Comprehensive Survey and Research Directions on Blockchain IoT Access Control

Hafiz Adnan Hussain[1], Zulkefli Mansor[2], Zarina Shukur[3]
Faculty of Science and Information Technology
The National University of Malaysia
Bandar Baru Bangi, 43000
Selangor, Malaysia

***Abstract*—The Internet of Things (IoT) is a widely used technology in the last decade in different applications. The Internet of things is wirelessly or wired to communicate, store, compute and track various real-time scenarios. This survey mainly discussed the core problems of Internet of things security and access control to unauthorized users and security requirements for IoT. The Internet of things is a heterogeneous device and has low memory, less processing power because of the small sizes. Nowadays, IoT systems are not sure and powerless to protect themselves against cyber attacks. It is mainly due to inadequate space in IoT gadgets, immature standards, and the lack of protected hardware and software design, development, and deployment. To meet IoT requirements, the authors discussed the limitations of traditional access control. Then the authors examined the potential to spread access control by implementing the safe architecture accommodated by the Blockchain. The authors also addressed how to use the Blockchain to work with and resolve some of the standards relevant to IoT security issues. In the end, an analysis of this survey shows future, open-ended problems, and challenges. It offers how the Blockchain potentially ensures reliable, scalable, and more efficient security solutions for IoT and further research work.**

***Keywords*—Blockchain; Internet of Things; IoT; access control; access control management**

I. Introduction

Internet of Things (IoT) is an infrastructure of smart things that exchange information over the Internet. In a different world, the Internet of things is used to obtain data, and certain events are triggered. The linked IoT devices are expected to be 50 billion in late 2020, according to CISCO. As the entire world population grows, the advancement of IoT devices is rapidly evolving. There seem to be enormous data produced by IoT devices. The infinite interlinking between physical and virtual objects notably stimulates processing, storage, and data exchange on the IoT. It is a primary base for rendering services in critical areas such as hospitals, cars, bridges, schools, retail outlets, public constructions, communities, and even within human bodies in the form of wearable devices. The foremost issues are how can efficiently handle services and data collected by IoT devices because they can contain personal information or even save people's lives. There are many difficulties in implementing IoT. In numerous IoT implementations, uniformity, interoperability, data management, processing, user authentication, identity, confidentiality, completeness, affordability, protection, and privacy are among the several open challenges. One of the famous approaches for data protection and privacy is making sure only validated and accredited users can see that data [1]. Data is coming massively from these devices, storing data to make sure it is secured and protected from hackers, and authenticating the user who wants to access that data is the correct user on the server. The authenticated user must have limited access to limited data.

Access control is a collection of rules and policies that enable a nominated user to be enabled or not accessed by users, services, procedures, or other approved mechanisms to access or limit access to an information system's resources. It decides whether or not the requirement for access to the related order is allowed [2]. Various concepts, like access control policy, layout, and method, have established a basis for developing an access control system. The access control policies form the basis for access arrangements implemented through the mechanisms for access control. The essential parts of the access control system are the object, subject, and owner of the thing. The current element is a subject that requests access to objects. The object is a receptive element in a system that is petitioned by the subject. The connection to an object determines access to documents, areas, directories, programs, and network nodes to its information. The network is also recognized as objects-related devices, including smart devices, routers, and mechanical elements. The owner of each entity defines access policies and supplies the necessary authorizations.

In IoT access control systems, certain restrictions are imposed because they have a complex and clustered infrastructure that does not meet the wide variety of IoT gadgets and the versatility situation in which nodes can connect and drop the network. IoT devices often need a lightweight low-latency access control system for CPUs, memory, and battery life [3]. Numerous literature attempts to create a distributed IoT control monitor utilizing edge paradigms such as Adhoc Web Cloud and Fog Computing by reducing the mentioned problems. However, due to the absence of trusted entities working to provide arbitrary services, the security problem persists. For example, a group of vehicles can accommodate road security assistance to other transports under traffic networks.

