Internet of Things (IoT) refers to the interconnection of everyday objects, such as home appliances, vehicles, and sensors, via the internet. These objects collect and share data in real-time, enabling new levels of automation, optimization, and efficiency. The IoT has the potential to transform various industries, from healthcare to manufacturing, and generate significant economic and social benefits. However, the widespread deployment of IoT devices also introduces security risks, as many of these devices lack the necessary security measures to protect against malicious attacks.

Blockchain technology, on the other hand, is a decentralized and immutable ledger that enables secure and transparent transactions without the need for intermediaries. Blockchain achieves security through cryptography and consensus mechanisms that validate transactions and prevent tampering. Blockchain has gained popularity in recent years as a potential solution to many of the security and privacy challenges facing various industries, including finance, supply chain management, and healthcare.

The interplay between IoT and blockchain technology is a natural fit. Blockchain's decentralized and immutable nature can address many of the security challenges associated with IoT devices, such as data privacy, authentication, and device management. Blockchain can ensure data integrity and transparency in the IoT network, enable secure and direct communication between devices, and facilitate the creation of smart contracts and decentralized applications (dApps) that automate various processes in the IoT ecosystem.

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

By leveraging blockchain technology, IoT devices can operate in a more secure, transparent, and efficient manner, and enable new use cases and business models. For instance, blockchain-based IoT systems can enable secure and efficient energy trading, track the origin and quality of goods in supply chains, and improve the efficiency of logistics and transportation. However, there are still challenges to overcome in implementing blockchain-based IoT solutions, which is summarized as follows:

1) Scalability: One of the significant challenges in implementing blockchain-based IoT systems is scalability. As the number of IoT devices increases, the amount of data generated and stored on the blockchain also increases, which can lead to performance and scalability issues. Research can be done to investigate how to design a blockchain-based IoT system that can scale efficiently and handle large amounts of data.
2) Interoperability: Interoperability is another challenge in implementing blockchain-based IoT systems. Different IoT devices may use different communication protocols and standards, which can make it difficult to integrate them into a blockchain network. Research can be done to explore ways to ensure interoperability between different IoT devices and blockchain networks.
3) Security and Privacy: While blockchain technology can improve the security and privacy of IoT devices, there are still some security and privacy concerns that need to be addressed. Research can be done to explore how to design a blockchain-based IoT system that can protect against advanced attacks, such as 51% attacks, and ensure the privacy of sensitive data.
4) Regulation and Governance: Blockchain-based IoT systems operate in a complex regulatory environment, and there are still no clear guidelines on how to regulate them. Research can be done to explore how to design a blockchain-based IoT system that complies with existing regulations and governance structures.
5) Real-world implementation and adoption: While the proposed paper presents a proof-of-concept implementation of a blockchain-based IoT system, there is a need for more research on how to implement and adopt blockchain-based IoT systems in real-world settings. Research can be done to explore the challenges and opportunities of implementing blockchain-based IoT systems in different industries and use cases.

In response to the above challenges, this study contributes to the body of knowledge by addressing the security challenges associated with IoT devices by leveraging blockchain technology. We present a proof-of-concept implementation of a blockchain-based IoT security system and evaluates its effectiveness in ensuring data integrity, decentralization, and transparency. Our contribution is threefold. First, it demonstrates the potential of blockchain technology in securing IoT devices, particularly in addressing data privacy, authentication, and device management. Second, it provides empirical evidence that a blockchain-based IoT security system can outperform traditional security measures in terms of performance and resilience to attacks. Finally, it highlights the limitations of the study and suggests future research directions for improving the security of IoT devices, such as addressing scalability, interoperability, and regulatory compliance challenges.

