International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Securing IoT system Access Control using Blockchain-Based Approach

Umar M Mulani[1], Dr. Manoj Patil[2]

Submitted: 06/09/2022 **Accepted:** 26/12/2022

Abstract: There are many reasons to be concerned about the safety and privacy of the Internet of Things (IoT), given its decentralised design and rapid growth. Controlling who can enter a building is a pressing concern. Centralized systems have low scalability and availability, which could cause a bottleneck in performance. This study introduces a novel approach to controlling the distribution of lightweight, decentralised, secure access management of an Internet of Things (IoT) system by combining a multi-agent system and a blockchain. To protect IoT access control and facilitate secure communication between local IoT devices, the proposed method proposes the development of Blockchain Managers (BCMs). In addition, the innovation enables safe connections between fog nodes, Internet of Things gadgets, and cloud servers.

Keywords: IoT, cloud computing, blockchain, and access control.

1. Introduction

The Internet of Things (IoT) is a recent advancement in Internet functionality that enables disparate electronic gadgets to communicate and share data with one another. To rephrase, "the Internet of Things" (IoT) refers to a system of interconnected electronic gadgets. Because each device has its own identifier and can talk to other devices, it enables people and organizations to connect and make crucial strategic decisions. Although the improvements brought about by the Internet of Things (IoT) will improve people's quality of life, there are a number of security concerns that must be addressed, such as those related to system configuration, access control, information storage and management. Security and privacy issues are a major problem for the Internet of Things. Heterogeneity [2] is a key feature of the Internet of Things that creates security concerns. The fundamental objective of the proposed method is to secure the entire IoT architecture, which includes cloud computing, fog nodes, and the communication between IoT devices.

The results of this study can be broken down into the following categories:

A novel blockchain-based architecture for securing an IoT system is the primary contribution of this study. The technique makes use of a multi-agent system with a decentralised access control mechanism.

Among the many Internet of Things (IoT) applications that can benefit from the blockchain technology we developed require a high degree of portability, scalability, and general-purposes.

Our approach is unique in that it uses a private hierarchical blockchain to guarantee the security of each layer of an IoT architecture while also allowing for a massive reduction in traffic overheads by adopting a lightweight consensus mechanism tailored to IoT needs and facilitated by mobile agent software (MAC).

In this paper's second section, we look at IoT's current access control architecture. Blockchain technology and its use in the IoT are introduced briefly in Section 3. The literature review is presented in Section 4. The suggested architecture is described in depth in Section 5. Section 6 wraps up the paper and looks ahead to potential lines of inquiry.

2. Background of Access Control System in IoT

2.1. Access Control in IoT

AC is the authentication and authorization of communication rights and resource access in compliance with security standards and regulations [4]. The process of allowing resources access to certified organizations by specified regulations is known as authorization control (AC).

[1]*Research Scholar,*
Dr. A. P. J. Abdul Kalam University Indore-India
Assistant Professor, Department of Computer Science and Engineering,
Sharad Institute of Technology, College of Engineering, Kolhapur, India.
umar.mulani@gmail.com
[2]*Associate Professor, Department of Computer Science and Engineering*
Dr. A. P. J. Abdul Kalam University Indore-India.
mepatil@gmail.com

A centralized architecture limits ACL's capacity to install cloud-based access control techniques with improved activity administration and tracking. The proliferation of IoT devices is coupled with a surge in the complexity of access restrictions, resulting in complex duty problems.

2.2. Access Control Challenges in IoT

Some of the main issues with using existing access control methods in an IoT setting are as follows:

Utilization of Already Existing Solutions

In spite of extensive study and successful implementation, access control techniques do not readily convert to an IoT architecture due to their complexity and non-conformity to IoT requirements. The processes of adopting, deploying, and settling into a new solution are time-consuming [1].

Methods for regulating access: centralised vs. decentralised

The control rules provided by centralized systems have a single point of failure yet are nonetheless convenient to access..

