Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **44** Issue **S-5 Year 2023** Page **1938:1943***

Analysis of Preventions of Attacks on IOT Using Block Chain: Review

Afsana Anjum

Lecturer, Dept. of Information Technology & Security Jazan University Jazan, KSA
ORCID: 0000-0001-8623-1712

**Corresponding author's E-mail: afsana24sajid@gmail.com*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 06 Nov 2023

Abstract

The increasing acceptance and integration of the Internet of Things (IoT) has made it a prominent element in our everyday existence. Regrettably, a significant level of vulnerability is present in Internet of Things (IoT) devices, which might potentially be abused by malicious actors. The predominant source of security vulnerabilities in IoT systems originates from their centralized architecture. The lack of adequate authentication and access control systems for managing access to information generated by Internet of Things (IoT) devices is a significant concern. Consequently, the issue of verifying the identification of the equipment or communication node arises. The decentralized nature of Blockchain serves as a viable alternative for ensuring secure operations inside a trustless environment. Extensive research has been conducted in the domain of the convergence of Internet of Things (IoT) and Blockchain, yielding notable progress in addressing several significant challenges encountered in the IoT realm. This study investigates the challenges and vulnerabilities associated with the Internet of Things (IoT), as well as explores the potential benefits of integrating Blockchain technology.

Keywords: *Technology, IoT, Blockchain, Security*

1. Introduction

The concept of the Internet of Things (IoT) first gained prominence in 1999 when Wireless Sensor Networks (WSN) and technologies such as Radio-Frequency Identification (RFID) were introduced. The fundamental principle underlying the Internet of Things (IoT) is the interconnection of all objects, enabling seamless connectivity across disparate entities regardless of location or temporal constraints. In order to establish both physical and virtual connections, various devices such as sensors and actuators are employed. The security of the Internet of Things (IoT) is of paramount importance in ensuring the integrity and reliability of IoT infrastructure. The Internet of Things (IoT) facilitates the collection of data from a vast expanse of rural areas through the utilisation of sensors and actuators. The Internet of Things (IoT) has experienced significant growth, facilitating the interconnection of a wide range of devices and networks across several domains such as residential, commercial, transportation, and urban environments.

The Internet of Things (IoT) has facilitated the establishment of a comprehensive operating picture (COP) that spans across diverse applications in contemporary daily life. The achievement of the COP is facilitated by the progress observed in wireless sensor network devices, which possess the capability to engage in network communication, facilitating information exchange and enabling diverse analytical operations. The exclusive method for transmitting information and verifying data within the Internet of Things is through a centralised server, hence giving rise to concerns regarding security and privacy. Device spoofing, fraudulent authentication, and lack of reliability in information sharing are all potential factors to consider. The concept of a central server is eliminated, and blockchain technology is utilised inside the Internet of Things (IoT) framework to address security and privacy concerns. The convergence of Blockchain and IoT offers several anticipated advantages. These include the establishment of trust among entities, ensuring the completeness, consistency, and integrity of stored data, preserving personal data in an immutable and tamper-proof manner, reducing expenses and facilitating cost-effective solutions, enhancing security measures, and enabling faster processing of large volumes of data.

This research investigates the possible security and privacy concerns related to the interaction between components in the Internet of Things (IoT), and explores the possibilities of distributed ledger-based blockchain (DL-BC) technology in addressing these difficulties. In this study, a comprehensive analysis was conducted to investigate the utilisation of BC in specific domains and classifications.During the discussion, certain difficulties pertaining to the Internet of Things (IoT) and IoT with blockchain (BC) were also addressed in order to gain a comprehensive understanding of the contributions made by blockchain technology. According to the second source, [2]

The issue of security pertaining to Internet of Things (IoT) devices is a persistent concern. The user's text does not provide any information or context. The absence of adequate security measures could pose a significant concern, particularly in relation to the utilisation of applications such as smart homes and smart automobiles. For example, a somebody with malicious intent could gain control over an autonomous vehicle that is occupied by a human passenger, or use the authorised privileges of an Internet of Things (IoT) system to engage in financial transactions. The necessity for robust security measures arises from the substantial amount of data that is collected and exchanged among Internet of Things (IoT) devices.