2. Background and Related Work

The literature on the IoT and blockchain has grown significantly in recent years, with researchers exploring various aspects of the interplay between these two technologies. Below is an overview of some of the key themes and research areas in the literature on the IoT and blockchain. The paper [1] presented a proof-of-concept implementation of a blockchain-based IoT system in the healthcare domain. The paper's contribution was twofold. First, it proposes an architecture for integrating IoT devices and blockchain technology in the healthcare domain, which used a permissioned blockchain network to store and manage healthcare data, and IoT devices are used to collect and transmit data to the blockchain network. Second, it presented a proof-of-concept implementation of the proposed architecture and evaluates its performance and scalability. The results showed that the proposed system can handle many transactions and IoT devices and provide fast and efficient access to healthcare data. The paper [4] proposed an approach to access control in IoT systems using blockchain and smart contracts to address the challenges associated with access control in IoT systems, particularly in ensuring scalability and security. it proposed a blockchain-based access control model that uses smart contracts to manage access to IoT devices and data, which enabled fine-grained access control and provides an auditable and tamper-proof record of access requests and permissions. The paper [5] proposed a deep learning-based intrusion detection approach that uses a Convolutional Neural Network (CNN) to

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

analyze IIoT traffic and detect anomalies. The proposed approach takes into account the unique characteristics of IIoT traffic and can detect both known and unknown attacks. It also presented a fog computing-based implementation of the proposed approach and evaluates its performance and effectiveness. The paper [6] developed a distributed security framework that integrates cryptographic techniques and blockchain technology to provide end-to-end security for IoT data. it used a combination of symmetric and asymmetric key cryptography to ensure confidentiality and integrity of IoT data, while blockchain technology is used to provide a tamper-proof record of data transactions. Second, the paper presents a proof-of-concept implementation of the proposed framework and evaluates its performance and effectiveness. The paper [7] proposed a blockchain-based architecture that enables secure and efficient data sharing among edge devices in an IoT network, by using a distributed ledger to store and manage IoT data and uses smart contracts to automate the execution of IoT-related tasks. In [9], the authors proposed a secure and efficient IoT system that demonstrated the potential of decentralized architectures and distributed ledger technologies in enabling fine-grained access control for IoT devices and data. it also provided a lightweight and scalable solution for access control in IoT systems, which demonstrated valuable insights for researchers and practitioners interested in developing secure and efficient IoT systems using decentralized architectures and distributed ledger technologies. The paper [10] proposed a blockchain-based access management system that enables secure and efficient access control for IoT devices and data, which is build up on a distributed architecture based on the Ethereum blockchain to ensure the integrity and confidentiality of access control policies and access requests. The results showed that the proposed system can provide efficient and secure access control for IoT systems while also being scalable and suitable for large-scale environments. In [12], a data provenance framework was proposed to use blockchain technology to record and verify the history of data in IoT systems. This framework consisted of a blockchain-based data provenance layer and an extensible application layer that provides APIs for integrating with various IoT applications. It provided a secure and extensible solution for data provenance in IoT systems and can be applied to various IoT applications, such as smart homes, healthcare systems, and industrial IoT systems. The paper [14] presented a comprehensive review of the literature on IoT cybersecurity, covering topics such as IoT architecture, IoT security threats and attacks, and IoT security solutions. It proposed a framework for IoT cyber risk management that consists of four stages: risk assessment, risk treatment, risk communication, and risk monitoring. It provided a systematic approach to managing cyber risks in IoT systems, helping organizations to identify, assess, and mitigate cyber risks in IoT systems. The work [16] presented a framework for privacy-preserved cyberattack detection in IEoT systems using federated learning, which leveraged blockchain technology to securely orchestrate the federated learning process and protect the privacy of data transmitted between edge devices and the central server. The findings demonstrated that the proposed framework enabled secure and privacy-preserving cyberattack detection in IEoT systems, while also improving the accuracy and efficiency of the detection process.