Adaptability

The growing number of interconnected gadgets is a burden on system administrators everywhere. Scalability is a key feature for a decentralised and distributed access control system, as more and more IoT devices of varying types are being deployed [9].

3. The Use of Blockchain in IoT

A blockchain is a decentralised database that records transactions in groups called blocks. These blocks contain data and are secured with cryptographic hashes (a chain of linked blocks). Editing records is cumbersome because they depend on previous records, as seen in Figure 1; each block comprises of a collection of new data records or transactions, the hash value of the preceding block, and a timestamp verifying the transactions when the league was formed. For security reasons, data stored on a blockchain cannot be modified [10].

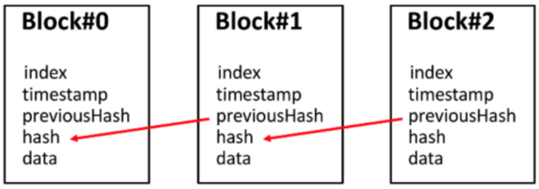


Figure 1. The components and basic architecture of the blockchain

3. Related Work

With some overlap, the relevant work in this paper can be classified into three broad categories: multi-agent systems for access control [27], existing security control solutions in IoT, and IoT access management using blockchain.

By combining secure session key generation, user anonymity maintenance, and mutual authentication, Ndibanje et al. [14] increased productivity while keeping communication costs to a minimum. But this tactic must guarantee the authenticity of transmitted communications.

In order to allow or disallow certain actions, Touati et al. [16] presented a framework to control activities based on user and system preferences (a broader version of context-aware access control). For DAP, they used ciphertext-policy attribute-based encryption in conjunction with a finite state machine (CP-ABE).

Additionally, Touati et al[17] .'s batch-based CP-ABE solution relied heavily on the key/attribute revocation problem. The proposed method decreases complexity and overhead while doing away with the requirement for additional processing nodes. The Cap-BAC method for managing access to services is founded on the principle of least privilege. To gain access to the necessary resources, the service provider must first verify the user's identity via an authorization certificate.

4. RESEARCH METHODOLOGY

As a result of the digitization of traditional cloud data, cloud services confront several difficult challenges, such as document storage and securely sharing information. Users must spend a significant amount of time querying the necessary data when accessing share records, but the results are only sometimes accurate, and access is occasionally restricted and insecure. One of the most critical tasks in the federated cloud is the upkeep of the cloud record store and the secure data sharing. A loss of confidentiality does not influence the safety of store records in this system. Still, a loss of integrity can have profound effects, such as an unknown individual entering a system containing personal and protected data. As a result, safeguarding the cloud storage of documents is critical. Modern federated cloud systems suffer from data privacy, security, and integrity, in addition to being extremely sophisticated and expensive. However, greater store record monitoring and administration will alleviate these complexity and security issues. Cryptographic cloud security has enormous potential for the cloud sector because it is trustworthy and decentralized. The main concerns of store record management are data management and data distribution, verification, and immutability. Employing cryptographic cloud security in cloud databases has several advantages due to its capacity to update record interoperability systems, which enhances access to records, tracking, secure systems, and user assets, among other things. Because cryptographic cloud security can considerably improve cloud services, virtual access to store records is required. As a result, it is critical to design a system that employs cryptographic cloud security to provide authentication while also providing cloud records and resource management integrity. The proposal's primary purpose is to provide a hybrid meta-heuristic-based Cryptographic Ciphertext Policy-Attribute-based encryption (CCP-ABE) based on permission secure blocks to ensure data secrecy and access control of cloud data while ensuring effective resource management. This architecture's phases comprise (a) data collection on virtual clouds and resource management, (b) CCP-ABE using a hybrid heuristic method, and (c) permission cloud blocks for security. In this situation, the enhanced meta-heuristic concept will be built throughout the encryption phases and will return optimized versions of all attributes from the cloud records. As a result, by reducing the ciphertext size, the optimization idea lowers the cost of encryption and transmission. In this case, attribute optimization in CCP-ABE will be performed using a hybrid method that combines the Grasshopper Optimization Algorithm [15] and the Deer Hunting Optimization Algorithm (DHOA) [16]. The performance study reveals that the proposed system is reliable and robust compared to current standard architectures. The proposed model is depicted in Fig. 2.