Blockchain is a Peer-to-Peer (P2P) distributed and decentralized public ledger over the network [4, 5]. It is used to

store transactions, events, and smart contracts. The smart contract includes a programable code that any customer can create and publish in the Blockchain as a transaction [6]. It has a specific number assigned by Blockchain. The contract is executed when the Blockchain user or smart contract calls it, and the smart contracts can communicate, among others. The first Blockchain scenario is a shared P2P digital currency. It is a service for high-security distributed applications with the introduction of a smart contract framework. Therefore, to make a distributed IoT access control, this paper can exploit the latest use of Blockchain as a distributed and decentralized infrastructure.

The rest of the paper is organized as in Section 2; related research work based on Blockchain in IoT access control like problems and limitations of traditional access models are identified. The security requirements for IoT are described in Section 3. Analysis and discussion of the entire survey are summarized in Section 4. Future research directions and open challenges are described in Section 5. The paper concludes with a conclusion of the work done in Section 6.

II. Related Research Work on Blockchain-based Access Control for IoT

A. Access Control and IoT

Reference [7] provides a full detailed review of various IoT access control solutions. The study shows that the new access control method employed in IoT and claims that Internet protocols widely used cannot be extended to compelled environments. Based on its comprehensive review of the literature, [7] Identify and Lines of 3 access control and decentralized authorization solutions: the IBM Adept (Autonomous Decentralized P2P Telemetry) [8] framework, DOAuth (Decentralized Open Authentication), and FairAccess [9, 10]. However, in these references, the author explained the OAuth-based access control solutions are the heavy mechanism for IoT situations because of their low processing overhead and communications. Lastly, IBM Adept offers a collaboration and file storage system to develop IoT apps without creating a process for access control. Further, [7] passed over the work has done in the IETF called CoAP Management Interface (CoMI) [11], and the result is done by the Open Mobile Alliance (OMA) called LWM2M [12] CoMI and LWM2M are primary mechanisms in a centralized environment for IoT device management.

B. Blockchain and IoT

This paper identified two main access control patterns using Blockchain, access control depending on the transaction and access control depending on the smart contract. Their pros and cons are summarized in Table I.

1) Access control depending on the transaction: Conoscenti et al. [13] performed systematic literature on the new technology Blockchain for the IoT. The study mentioned many articles that handle the data gathered from IoT devices. For example, [14] shows a method for verifying the status of the data, and [15] reports the procedure for maintaining the data holding of IoT gadgets. None of the mentioned research articles suggest an architecture. The administrators can control the entire IoT life cycle access policies rather than their roots or location. The best of experience, the old work relevant to Blockchain access control for IoT, is [9] that shows a cryptocurrency Blockchain access control structure called FairAccess. Nevertheless, Access Control Policies describe the creation of transactions for that Smart Contract by creating various Smart Contracts for the Access Control Policy of each source request pair that are not suitable for the IoT environment.

The authors in [16] suggested a new method of Authentication of access control and a user to make IoT secure and safe for illegal users and get open access to information. The proposed system is based on the following: i) Registration Authority (RA), and ii). Home Registration Authority (HRA). The RA was created to simplify the authentication system for IoT gadgets. Each device should be registered with the RA.

The authors in [17, 18] suggest a multi-tier Blockchain base system for sharing data between communities and individuals for users and IoT gadgets. The mentioned design has three key components: data management protocol, data storage mechanism, and message services. The data management system offers a structure for the data manager, data requestor, or correspondence channel. The messaging tool used in this context increases device scalability by publishing / subscribing patterns. In the end, Blockchain uses data storage systems to store data anonymously.

In [19], The author proposed the Blockchain base design to enforce the access control mechanism based on the attribute. The policies are formulated by XACML and processed in Blockchain as compressed transactions. The smart contract codes all the elements needed for policy assessment. Authors design storage and maintenance feature by utilizing innovative contracts. It reflects self-assessment procedures pursued straightforwardly and transparently when the user is requesting access. This method merges smart contract and transaction structures to create an access control system that allows users to understand the policies that affect their access requests. It offers a centralized audit system and identifies sections that are fraudulently modifying the rights given by executable policies. Proof of the concept (PoS) implemented in the above method by using the Ethereum Blockchain to show and verify the proposal's validity.

