Access Control Mechanism in Internet of Things using Blockchain Technology: A Review

Conference Paper · December 2020

DOI: 10.1109/ICISS49785.2020.9316126

Avani Jayantilal Dadhania
LDRP Institute of Technology and Research

Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020]
IEEE Xplore Part Number: CFP20M19-ART; ISBN: 978-1-7281-7089-3

Access Control Mechanism in Internet of Things using Blockchain Technology: A Review

Avani J. Dadhania
Computer Engineering Department
LDRP Institute of Technology and Research
Gandhinagar, India
avani26.22@gmail.com

Hiren B. Patel
Computer Engineering Department
Vidush Somani Institute of Technology and Research
Kadi, India
hbpatel1976@gmail.com

2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) | 978-1-7281-7089-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICISS49785.2020.9316126

Abstract— **As the number and variety of connected objects continue to grow and the devices themselves become smarter, IoT has demonstrated to be the foremost rising innovation where millions of gadgets can interface to the web which makes the life attainable with no human intercession. However, the security and privacy of this IoT environment face some issues that must be overcome to meet the novel solution for IoT applications with no margin for error. Hence, secure architecture for centralized servers is necessitating maintaining the authenticity and protection of information. However, centralized architecture suffers from some challenges viz. reduction in performance, single point of failure and prone to attacks which could be addressed through decentralized or distributed architecture. Blockchain, being decentralized in nature, immutable in function, transparent in-process and reliable without a trusted third party, could be efficient attention for addressing IoT security challenges. In this research work the security concerns like access control mechanisms for IoT applications like smart city, smart healthcare system through Blockchain innovation is addressed. Blockchain being a distributed ledger provides an approach to securely store the data cryptographically. Specifically, proposed work intend to cover different access control methods for the protection of information and IoT security. This paper makes an exhaustive review of how decentralized architecture using Blockchain might potentially improve IoT access control.**

*Keywords— **IoT; Access Control; Security; Blockchain Technology***

I. INTRODUCTION

Internet of Things (IoT) is a growing technology that advanced world to our real-life activities through empowering an increasing range of objects (i.e. sensors, actuators, chips) that comprehend us, to be related to the web [1]. IoT is termed as billions of intelligent gadgets that are connected with the internet which may sense, collect, store and exchange information with IoT devices and platforms. Nowadays, the Internet of Things (IoT) plays an associate integral role in numerous domains of life which contains transportation, home automation, smart grid, industrial IoT, supply chain, energy sector, smart healthcare system among others [2].Gartner declared that 8.4 billion of connected objects were in use in 2017 (up 31% from 2016) and estimate 20.4 billion for 2020, therefore quite 240% of growth over successive 3 years, and therefore the study predicts that the IoT market can develop to over $3 trillion yearly by 2026[3]. Due to huge in number and wide these applications, numerous challenges are encompassing within the zone of protection of information and security in the real world. Without proper measures, the IoT design is often compromised by malicious users and information is often leaked. Hence, It is of utmost required to place an appropriate access control mechanism that defined what part of data should be made available among selected users. It is exigent to characterize and actualize compelling access management systems for addressing the security issues of IoT [1]. Thus, access management mechanism that intends to forestall defend against the illicit resource access from forbidden individuals has been considered as a progressively indispensable research issue in the IoT [4-6]. Undeniably, it is informative to attention that the smart devices are immense resources constrained regarding their computing capability, storage capacity and power for building the prevailing solutions for access control is impracticable [13] therefore researchers, industry, and government moves to handle these security questions like confidentiality, integrity, privacy, access management amidst alternative challenges have started.

An access control mechanism is techniques that outline some predefined rules and policy to check before granting access to any device or user [7]. The existing access control mechanisms(ACM) like discretionary access control[8], mandatory access control [18], Identity-based access control [9], attribute-based access control [10], role-based access control [11], capability-based access control(CAPBC) have their own benefits and challenges, resulting in the lack of a solution for securing IoT devices and protecting user's information against threats and attacks. Additionally, majority of security solutions depend on a centralized architecture that makes IoT applications are considerably more convoluted for a huge number of resources [13]. Along these lines, a distributed or decentralized architecture is needed to handle security questions for IoT infrastructure [13]. Therefore, through this research, an extensive literature survey that incorporates a detailed study of existing access control mechanisms and different solutions according to a distributed or decentralized approach is presented.

