https://doi.org/10.46335/IJIES.2022.7.8.20 **e-ISSN: 2456-3463**
Vol. 7, No. 8, 2022, PP. 110-116
International Journal of Innovations in Engineering and Science, www.ijies.net

An Analytical Review on Challenges and Solutions for Secure Data Access through Blockchain-Based IoT

Manisha Gokuldas Gedam[1], Swapnili Karmore[2], Waibhav Khemraj Deogade [3]

[1]*Faculty of Science & Technology: G. H. Raisoni University, Saikheda*
[2]*Associate Professor, Department of Data Science: GHRIET, Nagpur*
[3]*Lead Engineer II: Lululemon, Banglore*

manishagedam2007@gmail.com

***Received on**: 11 June ,2022* ***Revised on**: 31 July ,2022,* ***Published on**: 03 August,2022*

Abstract-*A number of security and privacy concerns are raised by the decentralized nature of IOT technology and its rapid growth on a wide scale. At the moment, access control is one of the most difficult problems to solve, and most of the time, this is done through centralised systems that are bound by accessibility and sustainability, which might results in a productivity constraint. Despite the fact that blockchain provides numerous benefits such as peer-to-peer technologies, confidentiality, improved efficiency, and additional security, the immutable structure of the blockchain is the primary reason it is the first choice. As a result of its distributed nature, blockchain can be employed as a vital technology in interconnected networks to eliminate the need for a trustworthy third party. In this article, we have explored the integration of Internet of Things (IoT) and blockchain technology, as well as offered an in-depth analysis of the blockchain-enabled Internet of Things systems. Currently available research is divided into three categories: data management and control strategies, large-scale data and cloud computing techniques, and industrial sectors. The comprehensive study of blockchain use cases will operate as a state-of-the-art for the researchers, allowing them to conduct cutting-edge research in the pursuit of block chain technology across a wide range of fields based on the findings .*

Keywords—*Internet of Things, Blockchain, Data Security, Access Control, Consortium Blockchain*

I -INTRODUCTION

In this century, the Internet of Things (IoT) has the potential to be one of the more impactful technological innovations the world has ever seen. A natural progression from the World wide web (of computers) to integrated and cyber physical systems, which are "things" that, while still not clearly computer systems themselves, have computers within them. With a network of inexpensive sensors and interconnected items, it is possible to collect information about our world and environment at a far finer level of granularity than previously possible. Indeed, thorough information will increase efficiencies and enable the delivery of professional technologies in a variety of application domains, particularly ubiquitous healthcare as well as smart city services, amongst other things.

For example, a smart home system based on the Internet of Things can utilise sensors to recognise when household devices need to be switched on (or off) and turn them on (or off) automatically, therefore reducing energy and making people's lives more convenient. Smart consumer gadgets such as smart televisions and wearable electronics are among the many types of IoT devices, which also include animals and humans implants (such as implantable devices or identification tags) and monitoring chips for animals. The Internet of Things has a very broad spectrum of applications, ranging from household consumer products to health, agribusiness, energy, and transportation, as well as any other industry that can profit from incorporating IoT technology into its operations. The number of Internet of Things devices is growing at an exponential rate, yet there are numerous issues associated with them. IoT devices, by their very nature, have restricted computational resources and are therefore vulnerable to security threats. As a result, while

https://doi.org/10.46335/IJIES.2022.7.8.22 **e-ISSN: 2456-3463**
Vol. 7, No. 8, 2022, PP. 1-6
International Journal of Innovations in Engineering and Science, www.ijies.net

eveloping an Internet of Things-based system, security is a critical consideration.