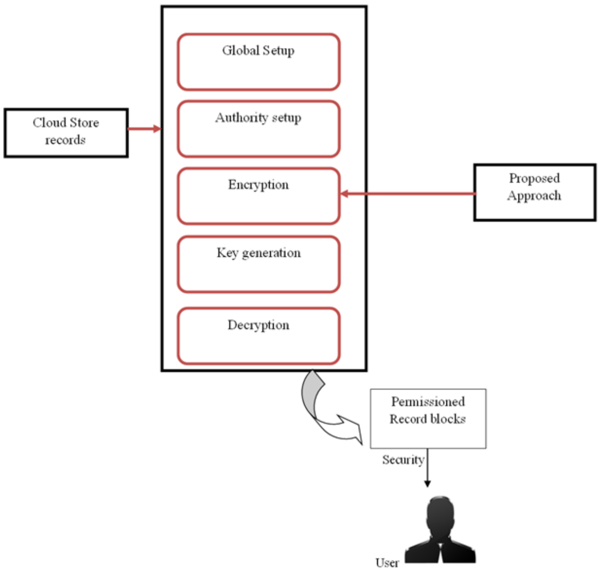


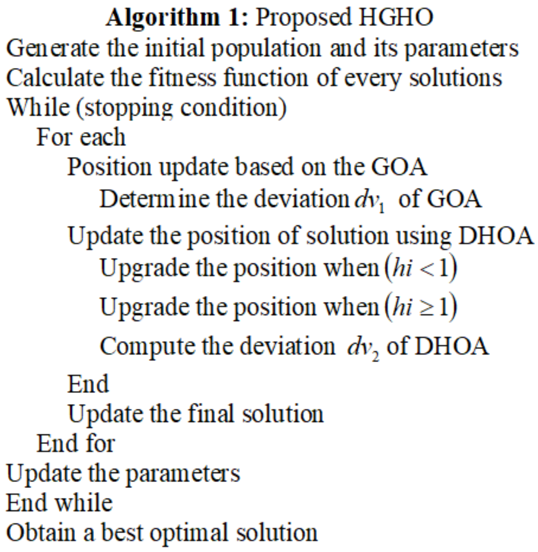
Figure 2: Diagrammatic representation of the proposed model using permissioned Record blocks using cryptography

4.1 Proposed Algorithm

The developed permissioned blockchain-based secured cloud to store data introduces choosing the optimal key for the encryption of medical text data to make highly secured cloud records. GOA [26] is used in the developed model owing to its improved efficiency in determining the optimal solution and does not undergo the optimum local problem. The developed approach is enclosed with the deviation-based concept for updating the final position of candidates to obtain the optimal solution. First, the GOA deviation is estimated with "the solution in GOA without any computations in it that is represented by dv_1". Similarly, the DHOA deviation is computed and expressed dv_2 without any computation in the DHOA. The final position upgrade is taken place as shown in Eq. (2).

$$Pos = Pos + dv_1 + dv_2 \qquad (2)$$

The pseudo-code of the proposed GHO is given in Algorithm 1. Here, the successor position of the hunter is depicted as Xt^{sp} . Then, determine the fitness value for every search agent and update both the leader and successor post until the stopping condition is satisfied. Finally, the best solution is attained.



Algorithm 1: Proposed HGHO

```
Generate the initial population and its parameters
Calculate the fitness function of every solutions
While (stopping condition)
    For each
        Position update based on the GOA
            Determine the deviation $dv_1$ of GOA
        Update the position of solution using DHOA
            Upgrade the position when $(hi < 1)$
            Upgrade the position when $(hi \geq 1)$
            Compute the deviation $dv_2$ of DHOA
        End
        Update the final solution
    End for
Update the parameters
End while
Obtain a best optimal solution
```

STEPS AND ALGORITHM DEFINITIONS FOR PERMISSIONED BLOCKCHAIN-BASED EHR SECURITY

Permissioned Blockchain Steps

The Cloud data sharing scheme is involved on the permissioned blockchain enclosed with different steps and six different algorithms as given below.