2) Access control depending on smart contract: In the Alphand, Amoretti [20] architecture based in Blockchain, the authors propose secure management of access resources from end to end, named IoT Chain. Resources servers of resource owners hold their resources through a proxy server in an encrypted and signed format [21]. The third party who requests access to protected resources is the customer. It calls for a critical server decryption key, which checks that a blockchain is allowed to contain. The approval process works in the following way: the resource owner establishes and publishes an intelligent contract for customers in the Blockchain. If certain conditions are met, the customer calls the relevant, intelligent contract to produce an access token. The permission tokens are not sent to the customer but stored

in the permanent memory of the transaction. The Client must seek the appropriate key to decrypt resources of the critical server, a node Blockchain, and hold a duplicate file of the Blockchain ledger once a token has been stored in an internal Contract database. At this point, the critical server tests that the Client has a token and transfers the key using a DTLS mode on Blockchain's smart contract system. The Client then installs and decrypts the encrypted device from the proxy server—this approach is primarily designed to replace a trusted ACE request system with a secure Blockchain permit.

In [22], the authors: described the main issues in the IoT access management system. The first is due to the core architecture, and the second is because access policies are handled dynamically. If the data is satisfied by the requester's access policies, the control contract is executed automatically, and a token of authorization is created and allocated to the requester. The input information relates to trust and reputation safety parameters to assists the resource owner in dynamically develop or change security policies. Order in verifying its validity; however, the model proposed requires evidence of description.

In [23] proposed the machine learning algorithms, and Smart contract access management checks the efficiency of multiple user access to a shared resource by maintaining sophisticated access control. The network architecture is made up of a single Judge Contract (JC), multiple Access Contracts (ACCs), and one Register Agreement (RC). Per ACC describes a subject-resource pair access control system and applies to update access control rules. A record of misconduct is maintained in the ACC smart contract for each property. It describes the actions of the subject matter of this platform, with several requests being identified in a short time and the decision of the Judge Contract (JC) penalty. The ACC is performed once an individual has been appointed to obtain access, and the ACC reports to the JC contract if the misconduct is detected. Based on an incorrect evaluation method, the contract for JC shows the appropriate penalty as a temporary blocking of subject access.

The author in [24] performed an access control and smart contract verification to tackle an IoT device security scalability problem. In reality, one or more IoT devices are operated by a customer, and each device needs its credentials. In this instance, however, the user should authenticate independently on each unit. This approach results in overhead verification and is challenging to measure. The main reason for using a smart contract is the validation of the user and IoT. The user signs up for the smart contract, verifying device identity by using the Ethereum wallet address. It is performed and examined in the blockchain environment of Ethereum. [25] introduces the Blockchain-enabled fog nodes for user authentication and authorization. The fog nodes manage and validating the authenticity of access to IoT devices on the Ethereum network interface. The system manager uses a smart contract to map all of the registered fog nodes and their associated IoT devices. Besides, it consists of the collection and permissions for entry to registered users. The arrangement includes the functionalities of registration, Authentication, and access control IoT device user link with a contract to verify the validity of the user. A token with access parameters is created if Authentication is successful. The next step is to sign the token and send it to the fog node to monitor the resource. The signature and token specifications are verified, and user access to the IoT gadgets is then granted or denied. A safe SSL connection between the user and the IoT device will be established for data exchange.