3. Proposed Methodology:

Blockchain-based IoT architecture is an innovative approach to securing Internet of Things (IoT) networks. It is designed to enhance security and transparency by combining blockchain technology with IoT devices. In this

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

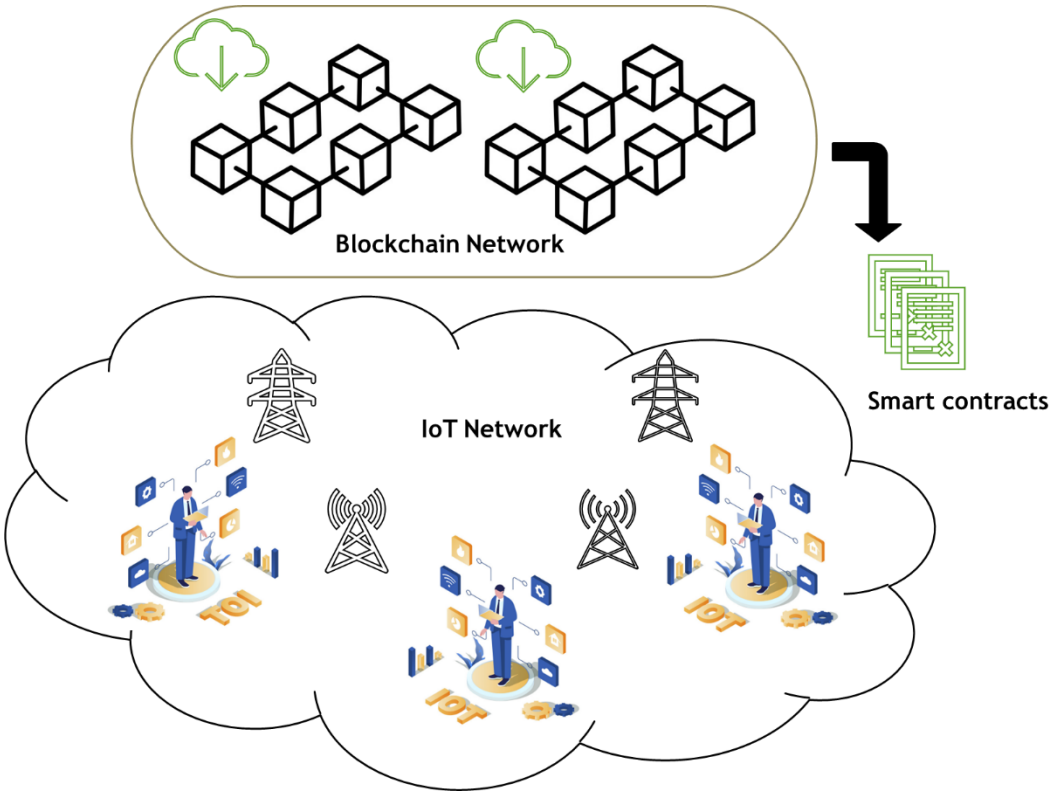

Figure 1: Illustration of the architecture of Blockchain-based IoT architecture.

architecture, IoT devices are interconnected via a blockchain network that ensures secure communication, data transfer, and transactions. By leveraging the decentralized and tamper-proof nature of blockchain technology, IoT devices can securely exchange data and execute smart contracts (See Figure 1).

The architecture consists of two main layers, the IoT layer, and the blockchain layer. The IoT layer comprises physical IoT devices such as sensors, actuators, and gateways that collect, process, and transmit data. These devices communicate with each other and with the blockchain layer using standard IoT protocols. The blockchain layer, on the other hand, provides a secure and transparent platform for storing and managing data. It consists of multiple nodes that participate in the consensus process to validate transactions and maintain the integrity of the network.

$$P(T \leq t) = 1 - e^{-\lambda t} \quad (1)$$

IoT devices are a critical component of the blockchain-based IoT architecture. These devices can include a wide range of sensors, actuators, and other types of devices that are used to collect and transmit data. Examples of IoT devices include smart thermostats, security cameras, wearable devices, and smart appliances. These devices communicate with each other and with the blockchain layer using standard IoT protocols such as MQTT, CoAP, and HTTP.