System Initialization:

$\text{Setup}(\lambda) \rightarrow (Pu, Sk)$: Here, the setup algorithm is processed with the help of the system manager. The input is obtained as a security parameter λ and the output as the master secret key Sk and public parameters Pu .

Key Generation:

$\text{KeyGen}(Sk, Pu, Su) \rightarrow TK$: Here, the secret key generation algorithm is involved and controlled by the system manager. The input is acquired as the attribute set Su of a user, public parameters Pu and master secret key Sk . Similarly, the output is regarded as the secret key TK .

Data Storage:

$Enc(Pu, S, U, N) \rightarrow (J, D)$ Here, the encryption algorithm is used, which the doctor handles. The EHRs N, keywords set U of shared cloud records, access control structure S of patient Pt and public parameters Pu are used as the input for the algorithm. The output is accomplished to be a ciphertext D and keywords index J.

Data Query:

$\mathrm{Trapdoor}(Pu, U', TK) \rightarrow S_{U'}$ The user handles the trapdoor generation algorithm, where the input is acquired as the secret key TK, search keywords set U' and public parameters Pu, and the algorithm's output is attained as search trapdoor $S_{U'}$.

$\mathrm{Search}(J, S_{U'}) \rightarrow D$: Here, the search algorithm is processed with the support of participants, who are presented in the permissioned blockchain. Here, the input is acquired as the search trapdoor $S_{U'}$ and keywords index J and the output is received as the ciphertext D.

Data Decryption:

$\mathrm{Decrypt}(Pu, Sk, D) \rightarrow N$: The user is accessed with the decryption algorithm with the input as ciphertext D, secret key Sk and public parameters Pu. Finally, the decryption algorithm provides the message N as the output.

5. Results and Discussions

Experimental setup

The permissioned blockchain-based secured cloud storage model is developed in Python, and further analysis was conducted to verify the system's transactional latency, time taken, and effectiveness. The evaluation was made between the developed and state-of-the-art methods to show improvement in the blockchain-based cloud data transmission model. The population size of 10 and the maximum count of iterations as 100 was utilized in the developed model [29]. The proposed CCP-ABE was distinguished from other existing algorithms like “ Whale Optimization Algorithm (WOA) [28], Coronavirus Herd Immunity Optimization (CHIO) [29], GOA [26] and DHOA [27], and machine learning algorithms like BIoTHR [3] and EACMS [4]”.

Convergence analysis

The convergence rate of the proposed model is evaluated with different existing algorithms at the increasing iterations as depicted in Fig. 3. The proposed CCP-ABE-based EHR transmission model secures less ciphertext size, computation cost, and encryption cost by tuning the encrypted keys for encryption and decryption, which is observed by comparing with the conventional optimization techniques. The betterment of the proposed model is observed to be 14.2%, 13.3%, 12.02% and 12.4% enhanced than WOA-CCP-ABE, CHIO-CCP-ABE, GOA-CCP-ABE, and DHOA-CCP-ABE, respectively at the 40th iterations. Hence, it is verified that the suggested HGHO-CCP-ABE-based model has secured the cloud store data transmission with superior performance.