The remainder of this paper is structured as follows. Section II depicts challenges in access control for the IoT domain. Sections III shows various existing access control methods and details about the same have been discussed. Section IV. Discuss Blockchain technology. In section V the solutions for access control in the IoT environment with decentralized architecture using Blockchain technology is discussed. In section VI some research directions in this area are identified and concluded the research work in section VII. Followed by a list of references used in the paper.

II. ACCESS CONTROL CHALLENGES IN TOT

Although extensive actions were given in the IoT security area, discussion presents the highlights of numerous issues to be tended to. Fig.1. shows the different access control challenges in IoT.

A. Scalability

Scalability refers to the potential of a device to handle a growing quantity of work. With the rapid growth of IoT where an increasingly large amount of smart gadgets interact with the internet needed scalability as a significant concern. For the resource-constrained devices access control on massive scale results in performance overhead. Hence access control mechanisms ought to be heightened in size, expands the structure, and enlarges the number of users and resources without contrarily influencing the quality of services given by IoT framework [14].

B. Lightweight

Because of restricted storage, processing power and computing capabilities of IoT devices leads to the destruction of the performance of access control services. In consequence, delivering a competent access control model for the IoT environment is an integral however exacting topic. To avoid that, an access control system designed for IoT needs to reduce the overhead because of the device to device interaction and processing power [15].

C. Centralized Architecture

IoT system with a large range of objects and subjects, under the authority of centralized servers which permits the authorization decision between the user and IoT device becomes a single purpose of failure [6] and compromises the privacy of users [16].The centralized architecture is sometimes appropriate for a fixed-sized network that is well forced in size and shape that doesn't seem to be amended or reconstructed**.**

D. Heterogeneity

IoT System alliance with heterogeneous computing nodes or combine different technologies and devices where each domain or platform has its specific demand for authorization policy is a fundamental challenge in IoT [17].Contributing to the traditional access control model in access rights delegation and transitivity are vital for effectual and structured intradomain authorization and access control. It is interesting to comprehend establishment confinements in this area.

E. Mobility

Internet of Things is a rising technology wherein the organize topology and network will continuously alter. For example, intelligent nodes will leave the network and new intelligent nodes can connect to the system. IoT frameworks have to be compelled to be ready to accommodate the dynamic nature of nodes [15].

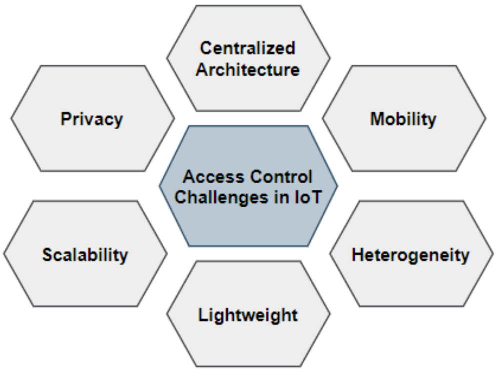

Fig.1. Acccess Control Challenges In IoT

F. Privacy

To prevent the user's data from unauthorized user is the biggest challenge. User's personal information should be accessed with the consent of the data owner for providing privacy preservation of use's information [35].

III. ACCESS CONTROL METHODS FOR IOT

Several access control methods contributed to the literature for addressing IoT security issues with distinct aims. These methods with different features can impact the suitability of access control mechanism for IoT.

In the conventional access control matrix, that characterizes each right of subjects who want to access resources for objects to be accessed. In traditional access control methods like discretionary access control (DAC), the resource owner can permit access their resources directly by making access control list (ACL) for every resource [19]. DAC provides flexibility and easy to implement but does not run well on extensive due to access control list explosion. Uniquely in contrast to DAC, the central authority of the system grants authorization for the entities that access resources to objects in the mandatory access control (MAC) [20] that gives limited user functionality. However, the research community believes to enhance the improved access control methods for growing IoT enterprise depend on user roles for accessing authorized data. In the role-based access control (RBAC) schemes, access control is assigned to subjects (i.e. entities that access resources) based on the user roles using privileges [21] which required less administration. Imposing access management by roles provides transparency but permissions cannot be assigned to objects and operations rather than subject roles. RBAC has the possibility of a role explosion where role defines for users in a static way do not provide role delegation. However, RBAC is unsuitable in a lightweight mechanism for constrained devices [10]. Therefore extension of role-based access control (RBAC) [30] model called context-based access control that introduces context constraints in access policies have been developed. Attribute-based access control is an alternative to overcome the limitations of RBAC. In the attribute-based access control (ABAC) scheme, based on the policy which combines various types of attributes, such assubject attributes, object (i.e., the entity that holds resources) attributes and environment attributes, etc., to define a set of rules expressing under what conditions access rights can be granted to subjects [22]. However, ABAC is a better alternative to address the limitations of RBAC which provides a dynamic, flexible, fine-grained and scalable solutions for access control system. Nevertheless, both RBAC and ABAC are inflexible on large scale networks. Therefrom access control lists and capability-based access control methods exist. In the access control list, service providers are required to check that a subject can grant permission for accessing the object. Furthermore, ACL as being centralized in nature and burdensome to remove all the rights to users on all the files. Whereas a capability may be a contagious and tamper-proof token generated from the authority that refers to a worth that references an object alongside an associated set of access rights [23] that supports fine-granularity and scalability for access management which does not require handling complex issues.