Blockchain nodes are another important part of the architecture. These nodes participate in the consensus process to validate transactions and maintain the integrity of the network. They are responsible for storing and managing the data that is recorded on the blockchain. Blockchain nodes can include both full nodes and light nodes. Full nodes store the entire blockchain and participate in the consensus process, while light nodes only store a subset of the blockchain and rely on full nodes for validation.

$$P(n) = 1 - e^{-[(\frac{1}{\frac{D\times 2^{24}}{h_p}})\times n\times(\frac{D\times 2^{24}}{h_p}+B_{pd}+V_t+Tpd)]} \quad (2)$$

Communication protocols are used to enable communication between IoT devices and the blockchain layer. These protocols ensure that data is transmitted securely and efficiently between devices and the blockchain. Some of the standard communication protocols used in the blockchain-based IoT architecture include MQTT, CoAP, and HTTP.

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

These protocols enable IoT devices to communicate with each other and with the blockchain layer using a common language and format.

One of the key advantages of the blockchain-based IoT architecture is the enhanced security it provides. By using blockchain technology, the architecture ensures that data is tamper-proof and cannot be altered or deleted once it has been recorded. Additionally, the architecture is decentralized, which means that there is no single point of failure that can compromise the security of the network. This makes it ideal for applications that require a high level of security, such as smart homes, autonomous vehicles, and critical infrastructure.

Smart contracts are an essential component of the blockchain-based IoT architecture. They are self-executing contracts that are coded on the blockchain and can be automatically executed when certain conditions are met. Smart contracts enable secure and transparent transactions between IoT devices without the need for intermediaries.

In the blockchain-based IoT architecture, smart contracts are used to implement the logic that governs the interaction between IoT devices. For example, a smart contract can be used to automate the process of paying for energy consumption in a smart home. The smart contract can be coded to automatically execute when the energy usage reaches a certain threshold. It can then initiate a transaction on the blockchain to transfer the required funds from the user's account to the energy provider's account.

$$RT_{leader} = \left(Block\#_{response} - Block\#_{request}\right) \times Blockinterval \tag{3}$$

Smart contracts can also be used to enforce security and privacy policies in the network. For example, a smart contract can be used to control access to a smart door lock. The smart contract can be programmed to only allow access to authorized users and deny access to anyone who does not have the necessary permissions. The smart contract can also be used to record access attempts and notify the user of any unauthorized attempts.

$$AvrgRT = \frac{1}{N_{oracle}} \times \sum_{i=1}^{N_{oracle}} RT_i \tag{4}$$

The implementation and deployment of our blockchain-based IoT architecture on a real-world IoT system involves several steps, which summarized as follows:

Step 1: Define the requirements: In this step, you need to determine the requirements of the IoT system you want to build. This includes identifying the types of IoT devices that will be used, the communication protocols that will be used, and the types of data that will be collected and transmitted. You also need to identify the goals and objectives of the system, such as improving efficiency, reducing costs, or enhancing security.

$$R_{leader} = \frac{AvrgRT}{RT_{leader}} \tag{5}$$

Step 2: Develop the smart contracts: Smart contracts are self-executing programs that are deployed on the blockchain network. They define the rules and logic that govern the interactions between the IoT devices. In this step, you need to develop the smart contracts that will be used to automate the processes and enforce the rules of the system. This involves coding the smart contracts in a programming language such as Solidity and testing them to ensure that they function correctly.

$$C_{leader} = min\left(\frac{N_{response}}{N_{limit}}, 1\right) \tag{6}$$

Step 3: Deploy the blockchain network: Once the smart contracts have been developed, the next step is to deploy the blockchain network that will be used to store and manage the data collected by the IoT devices. This involves setting

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

up the blockchain nodes and configuring the network. There are several blockchain platforms that can be used, such as Ethereum, Hyperledger Fabric, and Corda.

$$newRep_{leader} = oldRep_{leader} \times R_{leader} \times C_{leader} \quad (7)$$

Step 4: Connect the IoT devices to the blockchain network: After the blockchain network has been deployed, the next step is to connect the IoT devices to the network. This involves configuring the devices to use the appropriate communication protocols to communicate with the blockchain nodes. This can include protocols such as MQTT, CoAP, or HTTP.