TABLE I. PROS AND CONS OF REFERRED ACCESS CONTROL SOLUTIONS

Ref.	Pros	Cons	Security Measures	Implemented
[7]	The authors highlighted how each solution produced various security specifications. They declared that centralized and distributed methods could complement each other.	Access Control Policies describe the creation of transactions for that Smart Contract by creating various Smart Contract to assign different Access Control Policy of each resource-request pair that are not suitable for the IoT environment.	VL	NA
[16]	IoT safe and secure for unauthorized users and open access This approach is secure for a man-in-the-middle attack	Critical scalability: The need for every device to have a RA and, similarly, for every user to have HRA could be a constraint for scalability	M	NO
[17]	Keep data privately Decentralized, open, and accessible data collected from data storage and architecture elements	Simple to do, but not feasible in all situations, as a large amount of computer power is needed for every node. It sends to the "Server," which decrypts an encrypted version of the info.	H	YES
[19]	Self-assessment policies continued in a straightforward and transparent way This model connects transactions and smart contract structures to create an access control system.	It offers a centralized audit system and identifies sections that are fraudulently modifying the rights granted by enforceable policies	VL	NO
[20]	Blockchain-focused IoTChain with ACE and OSCAR (IoT Object Security Architecture) authority. The suspect method to handle approval when OSCAR uses the public registry to create multidisciplinary groups for authorized customers.	Difficult to preserving the availability of the IoT	M	YES
[23]	To carry out centralized, secure access management for IoT networks, the author proposed a smart contract-based architecture composed of different access control contracts, an authority contract, and a registered agreement.	A large amount of contract requirements for a massive crowd is a daunting task.	M	YES
[24]	In a smart contract, users are authenticated, and an IoT token is issued. The contract decides whether the user will access the services and transmits tokens to the consumer and the required IoT computer.	For large IoT networks, this method suffers from the scalability problems associated with Blockchain. Ethereum smart contracts have the biggest drawback of fluctuating Ethereum rates, which is a problem for the consumers.	H	YES

III. Security Requirements for IoT

Various mechanisms and parameters must be considered, as listed below, for a secure IoT deployment.

A. Data Integrity, Privacy, and Confidentiality

When IoT data move across multiple hops throughout the network, a conventional encryption process is needed to guarantee data confidentiality [26]. Since systems, frameworks, and networks are configured differently, data held on a device are susceptible to protection and privacy infringement by disturbing live IoT network nodes. Attack vulnerable IoT devices may enable an intruder to contact data integrity by malicious data handling.

B. Accounting, Authentication, and Authorization

Authentication is needed for two parties to interact with each other to secure communication in IoT. Applications must be encrypted for exclusive access to services. The variation of IoT authentication procedure lives primarily because of different heterogeneous architectures and environments that help IoT gadgets. Such conditions pose a complexity in defining the standard global IoT authentication protocol [27]. Same as the authorization mechanisms guarantee that authorized persons have access to the systems or information. Usual authorization and authentication results are implemented in a stable environment that guarantees a protected communication environment. Moreover, accounting for the use of resources, reporting, and auditing produces a secure network security system.

C. Available for Services

Attacks on IoT devices will avoid general denial of service attacks involving utilities. Different tactics have led to IoT's consumers, including sinkhole assaults, jamming rivals, or replay attacks use IoT components on various levels to deteriorate the level of service (QoS) [28, 29].

D. Trustworthy

To maintain the end-to-end integrity of data gathered and related communications, the IoT applications require trust mechanisms that cover these scales. In addition to the capacity to evaluate these processes and interactions, the transparency of data collection systems and relevant experiences are the key to satisfying these criteria [30]. Both the requirements of clarity and auditing drive Blockchain to create trust in IoT.

E. Energy Efficiency and Cost-Effective

IoT gadgets are generally restricted to resources and have a lower capacity to store data. The author in [31] attacks on IoT systems may result in improved electricity consumption by intravenous or false service inquiries and by exhausting IoT resources.

F. Single Points of Server Failure

A significant number of single points of vulnerability That may depreciate service provisioned by IoT may be exposed by the ongoing development of heterogeneous IoT connectivity networks [32]. It includes designing a strategic framework for a broad category of IoT gadgets and implementing new methods for utilizing a network of fault tolerance.

IV. Analysis and Discussion

Based on the literature analysis and survey, Blockchain technology may be seen as a new bearing in IoT access control. The incentive to use the Blockchain is to help its stable and secure distributed nature that solves many IoT access requirements. In this survey, the authors also defined two ways of access control for Blockchain in IoT perspectives.