Because of its qualities like as immutability and irreversibility, blockchain is the most efficient of all the technologies now accessible for data protection and privacy applications. Blockchain is essentially computer technique used to produce ledger records that are extremely difficult to tamper with. It enables the preservation of all interactions into irreversible records, with each record being dispersed among a large number of participant nodes. Because of the use of substantial government cryptography, a powerful cryptographic hash, and total decentralisation, the security is ensured. The blockchain is impervious to data tampering and manipulation. When a modification is made to the ledger through the use of transactions, the changes are sent to all of the nodes, which then check and update their respective transcripts of the ledger. Once a transaction has been verified by all of the nodes within the network, this is not feasible to make changes to the transaction without affecting the blocks that came before and after it. As a result, blockchain transactions are irreversible, and the data associated with them is constantly updated. Each node is connected to the next by a link, which is indeed known as a link chain. The hashes of the preceding block is included in the subsequent block, which allows the chain to be visited in reverse chronological order.

A great deal of personally identifiable information is saved by the gadgets obtained from multiple IoT devices, and this information must be kept private and accessible only by the device's owner and other permitted and validated stakeholders. In addition, the blockchain is one of the most likely options that can ensure the confidentiality and reliability of data, and it can be used in conjunction with smart contracts to allow the owner to govern the sharing of the data on his terms. The decentralization, immutability, and nonrepudiation of recorded information are some of the most significant benefits of blockchain technology in the Internet of Things. Figure 1 depicts the general operating process of blockchain networks in conjunction with the Internet of Things-based system. The data produced by that of the IoT devices is processed by the smart contract, which then records the results on the blockchain.

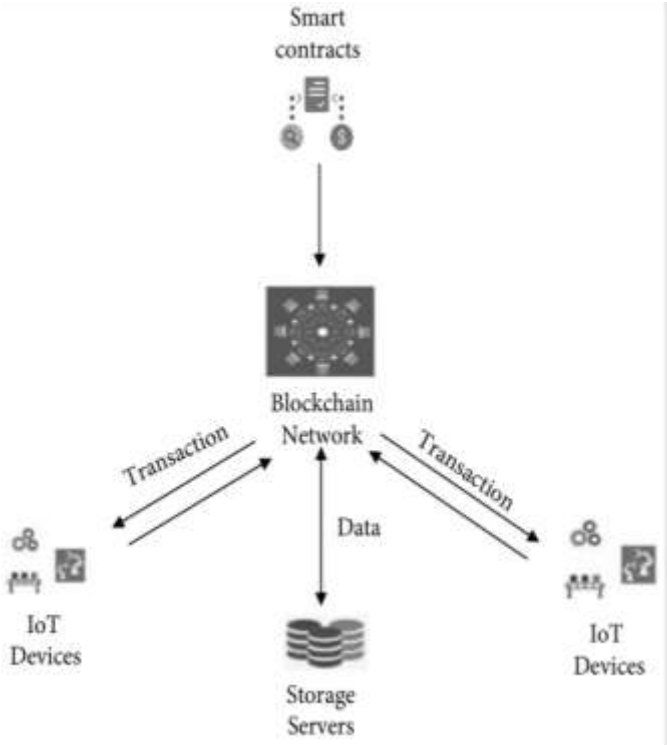

Fig 1- Integration of IoT Based system to smart contracts via Blockchain Network

As the Internet of Things (IoT) has begun to penetrate the mainstream sector, the key issues associated with the technology are quickly becoming apparent. The security of IoT deployments is one of the most important considerations. The following are the most significant security problems for Internet of Things infrastructure and services:

- In an environment where there is a high probability of device proliferation, it presents a significant difficulty to identify, verify, and protect the devices that exist.
- Scaling, maintaining, and managing a centralised security architecture will be extremely complex and expensive, as will managing and maintaining it.
- A centrally controlled security system would serve as a single point of failure, making it a great target for widespread denial of service attacks, which are becoming increasingly common.
- The implementation of centralised infrastructure in an industrial setting in which the edge nodes are widely dispersed geographically will be problematic.