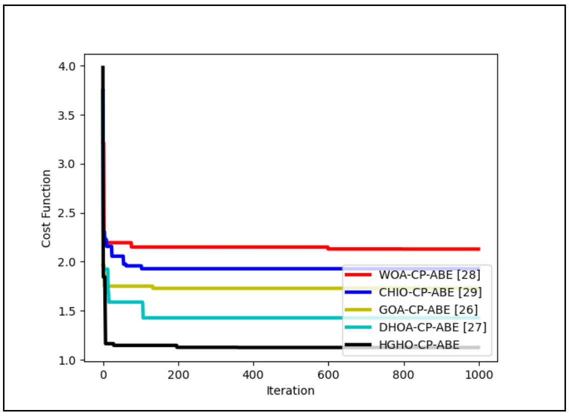
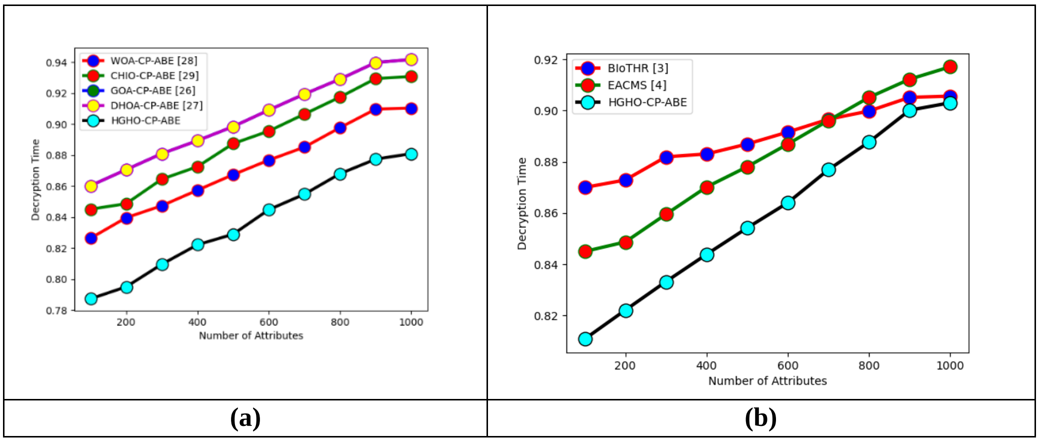


Figure 03: Convergence analysis on proposed permissioned blockchain-based secured Cloud storage data model

Decryption time analysis

The proposed model based on the heuristic-based CCP-ABE approach is analyzed to show efficient decryption performance with its time efficiency as in Fig. 4. Here, the analyses are done between the algorithms and other baseline approaches. The developed method reveals a minimum decryption time for retrieving the medical records, where the proposed model is 11.67% and 13.6% superior to BIoTHR and EACMS, respectively.

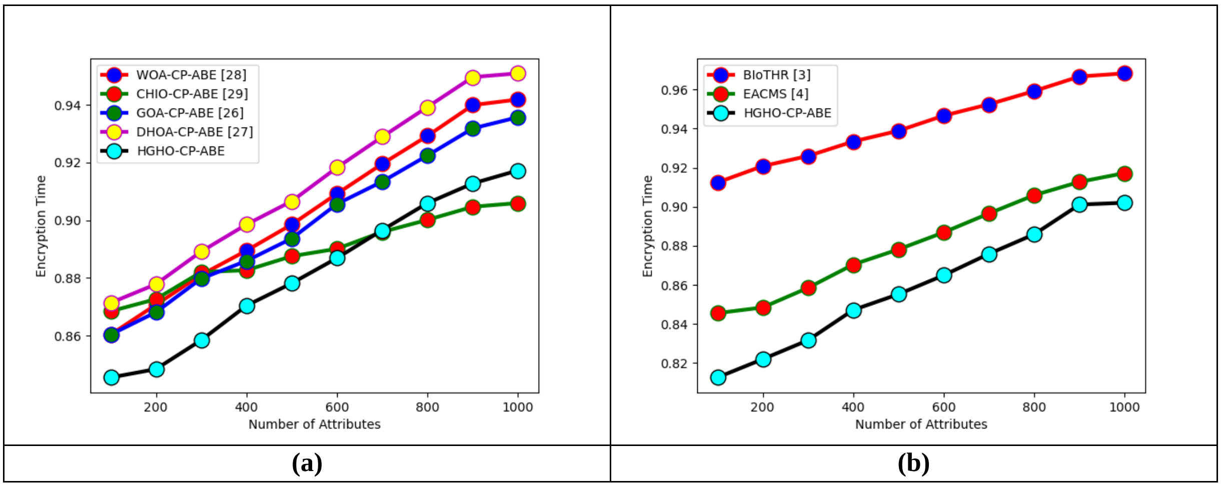


(a) (b)