The first one consists of the transaction system to request, receive, assign, and revoke connections. In essence, the transaction is used to make a connection between the asset owner and the subject. Connection decisions may be made directly by the owner of the asset. If this is not the case, the access request shall be transferred to the external entity responsible for assessing the appeal, making the decision, and returning it to the asset owner, as stated in [33, 34]. In this case, Blockchain's primary aim is to securely transfer the access token by defining individuals' access rights and guaranteeing to check and trace all access transactions. The power delegate is often an essential method in the collaboration framework, which can be delegated to the new topic from the current issue in a verifiable manner depending on the transaction. It implies the freedom of a subject to pass partly or entirely the right to access another individual. The delegated receiver is then allowed to carry out the delegating customer's activities. To restore the transaction-based access regulation, unified access token management can fix the dual cost issue and guarantee the trackability of all transactions. However, The recognition of an entry is rendered by a single person who may be the property owner or another agency identified by the Access Control Model application. The model can be called hybrid and not distributed.

The second approach evaluates a user control demand using a smart contract definition. It takes an access option depending upon the rules defined by the property owner and applied in the agreement. The contract is executed until the customer requirement is met with the access agreement, and the effect is a consumer consent authority token. Ultimately, the token is sent to the permission applicant utilizing a particular operation. The principal objective of this strategy is to return a single permission server with a distributed smart contract to construct a distributed permission network [20]. All-access control functions may be executed on the authenticated and recorded contract in the registry of Blockchain. Blockchain nodes can establish a mutual copy and carry out a contract without a mediator. Distributed smart contract ownership per the delivery and implementation by Blockchain will solve a single point of server failure in a centralized access control manner.

In comparison, the corresponding studies investigate the feasibility of producing dynamic access control evaluation by smart contracts that incorporate a machine-readable algorithm to find and detect behavioral subjects [22]. However, there is no approved smart contract access control paradigm validated and examined in specific application domains such as Intelligent Transport System or Smart Cities to prove its viability. Most of the proposed approaches show that they are applied using one of the Blockchain platforms, such as Bitcoin and Ethereumare, not evaluated in real environments.

For future access control, the Blockchain would be the essential engine. It has new dynamics and technologies that solve big systems problems. This is only the start, and approaches to measure their success should be tested. The goal is to build a transparent access control platform built on Blockchain, which will enable the future generation of the distributed network.

V. Future Research Directions and Open Challenges

This segment explains the proposed issues for the efficient implementation of IoT security.

A. Limitations of Resources

IoT's resource-restricted nature had been a significant obstacle to identifying a reliable security mechanism. Cryptographic algorithms can only operate under these powers, unlike normal ones. By [35] ensure efficient implementation of IoT security and communication protocols over the network, any communications or multicasts needed to transfer the key or certificate, storage and resources must be dealt with it. It means that these protocols are optimized to be lightweight and energy-efficient, given the need for sophisticated computation and advanced energy harvesting techniques.

B. Heterogeneous Devices

A multi-layer security structure must be discussed, as with heterogeneous sensors, exceptionally compact, high-end servers, and low-power sensor systems. The structure will first adjust to new resources and selections on the collection of IoT layer security mechanisms even before services are granted to end-users [36]. Such a flexible and compact structure requires information that is dependent on the uniformity of IoT architectural tools.

C. Single Points of Server Failure

For heterogeneous systems, structures, and protocols, the IoT standard is risky to single-point-of-server-failure than any other system. There needs to be more research work required to ensure appropriate IoT elements, especially in mission-critical applications. It would need devices and guidelines to perform continuity in mind the trade-off among values and the functionality of the entire infrastructure.

D. Interoperability of Security Protocols

Protocols intended at various layers require interoperation within the requirement of translation mechanisms to regulate the global security structure for IoT [37]. The active synthesis of safety measures on each layer can then be determined in the worldwide system framework, taking into account architectural limitations.