IV. BACKGROUD:BLOCKCHAIN TECHNOLOGY

The coming of crypto-currencies like Bitcoin [31] Blockchain technology is transformed into the most promising innovation that changes the traditional centralized client-server architecture into a decentralized architecture, which can improve trust in record keeping and financial transactions [32]. Blockchain is an arrangement of recording data such that makes it troublesome or unachievable to tamper the data in the framework [33]. Blockchain is basically a digital ledger of transactions that is copied and distributed over the whole Blockchain network. Blockchain consists of a number of blocks, each block in the chain contains a hash of the previous block, and every time a new transaction occurs on the Blockchain, a record of that transaction is added to every participant's ledger [34] as shown in Fig.2. All the transactions are noticeable which are mined into the block called pool miners [14]. The decentralized database that is being managed by multiple participants is known as Distributed Ledger Technology (DLT)[34]. When a node executes a transaction it signs and broadcast to its one-hop peers while peers of node validate the signed transaction before retransmitting [34].

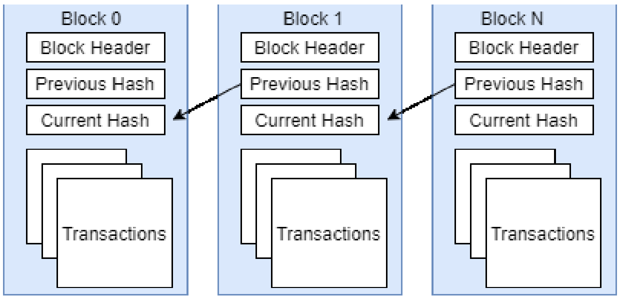

Fig.2. Blockchain Structure

V. RELATED WORKS: ACCESS CONTROL FOR IOT USING BLOCKCHAIN

Recently, various proposals related to access control in IoT with different objectives aiming to address the aforementioned problems regarding emerging IoT scenarios are mentioned. Therefore a survey on Smart contract-based access control and Transaction based access control model in the Blockchain is analyzed in the literature review as shown in Table 1.

A. Smart Contract-Based Access Control

1) Ronghua Xu et al. [24] identify access authorization as one of the prime key challenges with respect to privacy and IoT security for the wide adoption of IoT. The authors express the concerns regarding the usage of a centralized authentication server because of its performance bottleneck and single point of failure. Authors further propose a prototype for the capability-based decentralized mechanism (BlendCAC) using Blockchain technology which makes use of token management for various permissions/revocations on access authorization. However, authors have implemented the mechanism on a local private Blockchain with devices such as Raspberry PI and desktops/laptops. Authors claim scalable and computationally lighter access control mechanisms.. Every domain requires a domain owner (which in turn is a centralized entity that may cause issues such as bottleneck, performance degradation, single point of failure, etc). Further, the domain owner has been assigned the duties of defining the authorization policies and making decisions based on the authentication process. The usage of public key infrastructure needs to address issues such as key generation, sharing, and storing the public/private keys. Every domain owner maintains a local chain which needs to be synchronized with the global Blockchain, periodically. A token is stored on the Blockchain which is visible for everyone will raise the privacy issues. Researchers may work on the said proposal to address the issues mentioned.