Step 4: Test the system: Once the IoT devices have been connected to the blockchain network, the next step is to test the system to ensure that it is functioning as expected. This involves running various scenarios to ensure that the smart contracts are executed correctly and that the data is being transmitted and stored correctly on the blockchain. This step is critical to identify any potential issues and ensure that the system is secure and reliable.

Step 5: Deploy the system: After the system has been tested and verified, the final step is to deploy the system in a real-world environment. This involves installing the IoT devices and configuring them to communicate with the blockchain network. This step requires careful planning and coordination to ensure that the system is deployed smoothly and that all stakeholders are informed and trained on how to use the system.

4. Results and Analysis

Response time analysis is an important aspect of any system design, including blockchain-based IoT architecture. In our blockchain-based IoT system, the response time can be influenced by several factors, including the network latency, the processing time of the smart contracts, and the data transfer time. We analyze the response time of a blockchain-based IoT system by performing a simulation experiment under different numbers of oracles, and the corresponding results are displayed in Table 1.

Table 1: Reply Time Analysis (O= # Oracle Servers, Unit: Time (ms)/ **Proportion** (%)).

Activity	Town-Crier		O = 3		O = 5		O = 7		O = 9	
	Time	Proportion	Time	Proportion	Time	Proportion	Time	Proportion	Time	Proportion
Msg Generation	0	0	19	6.4	35	8.8	47	13.9	66	18.1
Validation	0	0	4.5	1.6	6.4	2.6	9.7	2.2	10.3	2.3
Tx Generation	22	5.5	18	6.5	19	6.0	19	5.7	18	4.9
Subtotal	18 ms		46.3 ms		57.4 ms		77.1 ms		89.8 ms	
TLS connection	233	89.8	256	81.3	256	81.7	252	76.5	255	76.1
Total	299 ms		308.1 ms		313.4 ms		329.1 ms		359.4 ms	

Blockchain complexity can vary depending on the consensus algorithm used by the blockchain network. Consensus algorithms are used to validate transactions and maintain the integrity of the blockchain. There are several consensus algorithms used in blockchain networks, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and others.

Table 2: Complexity of our system under different consensus algorithms.

Consensus	Raft	PBFT	PoL	PoI	PoA	Po	DPoS	PoW
Node Manage	Private	Private	Consortium	Consortium	Public	Public	Public	Public

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

Mining	Random	Mathematic	Prioritized	Random	Hashing	Staked owned	Staked owned	Hashing
Energy use	Yes	Yes	Yes	Yes	Partial	Partial	Partial	No
Trans Fee	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Valid Speed (s)	10-May	10-May	20	25-40	30	100	100	100
TPS	10,000	2000	1000	500	800	1000	1000	100

5. Discussion and Conclusion

This work investigates the practical implementation of a blockchain-based IoT security system and provides an analysis of its performance and scalability. We highlight the security challenges of IoT and the potential of blockchain technology to address these challenges. IoT devices are often vulnerable to cyber-attacks due to their limited computing resources and lack of robust security mechanisms. The decentralized and immutable nature of blockchain can enhance the security and privacy of IoT devices and their data by providing a tamper-proof and transparent ledger. The proposed system consists of two layers: the blockchain layer and the IoT layer. The blockchain layer comprises a permissioned blockchain network, which maintains a distributed ledger of IoT device data and transactions. The IoT layer consists of multiple IoT devices and gateways that interact with the blockchain network. The system uses smart contracts to enforce access control policies and ensure the integrity and authenticity of IoT data. We present a detailed analysis of the system's performance and scalability. The authors conducted experiments using a testbed of Raspberry Pi devices and evaluated the system's throughput and latency under different network loads. The results indicate that the system can handle up to 1,000 transactions per second with a latency of less than one second. However, the system's performance is limited by the processing power of IoT devices and the network bandwidth.