The convergence of the Internet of Things (IoT) and Blockchain has become a prominent subject of discussion, with various industries and fields of application witnessing the emergence of novel use cases that integrate these two technologies. The user did not provide any text to rewrite. Before delving into the overall value of the innovative fusion of Internet of Things (IoT) and Blockchain, it is imperative to bear in mind a few fundamental principles pertaining to these domains. This is essential due to the highly precise and specific language employed within both sectors. The latter half of this essay will examine blockchain technology, which provides users with protection against single points of failure and other challenges, while also eliminating the need for reliance on trusted third parties. The integration of Blockchain technology into the Internet of Things (IoT) ecosystem has garnered significant attention from researchers, prompting them to explore this area further.

In recent years, there has been an emergence of decentralised cryptocurrency systems. The utilisation of blockchain technology in these systems originated with the inception of Bitcoin. Bitcoin enables users to engage in safe transactions and transfer currency (bitcoins) with others, eliminating the necessity for a trusted intermediary. The user's text does not provide any information to rewrite in an academic manner. The blockchain functions as an unchangeable record of blocks that contain timestamps, and this record is distributed among all nodes in the network. This decentralised structure eliminates the necessity for a central governing entity [10]. The aforementioned technology is employed for the purpose of disseminating and retaining data in a decentralised way through a network of peers [11]. In contemporary times, the utilisation of blockchain technology has proven to be highly impactful in facilitating secure and efficient financial transactions [12]. Additionally, it has the potential to serve as a facilitator in various other domains. Examples of decentralised technologies in the field of Internet of Things (IoT) [13], identity-based Public Key Infrastructure (PKI) [14], supply chain management [15], proof of document existence [16], and storage [17–19] can be cited.

IOT Architecture:

IoT has a three-layered architecture. The three layers are as follows:

The primary objective of the application layer is to provide specialised services to its users [5]. The text provides an overview of several Internet of Things (IoT) applications, encompassing domains such as smart homes, healthcare, and urban environments, wherein the technology can be effectively employed.

The network layer is a crucial component of the networking architecture, responsible for facilitating communication between different networks. The layer in question is prone to experiencing attacks, as it is responsible for gathering data from pre-existing infrastructures and transmitting it to upper layers. The data collected by the sensors undergoes processing. The primary security concerns often pertain to the authentication and data integrity during transmission [6].

The Perception Layer, which is commonly known as the physical layer, serves as the foundational component of the Internet of Things architecture. It functions as the cognitive center of the third layer. Within this particular stratum, one can find many sensory constituents such as sensors and actuators. This particular layer is alternatively referred to as the sensor layer [7, 8]. The data presented in Tables 1 and 2.

Issues and Challenges in IoT:

Although the Internet of Things (IoT) presents several benefits and has the potential to address various challenges in diverse sectors, it is not without its own set of challenges. These challenges may manifest as the resolution of security concerns, privacy issues, and other related matters. This section provides a concise overview of the potential challenges that may arise while examining the interaction of IoT components in a study. The user's text is too short to be rewritten in an academic manner.

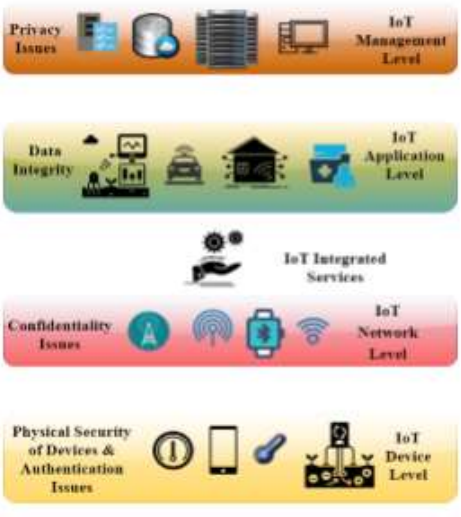
Challenges in IoT

The primary concerns within the realm of Internet of Things (IoT) predominantly pertain to the challenges associated with privacy and security. Furthermore, the concept of interoperability presents several additional barriers, including the absence of standardized protocols, legal complexities, regulatory hurdles, concerns regarding intellectual property rights, issues related to the burgeoning Internet of Things (IoT) market, and several developmental concerns. The user's text does not contain any information or context to be rewritten in an academic manner.