2) Oscar Novo [25] proposed architecture by considering mobility, lightweight, concurrency, resilient, accessibility principles. The entire procedure in the Blockchain network aside from the IoT gadgets, which can minimize overhead due to IoT device interaction with Blockchain network and provide better adaptability in lightweight IoT Scenario. In this architecture, IoT nodes are not characterized as Blockchain networks yet management hub which will communicate with Blockchain for access requests of IoT devices. Whereas,the agent node is responsible for deploying a smart contract in the Blockchain architecture. The manager is trustworthy for dealing with access authorization for IoT devices. IoT devices communicate among them in the WSNs using COAP and recognized using public keys in the Blockchain network. Devices are executed utilizing the LibCoAP library7. The management Hubs are situated at the edge of the WSNs. The management Hub is a JavaScript interface that interprets the data encoded in CoAP messages, by the IoT gadgets, into RPC messages. The RPC messages are reasonable by the Blockchain hubs. The Management Hub is associated legitimately to a Blockchain hub. The interface utilizes the web3 JavaScript API to speak with Ethereum hubs through RPC calls and a CoAP JavaScript library9 to interface with the IoT gadgets. However, we believe to think after viewpoints in the said research. It does not provide fine-grained access control. Miners can store a local copy of the Blockchain that would violate the primitive principle of distributed storage, immutability, and transparency.

Table 1. Comparison on Blockchain-based access Control models with existing work

Authors	**Year**	**Blockchain based access control model**	**Objective**	**Merits**	**Demerits**
Ronghua Xu[24]	2018	Smart contract based	Access control authorization using capability token	Provide capability revocation and delegation	Performance Overhead
Oscar Novo[25]	2018	Smart contract based	A Decentralized Access control Architecture for Scalable access Management	Provide scalable access management	Does not provide fine granularity
Yuanyu Zhang[26]	2019	Smart contract based	A smart contract based access architecture	Provide Static right validation, dynamic right validation	Does not provide scalability
Shuang Sun[27]	2019	Smart contract based	Multiple smart contract are developed for access right establishment and storing the database	Provide Scalability and access management for different types of IoT device	Transaction validation and verification is time consuming
Nabil Rifi[28]	2018	Smart contract based	Access Control mechanism for smart building	Publisher-subscriber mechanisms for the privacy of information	Performance overhead due to scalability
A.Ouaddah [1]	2016	Transaction based	A Blockchain based framework protocol has been	Transaction based access authorization management	Does not Support token revocation and delegation
G. Zyskind [29]	2015	Transaction based	Decentralized mechanism to protect personal data	Support Privacy	Storage is limited

3) The authors propose in [26] a smart contract-based access control in which multiple access control in which multiple access control contracts(ACCs), One judge contract(JC), and One register contract(RC) are developed using Ethereum smart contract platform for registration, access control rights, and misbehavior judging methods to accomplish authorization. In architecture, every ACC gives one access control strategy for a subject-resource pair, which actualizes both static access right approval dependent on pre-established policy and dynamic access right approval by examining the behavior of the subject. To encourage the dynamic approval of the ACCs, the JC gives a misbehavior judging technique, which gets misbehavior reports about the subject from ACCs decides return the relating punishments.

4) Shuang Sun et al. [27] proposed an access control mechanism that focusing IoT security and pivacy for data and devices which provides scalability and fine granularity. As described in this paper author had implemented multiple contracts for secure insertion of IoT device, access right establishment and storing hash value by the device on the Blockchain. The users and resources are considered as subject-object pair based on the roles assigned to a particular user with read, write, and execute privilege. All the users can access user information and device resource information which are stored in heterogeneous tables. Users can access contracts by implementing encapsulation of device identification, resource access information and different operations.

5) Authors in [28] illustrate the Blockchain-based design and a protocol for information access in IoT devices using smart contract and publisher-subscriber mechanisms for the privacy of information. IoT devices and information access mechanisms to communicate with the Blockchain needed high computational power. Having a centralized system to access a large quantity of information might tamper the data due to hack the server by attackers. Therefore the author presented an access control mechanism for smart buildings where the gateway can play a role for the publisher to attach to the Blockchain when sensors are unable for direct connection with Blockchain. When a huge number of smart gadgets generate the information can decrease the performance in terms of dealings time.