Figure 04: Decryption time analysis on proposed permissioned blockchain-based secured cloud storage model with "(a) different heuristic algorithms and (b) existing models"

Encryption time analysis

The evaluation was made between the proposed and conventional algorithms to check the encryption time of the cloud records as in Fig. 5. The proposed CCP-ABE shows 12.6% and 13.2% improved than BIoTHR and EACMS, which demonstrates that less encryption time is required for the proposed model.



(a) (b)

Figure 05: Encryption time analysis on proposed permissioned blockchain-based secured cloud storage model with "(a) different heuristic algorithms and (b) existing models"

6. Conclusions and Future Works

There are a number of privacy and security issues that need fixing with IoT devices. There are benefits and drawbacks to both centralised and decentralised methods. While centralised approaches have scaling limitations, decentralised ones are limited by latency, computational cost, and energy concerns. Our group proposed a multi-agent architecture to facilitate low-overhead, distributed approaches to protecting the Internet of Things from malicious actors. All of the security needs of cloud computing, local IoT device connectivity, fog node security, core fog node security, and access control may be met via blockchain management. The suggested architecture is adaptable and might be used in a wide variety of Internet of Things (IoT) use cases. The focus of earlier studies has been on access control issues in niche IoT applications like smart homes, rather than general IoT barriers, hence this has limited their ability to solve broader IoT issues. The writers understand that it is during the testing and implementation phases where the solution's applicability and effectiveness in relation to similar research can be assessed. Though this study is still in its infancy, the authors believe that the findings from these two phases should be revealed independently due to the expected need to give substantial more material and new perspectives.

Using the proposed paradigm, future studies can assess whether or not the four core security goals—integrity via digital signatures, authentication via shared secret keys, authorization via the MAC policy, and confidentiality via public key encryption—have been met. The issue of the blockchain's extremely large header size will be discussed, as well as potential remedies. One solution is to remove the header block's access control policy from the blockchain's block structure and store it in a separate policy file, such as an encrypted text file. We will present a case study of IoT applications that require stringent security to back up our proposed architecture. A Raspberry PI internet of things device and a private blockchain platform will be used to implement the solution. Subsequent works will provide further detail.

References:

[1]. Zhao, Z., Zhou, H., Li, C., Tang, J., Zeng, Q. Deepemlan: deep embedding learning for attributed networks. Inf. Sci. 543, 382–397 (2021)

[2]. Pooranian Z, Shojafar M, Garg S, Taheri R, Tafazolli R (2021) LEVER: secure Deduplicated cloud storage with EncryptedTwo-party interactions in cyber-physical systems. IEEE Transact Industrial Informatics. https://doi.org/10.1109/TII.2020.3021013

[3]. Narendra, M. Research Reveals the Most Vulnerable IoT Devices. Available online: https://gdpr.report/news/2019/06/12 /research-reveals-themost-vulnerable-iot-devices/ (accessed on 11 January 2021).

[4]. NTT Innovation Institute. Mandatory Access Control over IoT Communications. Available online: https://labevent.ecl.ntt.co.jp/ forum2017/elements/pdf_eng/03/C-18_e.pdf (accessed on 16 November 2020).