The Internet Society (ISOC) released a paper in 2015, authored by Karen Rose et al., which examines the concerns and challenges related to the Internet of Things (IoT). The research discusses a range of potential issues that have been identified and the manner in which they have been brought to attention. The user's text does not contain any information to rewrite. The difficulties and challenges discussed in Table 1 were summarized.

Security and Privacy Issues in IoT:

Table 1 presents a comprehensive overview of the various manifestations of problems that may arise in the context of the Internet of Things (IoT). The table provides a clear and concise representation of the possibility of these problems occurring, as categorized into seven distinct ways. The subsequent obstacles associated with these concerns are also enumerated. In order to provide clarity on the multifaceted concerns surrounding security and privacy, this study focuses on the examination of interactions among components inside the Internet of Things (IoT) framework. References 22 and 23.



Could Blockchain Technology Can be a Remedy?

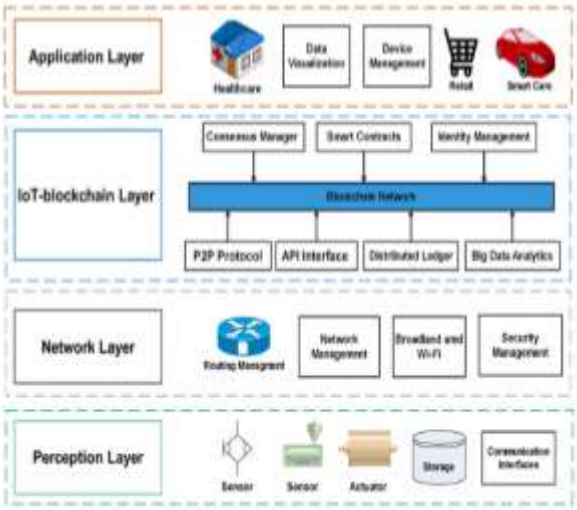
Indeed, Blockchain technology has the potential to serve as a viable solution for mitigating the security and privacy concerns associated with the Internet of Things (IoT). The user's text is too short to be rewritten in an academic manner. The elimination of a centralized server in the Internet of Things (IoT) is made possible by blockchain technology, which enables the secure and verified movement of data across the distributed ledger for each transaction.

The blockchain technology operates as a decentralized ledger system that records and monitors every instance of data modification or removal. A permanent digital signature that is inherently associated with each transaction and possesses an immutable character, hence preventing any alteration or removal. Every gadget would possess strong cryptographic measures due to the implementation of blockchain technology, hence enhancing the level of safe connectivity with other gadgets.

The implementation of blockchain technology has the potential to mitigate the risks associated with distributed denial-of-service (DDoS) attacks, which have been observed to impact many devices simultaneously, as evidenced by recent significant incidents in the realm of Internet of Things (IoT) security.

In light of the extensive array of security measures proposed for IoT devices, encompassing biometrics and two-factor authentication, the use of blockchain technology emerges as a potential solution for enhancing IoT security. The blockchain technology possesses strong security mechanisms that effectively deter unauthorised data manipulation, impose limitations on the connectivity of Internet of Things (IoT) devices, and provide prompt deactivation of compromised IoT network devices.

Within a Blockchain network, the Shared Ledger assumes the crucial responsibility of ascertaining the ownership of assets or transactions. It serves as the sole point of reference for this purpose. According to the study conducted by the authors [4], the participants in the system utilise peer-to-peer replication mechanisms to ensure that they own an identical state of the register. This state is consistently updated following each transaction.