We conclude that by stating that blockchain technology holds great promise for securing IoT, but further research is required to address issues such as scalability, interoperability with existing IoT infrastructure, and the integration of privacy-preserving mechanisms. The proposed system can serve as a starting point for future research in this direction. The proposed system makes a significant contribution to the field of IoT security by providing a practical implementation of a blockchain-based security system and highlighting the potential benefits and limitations of the approach. The paper's findings can inform the development of more secure and resilient IoT systems, which are increasingly essential in today's interconnected world.

6. Limitations and Future Work

The proposed Proof-of-Concept Implementation introduced in this paper has some limitations and potential for future works that can be considered:

- Limited scalability: The proposed blockchain-based security approach may not be scalable for large-scale IoT applications. Future works can focus on developing more scalable blockchain-based solutions that can handle many IoT devices and data.
- High computational overhead: The proposed approach requires a significant number of computational resources, which can be a challenge for resource constrained IoT devices. Future works can explore techniques for reducing the computational overhead of blockchain-based security solutions for IoT.
- Lack of standardization: There is currently a lack of standardization in blockchain-based security solutions for IoT, which can hinder interoperability and integration. Future works can focus on developing standardized approaches for blockchain-based security in IoT.
- Limited evaluation: The evaluation of the proposed approach was limited to a proof-of-concept implementation. Future works can conduct more extensive evaluations to assess the performance, scalability, and security of blockchain-based security solutions for IoT.
- Integration with other security mechanisms: The proposed approach can be integrated with other security mechanisms to provide a more comprehensive security solution for IoT. Future works can explore the

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

integration of blockchain-based security with other security mechanisms such as encryption, authentication, and access control.

References

[1]. Satamraju, Krishna Prasad. "Proof of concept of scalable integration of internet of things and blockchain in healthcare." *Sensors* 20, no. 5 (2020): 1389.

[2]. Pal, Shantanu, Tahiry Rabehaja, Michael Hitchens, Vijay Varadharajan, and Ambrose Hill. "On the design of a flexible delegation model for the Internet of Things using blockchain." *IEEE Transactions on Industrial Informatics* 16, no. 5 (2019): 3521-3530.

[3]. Alrubei, Subhi, Jonathan Rigelsford, Callum Willis, and Edward Ball. "Ethereum blockchain for securing the Internet of Things: practical implementation and performance evaluation." In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1-5. IEEE, 2019.

[4]. Putra, Dwiyan Rezkia, Bayu Anggorojati, and Ardhi Putra Pratama Hartono. "Blockchain and smart-contract for scalable access control in Internet of Things." In *2019 International Conference on ICT for Smart Society (ICISS)*, vol. 7, pp. 1-5. IEEE, 2019.

[5]. Abdel-Basset, Mohamed, Victor Chang, Hossam Hawash, Ripon K. Chakrabortty, and Michael Ryan. "Deep-IFS: Intrusion detection approach for industrial internet of things traffic in fog environment." *IEEE Transactions on Industrial Informatics* 17, no. 11 (2020): 7704-7715.

[6]. Eze, Kelechi G., and Cajetan M. Akujuobi. "Design and evaluation of a distributed security framework for the internet of things." *Journal of Signal and Information Processing* 13, no. 1 (2022): 1-23.

[7]. Rivera, Abel O. Gomez, Deepak K. Tosh, and Laurent Njilla. "Scalable blockchain implementation for edge-based internet of things platform." In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*, pp. 1-6. IEEE, 2019.

[8]. Maitra, Sudip, Venkata P. Yanambaka, Deepak Puthal, Ahmed Abdelgawad, and Kumar Yelamarthi. "Integration of Internet of Things and blockchain toward portability and low-energy consumption." *Transactions on Emerging Telecommunications Technologies* 32, no. 6 (2021): e4103.

[9]. Pinjala, Sandeep Kiran, and Krishna M. Sivalingam. "DCACI: A decentralized lightweight capability based access control framework using IOTA for Internet of Things." In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 13-18. IEEE, 2019.