B. Transaction Based Access Control

1) Aafaf Ouaddah et al. [1] proposed a framework titled fair-access as privacy-preserving authorization management for access management. In this paper, the authors presented a framework within objectives, models, design, and mechanism specification in IoT that introduces dealing for grant the permission, delegation and revocation of access rights using Blockchain transaction. The paper focuses on, a framework that was developed supported the subsequent principles like User-Driven and Transparency , Fairness and Fine Granularity. It additionally illustrates on centralized and decentralized approach that is being employed to manage access management policies for IoT devices. Whereas a decentralized approach used for peer to peer communication for every organization and due to resource-constrained IoT devices. Whereas all the resource constraint devices don't seem to be able to do the authorization operate by themselves in order that authors used a centralized entity referred to as authorization management that manages and approves authentication and authorization of resources. The aforesaid paper illustrates the use of a bitcoin-like address to identify all interacting entities and access management policies keep within the sort of transactions within a Blockchain. Smart contracts used to define the access policy and authorization token as digital signature defined by the creator which represents access rights for the users who are going to access specific resources identified by its address Further authors had implemented the framework with the use of Raspberry Pi connected to a WLAN (for remote access) with the use of the dedicated camera, SD card, and local Blockchain. However, limitation of FairAccess is that, it neither supports the updation nor revocation of an access token.

2) In [29] the author proposed an architecture to protect user's personal data in a decentralized way. In this paper, two types of transactions are used to store and share the data, access control management to grant permission for services. The authors express some privacy concerns like data ownership, data transparency and auditability by applying Blockchain and off-Blockchain storage for managing personal information of users. Authors have mentioned some future directions regarding the storage of data, trust and decision making using Blockchain technology.

VI. RESEARCH DIRECTIONS

The usage of IoT applications and its importance in our routine life increases on large extent needed secure access rights from the resource owner to the users in the IoT network. In this section the major challenges and for access control in different domain and future directions in which Blockchain can be integrate with IoT domain are addressed. Health care sector require the major concern about the privacy of patient's personal information, interoperability and centralized storage of patient's data. So more research attempt should also made to guarantee the security and privacy for accessing user's information in the Internet of Things environment.

VII. CONCLUSION

The expansion of the internet in the direction of the Internet of Things is being conveyed in a growing cyber-physical system for example access control solutions. In this survey, the main challenges of IoT is identified. The limitations of traditional access control methods for IoT architecture is also discussed. Traditional IoT infrastructure is depended on centralized architecture. A decentralized Blockchain network reduce this possibility with millions of individual nodes that transfer data on a peer-to-peer basis to keep the rest of the IoT network running smoothly. Blockchain technology is investigated as a promising innovation that may offer a high level of security of IoT transactions. Many researchers considered that Blockchain could be an encouraging paradigm for IoT security and services. Consensus protocol will play a key function in the consideration of IoT device to mine the new block in the Blockchain. At present, this innovation is still just in its beginning phase, and thusly a lot of research must be led to provide efficient security solutions for IoT world. Then different access control methods are discussed and evaluated related literature work for access control mechanisms from IoT perspective dealing with scalability, heterogeneity, privacy using decentralized architecture. Finally, apart the lightweight node and scalability which influence the Blockchain and IoT both, researchers should work on the security and privacy of the IoT infrastructure. In future, scalability issue for IoT environment can be focused and future work consists of implementing a scalable access control framework for IoT using decentralized architecture.

REFERENCES

[1] A. Ouaddah, A. Kalam, and A. Ouahman, "FairAccess: a new Blockchain- based access control framework for the Internet of Things," Security and Communication Networks, vol. 9, pp. 5943–5964, 2016.

[2] M. Hassan, M. Rehmani, and J. Chen "Privacy preservation in Blockchain-based IoT systems: Integration issues, prospects, challenges and future research directions," In Future Generation Computer Systems, 97, 512–529, 2019.

[3] https://www.iotforall.com/what-is-iot-simple-explanation.

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp.146–164, 2015.

[5] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "security considerations for cloud-supported internet of things ", IEEE Internet Things J., vol. 3, pp. 269–284, 2016.

[6] A. Ouaddah, H. Mousannif, A. Elkalam, and A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," Computer Networks, vol. 112, Elsevier, 237-262, 2017.

[7] P. Samarati, and D. Vimercati, "Access control: policies, models, and mechanisms," In: International school on foundations of security analysis and design, Springer, pp. 137–196, 2000.

[8] YA. Younis, K. Kifayat, M. Merabti, " An access control model for cloud computing," J Inf Secur Appl pp. 45–60, 2014.