4. Conclusion

Blockchain and IoT:

The comparison between the Biological Internet of Things (BioT) and the Internet of Things (IoT) reveals that while the IoT holds promise, it is hindered by some unresolved challenges that impede the widespread adoption of IoT devices. One of the concerns pertains to a deficiency in trust. In the current centralised Internet of Things (IoT) paradigm, a third-party central authority is employed, exercising full authority over the collection, analysis, and utilisation of data from various IoT devices. Hence, the central authority serves as an opaque entity for IoT users, presenting an attractive proposition for the majority of owners of IoT devices. In contrast, blockchain technology provides a distributed, autonomous, trustless, and decentralised ecosystem. The utilisation of a decentralised design in blockchain enables the utilisation of processing resources from all participating entities, as opposed to the centralised approach. This decentralised approach addresses several concerns associated with a single point of failure, trust, and security. Furthermore, the utilisation of blockchain technology provides enhanced security and data integrity as a result of its inherent attributes of being tamper-proof and immutable. There exist a multitude of parallels and differences between the Internet of Things (IoT) and blockchain technology. The user did not provide any text to rewrite.

Items	IoT	Blockchain
Privacy	Lack of privacy	Ensures the privacy of the participating nodes
Bandwidth	IoT devices have limited bandwidth and resources	High bandwidth consumption
System Structure	Centralized	Decentralized
Scalability	IoT considered to contain a large number of devices	Scales poorly with a large network
Resources	Resource restricted	Resource consuming
Latency	Demands low latency	Block mining is time-consuming
Security	Security is an issue	Has better security

References:

1. Nallapaneni Manoj Kumar et al. / Procedia Computer Science 132 (2018) 1815–1823
2. Ramesh, S. P., Abdulwahid, A. H., Anjum, A., Venkatesh, N., Singh, R., & Chakravarthi, M. K. (2023, March). Designing a Secure Smart Remote Patient Monitoring and Warning System using Big Data and Internet of Things Ecosystems. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1306-1310). IEEE.
3. Christiansen, F. (2020). Predicting Ovarian Malignancy based on Transvaginal Ultrasound Images using Deep Neural Networks.
4. Srinivas, C. M. V., Rena, H., Arunarani, A. R., Naitik, S. T., Al Ansari, M. S., & Younas, A. (2023, August). Improved Red Deer Algorithm for Scientific Workflow Scheduling in Cloud Environment. In *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 662-667). IEEE.
5. Younes ABBASSI, Habib Benlahmera, "IoT and Blockchain combined for decentralized security" August 2021, https://creativecommons.org/licenses/by-nc-nd/4.0
6. Al-Fuqaha, A., Guizani,M.,Mohammadi, M.,Aledhari,M., &Ayyash, M.(2015). Internetof things: Asurveyonenablingtechnologies,protocols,andapplications.IEEECommunications Surveys & Tutorials, 17(4), 2347–2376.
7. Siddiqua, A., Anjum, A., Kondapalli, S., & Kaur, C. (2023, January). Regulating and monitoring IoT controlled solar power plant by ML. In *2023 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-4). IEEE.
8. Pongle, P., & Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. In 2015 International Conference on Pervasive Computing (ICPC) (pp. 1–6). IEEE.
9. Tsai, C. W., Lai, C. F., & Vasilakos, A. V. (2014). Future Internet of Things: Open issues and challenges. Wireless Networks, 20(8), 2201–2217.
10. 8. Sethi,P.,&Sarangi,S.R.(2017).Internetofthings:Architectures,protocols,andapplications. Journal of Electrical and Computer Engineering.
11. Kaur, C., Kumar, M. S., Anjum, A., Binda, M. B., Mallu, M. R., & Al Ansari, M. S. (2023). Chronic Kidney Disease Prediction Using Machine Learning. *Journal of Advances in Information Technology*, *14*(2).
12. Arunarani, S. Selvanayaki, M. Saleh Al Ansari, M. A. Ala Walid, N. Devireddy and M. M. Keerthi, "Crop Yield Prediction Using Spatio Temporal CNN and Multimodal Remote Sensing," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 1042-1048, doi: 10.1109/ICECAA58104.2023.10212267.
13. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008.
14. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy, arXiv:1712.02969 , Dec 2017.
15. Andino Maseleno, D. D., Ashok, K., Al Ansari, M. S., Satheesh, N., & Reddy, R. V. K. An Ensemble Learning Approach for Multi-Modal Medical Image Fusion using Deep Convolutional Neural Networks.
16. Anjum, A., Kaur, D. C., Kondapalli, S., Hussain, M. A., Begum, A. U., Hassen, S. M., ... & Osman Abdalraheem, D. M. H. (2021). A Mysterious and Darkside of The Darknet: A Qualitative Study. *Webology*, *18*(4).
17. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smar Contracts," in 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, August 2016.
18. Nagabhooshanam, N., Murthy, C. R., & CosioBorda, R. F. (2023). Neural network based single index evaluation for SQL injection attack detection in health care data. *Measurement: Sensors*, *27*, 100779.
19. Blockchain for Financial Services. Accessed: Mar. 25, 2018. Online. Available: https://www.ibm.com/blockchain/financialservices
20. Anjum, A., Siddiqua, A., Sabeer, S., Kondapalli, S., Kaur, C., & Rafi, K. (2021). Analysis Of Security Threats, Attacks In The Internet Of Things. *Int. J. Mech. Eng*, *6*, 2943-2946.
21. A Decentralized Network for Internet of Things. Accessed: Mar. 25, 2018. Online. Available: https://iotex.io
22. C. Fromknecht and D. Velicanu. (2014). A Decentralized Public Key Infrastructure With Identity Retention. Online. Available: https://eprint.iacr.org/2014/803.pdf