[10]. Novo, Oscar. "Scalable access management in IoT using blockchain: A performance evaluation." *IEEE Internet of Things Journal* 6, no. 3 (2018): 4694-4701.

[11]. Akinbi, Alex, Áine MacDermott, and Aras M. Ismael. "A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models." *Forensic Science International: Digital Investigation* 42 (2022): 301470.

[12]. Sigwart, Marten, Michael Borkowski, Marco Peise, Stefan Schulte, and Stefan Tai. "A secure and extensible blockchain-based data provenance framework for the Internet of Things." *Personal and Ubiquitous Computing* (2020): 1-15.

[13]. Riabi, Imen, Hella Kaffel Ben Ayed, and Leila Azzouz Saidane. "A survey on Blockchain based access control for Internet of Things." In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 502-507. IEEE, 2019.

[14]. Lee, In. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." *Future Internet* 12, no. 9 (2020): 157.

[15]. Sigwart, Marten, Michael Borkowski, Marco Peise, Stefan Schulte, and Stefan Tai. "Blockchain-based data provenance for the internet of things." In *Proceedings of the 9th International Conference on the Internet of Things*, pp. 1-8. 2019.

[16]. Abdel-Basset, Mohamed, Nour Moustafa, and Hossam Hawash. "Privacy-Preserved Cyberattack Detection in Industrial Edge of Things (IEoT): A Blockchain-Orchestrated Federated Learning Approach." *IEEE Transactions on Industrial Informatics* 18, no. 11 (2022): 7920-7934.

[17]. Fatrah, Aicha, Said El Kafhali, Abdelkrim Haqiq, and Khaled Salah. "Proof of concept blockchain-based voting system." In *Proceedings of the 4th International Conference on Big Data and Internet of Things*, pp. 1-5. 2019.

[18]. Nehra, Vibha, Ajay K. Sharma, and Rajiv K. Tripathi. "Blockchain implementation for Internet of Things applications." In *Handbook of Research on Blockchain Technology*, pp. 113-132. Academic Press, 2020.

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022

[19]. Hofman, D., Shannon, C., McManus, B., Lemieux, V., Lam, K., Assadian, S., & Ng, R. (2018, July). Building trust & protecting privacy: Analyzing evidentiary quality in a blockchain proof-of-concept for health research data consent management. In *2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE Smart data (SmartData)* (pp. 1650-1656). IEEE.

[20]. Abdel-Basset, Mohamed, Nour Moustafa, Hossam Hawash, Imran Razzak, Karam M. Sallam, and Osama M. Elkomy. "Federated intrusion detection in blockchain-based smart transportation systems." *IEEE Transactions on Intelligent Transportation Systems* 23, no. 3 (2021): 2523-2537.

[21]. Hasselgren, Anton, Jens-Andreas Hanssen Rensaa, Katina Kralevska, Danilo Gligoroski, and Arild Faxvaag. "Blockchain for increased trust in virtual health care: Proof-of-concept study." *Journal of Medical Internet Research* 23, no. 7 (2021): e28496.

[22]. Steger, Marco, Ali Dorri, Salil S. Kanhere, Kay Römer, Raja Jurdak, and Michael Karner. "Secure wireless automotive software updates using blockchains: A proof of concept." In *Advanced Microsystems for Automotive Applications 2017: Smart Systems Transforming the Automobile*, pp. 137-149. Springer International Publishing, 2018.

[23]. Pešić, Saša, Miloš Radovanović, Mirjana Ivanović, Milenko Tošić, Ognjen Iković, and Dragan Bošković. "Hyperledger fabric blockchain as a service for the IoT: proof of concept." In *Model and Data Engineering: 9th International Conference, MEDI 2019, Toulouse, France, October 28–31, 2019, Proceedings 9*, pp. 172-183. Springer International Publishing, 2019.

Doi: https://doi.org/10.54216/JCIM.100203
Received: May 19, 2022 Accepted: August 15, 2022