E. Trusted Updates and Management

Scalable and reliable software management and upgrades to millions of IoT gadgets lead to open issues for future research. Besides, problems associated with the safe and trusted IoT device supply chain, ownership, and data privacy are the main research concerns that need to be tackled by the researchers to raise significant and broad IoT acceptance [38]. These IoT security solutions are also available in Blockchain technology. However, blockchain technology itself claims to face problems in scalability, accuracy, arbitration/regulation, and essential collisions.

F. Hardware/Firmware Culnerabilities

The IoT structure becomes vulnerable to hardware flaws when the low-cost and low-performance system is traditional. It is not just a physical malfunction, but it must be verified before IoT deployment to implement security algorithms in hardware, routing, and packet processing operations [39]. Some Security flaws exposed since launch have displayed challenging to identify and mitigate. The regular confirmation protocol is, consequently, a requirement for the use of IoT security.

G. Blockchain Vulnerabilities

Despite affording robust solutions to IoT security, blockchain systems are also exposed [40]. The consensus mechanism based on the hacking capacity can be violated to enable the attacker to handle the private database keys with minimal randomness that may also be used for blockchain accounts negotiation [41, 42]. There is still a need to develop efficient mechanisms to protect transactions' privacy and prevent race attacks, resulting in duplication of transaction costs.

VI. Conclusion

In this survey, the authors first study the various security problems and challenges in IoT applications and access control for authorized and unauthorized users. Secondly, the authors have deep dive into previous research to figure out their solutions and existing problems. From the survey, it was found that some of the research has been already done in IoT access control by using Blockchain, and found that IoT systems are vulnerable and powerless to defend themselves. Due to insufficient resources in IoT gadgets, immature standards, and the lack of reliable software and hardware development, design, and deployment, as well as trusted updates and managements. The authors have acknowledged the restrictions of old access control to reply to IoT demands and investigated the ability to use the secure Blockchain system to manage access control. The authors demonstrate how the Blockchain can address and resolve some of the fundamental IoT security problems. The article also explains and recognizes future issues and challenges that the researchers need to provide reliable, effective, and scalable IoT security solutions.

Acknowledgment

This work was supported by The National University of Malaysia under the Research Excellence Consortium Fund (Grant number KKP/2020/UKM-UKM/4/3). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

References

[1] A Hassen, O., A Abdulhussein, A., M Darwish, S., Othman, Z. A., Tiun, S., & A Lotfy, Y. (2020). Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IoT Blockchain Network. Symmetry, 12(10), 1699.

[2] Alliance, O. M. (2017). Lightweight machine to machine technical specification. Approved Version, 1(1).

[3] Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., & Salah, K. (2018). A user authentication scheme of IoT devices using blockchain-

enabled fog nodes. Paper presented at the 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA).

[4] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., . . . Zanichelli, F. (2018). IoTChain: A blockchain security architecture for the Internet of Things. Paper presented at the 2018 IEEE wireless communications and networking conference (WCNC).

[5] Aman, A. H. M., Yadegaridehkordi, E., Attarbashi, Z. S., Hassan, R., & Park, Y.-J. (2020). A survey on trend and classification of Internet of things reviews. Ieee Access, 8, 111763-111782.

[6] Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. (2018). Blockchain with Internet of things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), 40-48.

[7] Ching, T. W., Aman, A. H. M., Azamuddin, W. M. H., Sallehuddin, H., & Attarbashi, Z. S. (2021). Performance Analysis of Internet of Things Routing Protocol for Low Power and Lossy Networks (RPL): Energy, Overhead and Packet Delivery. Paper presented at the 2021 3rd International Cyber Resilience Conference (CRC).

[8] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of things. Ieee Access, 4, 2292-2303.

[9] Cohn, J. M., Finn, P. G., Nair, S. P., Panikkar, S. B., & Pureswaran, V. S. (2019). Autonomous decentralized peer-to-peer telemetry. In: Google Patents.

[10] Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. Paper presented at the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA).

[11] Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094.

[12] Dedeoglu, V., Jurdak, R., Putra, G. D., Dorri, A., & Kanhere, S. S. (2019). A trust architecture for Blockchain in IoT. Paper presented at the Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services.