23. Blockchain for Supply Chain. Accessed: Mar. 25, 2018. Online. Available: https://www.ibm.com/blockchain/supply-chain
24. Al Ansari, M. S. (2023). UTILIZATION OF ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) IN THE FIELD OF ENERGY RESEARCH.
25. Proof of Existence. Accessed: Mar. 25, 2018. Online. Available: https://proofofexistence.com
26. S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, ''Storj a peerto-peer cloud storage network,'' White Paper. Accessed: Mar. 25, 2018. Online. Available: https://storj.io/storj.pdf
27. P. Labs. (2018). Filecoin: A Decentralized Storage Network. Online. Available: https://filecoin.io/filecoin.pdf
28. J. Benet. (2014). ''IPFS-content addressed, versioned, P2P file system.'' Online. Available: https://arxiv.org/abs/1407.3561
29. Pal, Y., Nagendram, S., Al Ansari, M. S., Singh, K., Gracious, L. A., & Patil, P. (2023, February). IoT based Weather, Soil, Earthquake, and Air Pollution Monitoring System. In *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 1212-1217). IEEE.
30. "Blockchain technology for security issues and challenges in IoT". (https://creativecommons.org/licenses/by-nc-nd/3.0/)
31. Ahmed Banafa (2017), "Three Major Challenges Facing IoT."IEEE Internet of things, newsletter, March 14, 2017 https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot
32. Karen Rose, Scott Eldridge, Lyman Chapin (2015) "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World."The Internet Society (ISOC), pp. 1-80. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoTOverview-20151221-en.pdf
33. Alkhalaf, Q., Suri, A. R. S., Chandel, S. S., Thapa, S., & Al Ansari, M. S. (2023). Performance investigation of a Scheffler solar cooking system combined with Stirling engine. *Materials Today: Proceedings*.
34. Celent, Interaction between the three components of internet of things.https://qph.ec.quoracdn.net/main-qimga1db8df2497ec1c595ca93deef7b25ca
35. Yisroel Mirsky1,2, Tomer Golomb2 and Yuval Elovici2 "Lightweight Collaborative Anomaly Detection for the IoT using Blockchain", JUNE 2020, Journal of Parallel and Distributed Computing, Elsevier, ISSN: 0743-7315.
36. Mazumdar, N., Sharma, J. K., Shavkatovich, S. N., Uike, D., & Al Ansari, M. S. (2023). Application of distinct multi criteria decision analysis techniques in the manufacturing sector: A comprehensive review.