[5]. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in Internet of Things: Challenges and Solutions. Yingyong Kexue Xuebao/J. Appl. Sci. 2020, 38, 22–33. [CrossRef]

[6]. Saad M, et al. (2020) Exploring the Attack Surface of Blockchain: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, 22(3):1977–2008

[7]. Chen, C.H., Lu, C.Y., Lin, C.B.: An intelligence approach for group stock portfolio optimization with a trading mechanism. Knowl. Inf. Syst. **62**(1), 287–316 (2020)

[8]. Liu Y, Yu F, Li X, Ji H, Leung VM (2020) Blockchain and machine learning for Communications and networking systems. IEEE Commun Survey Tutorials 22(2):1392–1431. https://doi.org/10.1109/COMST.2020.2975911

[9]. Zhao, Z., Zhang, X., Zhou, H., Li, C., Gong, M., Wang, Y.: Hetnerec: Heterogeneous network embedding based recommendation. Knowl. Based Syst. 204, 106218 (2020)

[10]. Fu X, Yu FR, Wang J, Qi Q, Liao J (2019) Resource Allocation for Blockchain-Enabled Distributed Network Function Virtualization (NFV) with Mobile Edge Cloud (MEC), IEEE INFOCOM 2019. In: IEEE conference on computer Communications workshops (INFOCOM WKSHPS), Paris, France, pp 1–6

[11]. Belotti M, Bozic N, Pujolle G et al (2019) A Vademecum on Blockchain Technologies: When, Which and How. IEEE Commun Surveys Tutorials 21(4):3796–3838. https://doi.org/10.1109/COMST.2019.2928178

[12]. Ali M, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehman M (2019) Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Commun Survey Tutorials 21(2):1676–1717

[13]. Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. J. Netw. Comput. Appl. 2019, 144, 79–101. [CrossRef]

[14]. Gao, W.; Hatcher, W.G.; Yu, W. A survey of blockchain: Techniques, applications, and challenges. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018. [CrossRef]

[15]. Aldowah, H.; Rehman, S.U.; Umar, I. Security in Internet of Things: Issues, Challenges and Solutions. In International Conference of Reliable Information and Communication Technology; Springer: Cham, Switzerland, 2018; pp. 396–405.

[16]. Ourad, A.Z.; Belgacem, B.; Salah, K. Using blockchain for IOT access control and authentication management. In International Conference on Internet of Things 2018 June; Springer: Cham, Switzerland, 2018; pp. 150–164.

[17]. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in Iot. In Europe and MENA Cooperation Advances in Information and Communication Technologies; Springer: Cham, Switzerland, 2017; pp. 523–533. [CrossRef]

[18]. Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. Comput. Netw. 2017, 112, 237–262. [CrossRef]

[19]. Ahmed, E.; Yaqoob, I.; Hashem, I.A.T.; Khan, I.; Ahmed, A.I.A.; Imran, M.; Vasilakos, A.V. The role of big data analytics in Internet of Things. Comput. Netw. 2017, 129, 459–471. [Google Scholar] [CrossRef]

[20]. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun. Policy 2017, 41, 1027–1038. [Google Scholar] [CrossRef]

[21]. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173–190. [Google Scholar] [CrossRef]

[22]. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Gener. Comput. Syst. 2019, 100, 325–343. [Google Scholar] [CrossRef]

[23]. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. Comput. Commun. 2019, 136, 10–29. [Google Scholar] [CrossRef]

[24]. Global, T.F. History of Blockchain. 2019. Available online:

https://www.tradefinanceglobal.com/blockchain/history-of-blockchain/ (accessed on 22 November 2020).

[25]. Buterin, V. A next-generation smart contract and decentralized application platform. White Pap. 2014, 3, 1–36. [Google Scholar]

[26]. The 5 Best Blockchain Platforms for Enterprises and What Makes Them A Good Fit. 2019. Available online: https://medium.com/swishlabs/the-5-best-blockchain-platforms-for-enterprises-and-what-makes-them-a-good-fit-1b44a9be59d4 (accessed on 7 September 2021).

[27]. Lu, Y. The blockchain: State-of-the-art and research challenges. J. Ind. Inf. Integr. 2019, 15, 80–90. [Google Scholar] [CrossRef]

[28]. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. 2018, 6, 2188–2204. [Google Scholar] [CrossRef]

[29]. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411. [Google Scholar] [CrossRef]