[13] Di Pietro, R., Salleras, X., Signorini, M., & Waisbard, E. (2018). A blockchain-based Trust System for the Internet of Things. Paper presented at the Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies.

[14] Din, Z., Jambari, D. I., Yusof, M. M., & Yahaya, J. (2019). Challenges in Managing Information Systems Security for Internet of Things-enabled Smart Cities. Paper presented at the 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS).

[15] Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016). World of empowered IoT users. Paper presented at the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI).

[16] Hernan, S., Lambert, S., Ostwald, T., & Shostack, A. Uncover security design flaws using the STRIDE approach (2006). URL http://msdn. microsoft. com/en-gb/magazine/cc163519. aspx, 15.

[17] Jafar, U., & Ab Aziz, M. J. (2020). A State of the Art Survey and Research Directions on Blockchain Based Electronic Voting System. Paper presented at the International Conference on Advances in Cyber Security.

[18] Jalal, I., Shukur, Z., & Bakar, K. A. A. (2020). A Study on Public Blockchain Consensus Algorithms: A Systematic Literature Review.

[19] Kamalinejad, P., Mahapatra, C., Sheng, Z., Mirabbasi, S., Leung, V. C., & Guan, Y. L. (2015). Wireless energy harvesting for the Internet of Things. IEEE Communications Magazine, 53(6), 102-108.

[20] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

[21] Lee, B., & Lee, J.-H. (2017). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. The Journal of Supercomputing, 73(3), 1152-1167.

[22] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853.

[23] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2017). Consortium blockchain for secure energy trading in industrial Internet of things. IEEE transactions on industrial informatics, 14(8), 3690-3700.

[24] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. Paper presented at the 2017 IEEE International Conference on Web Services (ICWS).

[25] Maesa, D. D. F., Mori, P., & Ricci, L. (2017). Blockchain based access control. Paper presented at the IFIP international conference on distributed applications and interoperable systems.

[26] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things, 1, 1-13.

[27] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 100227.

[28] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system," http://bitcoin. org/bitcoin. pdf.

[29] Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: a new Blockchain ‐ based access control framework for the Internet of Things. Security and Communication Networks, 9(18), 5943-5964.

[30] Ouaddah, A., Abou Elkalam, A., & Ouahman, A. A. (2017). 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 (pp. 523-533): Springer.

[31] Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. Computer networks, 112, 237-262.

[32] Ourad, A. Z., Belgacem, B., & Salah, K. (2018). Using Blockchain for IOT access control and authentication management. Paper presented at the International Conference on Internet of Things.

[33] Outchakoucht, A., Hamza, E., & Leroy, J. P. (2017). Dynamic access control policy based on Blockchain and machine learning for the Internet of things. Int. J. Adv. Comput. Sci. Appl, 8(7), 417-424.

[34] Putra, G. D., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2020). Trust management in decentralized iot access control system. Paper presented at the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).

[35] Sahraoui, S., & Bilami, A. (2014). Compressed and distributed host identity protocol for end-to-end security in the IoT. Paper presented at the 2014 International Conference on Next Generation Networks and Services (NGNS).

[36] Tseng, L., Wong, L., Otoum, S., Aloqaily, M., & Othman, J. B. (2020). Blockchain for managing heterogeneous Internet of things: A perspective architecture. IEEE Network, 34(1), 16-23.

[37] Van der Stok, P., & Greevenbosch, B. (2014). CoAP management interfaces (draft-vanderstok-core-comi-04). IETF, available at: https://datatracker. ietf. org/doc/draft-vanderstok-core-comi.

[38] Wilson, D., & Ateniese, G. (2015). From pretty good to great: Enhancing PGP using bitcoin and the Blockchain. Paper presented at the International conference on network and system security.

[39] Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. Computers, 7(3), 39.

[40] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the Internet of things. IEEE Internet of Things Journal, 6(2), 1594-1605.

[41] Zhang, Y., & Wu, X. (2016). Access control in Internet of things: A survey. arXiv preprint arXiv:1610.01065.

[42] Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using Blockchain to protect personal data. Paper presented at the 2015 IEEE Security and Privacy Workshops.