[9] A. Singh, and K. Chatterjee,"Trust: identity and trust based access control model for healthcare system security", Multimedia Tools and Applications, 78(19), 28309–28330,2019.

[10] Y. Zhang, D. Zheng and R. Deng, " Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control " Internet of Things Journal, IEEE 5(3), 2130–2145, 2018.

[11] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role based access control models," Computer, vol. 29, no. 2, pp. 38–47, 1996.

[12] S. Gusmeroli, S. Piccione, D. Rotondi, S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things", Mathematical and Computer Modelling, vol.58, Issues 5–6, Elsevier, pp. 1189-1205, 2013.

[13] D. Eddine, A. Bouabdallaha, and H. Lakhlef, " Internet of things security: A top-down survey ", Computer network journal,vol.141,199-221, Elsevier, 2018.

[14] O, Novo, "scalable access management in iot using blockchain: a performance evaluation" IEEE journal of internet of things class files, vol. 14, no. 8, november 2018.

[15] S. Ravidas, A. Lekidis, F. Paci, and N. Zannonea, "Access control in IoT: A survey," journal of network and computer application,2019.

[16] J. Hernandez-Ramos, A. Jara, L. Marin, and A. Skarmeta," Distributed Capability-based Access Control for the Internet of Things," Journal of Internet Services and Information Security (JISIS), vol.3, pp. 1-16, 2013.

[17] R. Lunardi, R. Michelin, C. Neu, and A. Zorzo, "Distributed Access Controlon IoT Ledger-based Architecture," Conference on IEEE/IFIP Network Operations and Management Symposium, 2018.

[18] H. Atlam , M. Alassafi , A. Alenezi , R. Walters, and G. Wills ," XACML for Building Access Control Policies in Internet of Things", 3rd International Conference on Internet of Things, Big Data and Security, Science and Technology, Scitepress, 2018.

[19] D. Sheng, C. jin, L. Chen, F. Kai. and L. Hui, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT," Special section on security and privacy for cloud and IoT, IEEE Access, vol.7, pp.38431 – 38441, 2019.

[20] S. Osborn, R. Sandhu, and Q.Munawear, "Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies," ACM Transactions on Information and System Security, vo.3, No-2, 2000.

[21] J. Cruz, Y. Kazi, and N. Yanai, "RBAC-SC: Role-based Access Control using Smart Contract," IEEE Access, vol.4, 2016.

[22] I. Ray, B. Alangot, S. Nair, and K. Achuthan, "Using Attribute-Based Access Control for Remote Healthcare Monitoring," 4th International Conference on Software Defined Systems, SDS 2017, IEEE , Valencia, Spain, 137–142, 2017.

[23] Y. Chen , R. Xu, E. Blasch, and G. Chen, "A federated capability-based access control mechanism for Internet of Things (IoTs)," SPIE Defense & Commercial Sensing 2018 (DCS), At: Orlando, FL, USA, 2018.

[24] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A Blockchain-ENabled Decentralized Capability-based Access Control for IoTs," IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)," 2018.

[25] O.Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, 1184–1195, 2018.

[26] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," IEEE Internet of Things Journal ,vol.6, Issue: 2, 2019.

[27] S. Sun, S. Chen, R. Du, W.Li, and D. Qi, "Blockchain based Fine-grained and Scalable Access Control for IoT Security and Privacy," Fourth International Conference on Data Science in Cyberspace (DSC), IEEE, 2019.

[28] N. Rifi, E. Rachkidi, N. Agoulmine and N.Taher, "Towards using Blockchain technology for IoT data access protection," IEEE 17th International Conference on Ubiquitous Wireless Broadband, 1–5. 2018.

[29] G.Zyskind, O. Nathan, and A. Sandy Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Security and Privacy Workshops , 2015.

[30] G. Zhang, J. Tian, "An extended role based access control model for the Internet of Things," International Conference on Information Networking and Automation (ICINA), pp. vol-319-323, IEEE, 2010.

[31] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008.

[32] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation," A systematic review, solutions, and challenges, Mechanical Systems and Signal Processing, vol.135, Elsevier 2020.

[33] https://www.euromoney.com/learning/Blockchain-explained/what-is-Blockchain.

[34] T. Fernadez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol.6, 2018.

[35] I. Makhdoom, Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A Blockchain-based framework for privacy-preserving and secure data sharing in smart cities," Computers and Security, 88, 2020.