Because of the numerous advantages outlined above, blockchain technology appears to be a feasible solution.

https://doi.org/10.46335/IJIES.2022.7.8.22 e-ISSN: 2456-3463
Vol. 7, No. 8, 2022, PP. 1-6
International Journal of Innovations in Engineering and Science, www.ijies.net

I. REVIEW OF LITERATURE

Several industries are deploying Internet of Things systems because of the numerous benefits they bring, such as the capacity to record data and connect with its neighboring equipment without the need for human or machine involvement. During these encounters, there seems to be a high likelihood of data leakage from the system. To solve this, a variety of solutions are used to handle this particular area of security concern.

Traditionally, before the Internet of Things (IoT) came into being, all of the data created was stored in a single location, making it subject to security breaches. Various research make use of the Internet of Things in order to avoid a performance degradation, and they make use of blockchain technology in order to provide security. There are a variety of benefits to using blockchain in the Internet of Things. Some of them are as follows: services in the Internet of Things system are unstable as a result of malicious attacks and are susceptible to a system failure.

Blockchain networks are decentralised designs in which a group of nodes that are not mutually trusted can come to an agreement on a commonly held view of an irreversible, tamper-proof, appendonly ledger by exchanging information. In its most basic form, a ledger is a list of transactions that have taken place between users. In the blockchain network, users can submit new transactions that are checked for validity by a selected at random specialised node known as the miner. If the transactions are found to be valid, they are attached to the ledger and the blockchain is updated. Smart contracts, which are computer programmes that run on ledgers, may also be included in more advanced versions of ledgers. In addition to the "state" that is maintained in the ledger, smart contracts are also associated with some "data." Customers can communicate with a smart contract through the use of transactions, and they have the ability to modify the contract's current state.

It is a difficult undertaking to apply an appropriate authentication protocol to billions of Internet of Things devices. This is because, regardless of the fact that identity and access management issues have been extensively investigated in the literature, these concerns are still in their infancy in the context of Internet of Things. In information technology infrastructure, the access control list (ACL) and role-based access control (RBAC) are three and among the most widely used access control mechanisms. But they are ill-suited for offering comprehensive, economical, and conveniently controllable application functionality in an IoT environment[1].

When using ACL, access control mechanisms are applied in the cloud, allowing for easier management and monitoring of actions, but they are hampered by the need for centralised management. As the quantity of Internet of Things devices grows, the difficulty of access control lists grows as well, resulting in a jumbled state of duty difficulties. The ACL lacks precision and scalability, as well as being very susceptible to a central destination of failure as a result of its centralised architecture [2].

Ethereum [3] is a blockchain architecture that is popular for its support of smart contracts. Considering Ethereum smart contracts from a high-level perspective, they can always be considered as coding classes, and subscribers can interact with the public features of all those classes through the use of transaction, which are a subset of transaction. Smart contracts are recorded in the blockchain and are distinguished from one another by an unique identification number, referred to as an address. Furthermore, once they have been deployed, it is impossible to change their code.

Unlike traditional contracts, which are written in high-level Turing-complete languages, Ethereum contracts are performed on a "virtual machine," referred to as the Ethereum Protocol, which runs in the background of the Ethereum blockchain. The Ethereum blockchain is the only source of information for smart contracts, which means they can only receive input from the ledger, other smart contracts, and the user who triggered them. As a result, smart contracts have no access to any information or assistance which were not encapsulated within in the Ethereum blockchain. Event classifications can be applied to smart contract state changes, and end-user programmers and frameworks that monitor the Ethereum blockchain may "raise alarms" whenever a specified sort of incident happens.

In an early effort to combine the technology Internet of Things with Blockchain, the number of novel blockchain systems were suggested. For example, the creators of [4] developed a smart home management system based on the blockchain. In their proposal, they envisioned a proprietary blockchain protocol in which the home gateways would act as miners. Such solutions are difficult to implement because they necessitate a "critical mass" of participants. Our technique is based on existing technologies and may be utilised with libraries and wallets that are already available on the market.

The author of this paper [5] solves the challenges of security and accurately measure efficiency in a multi-user MECCO networking using blockchain at the same time. In order to increase offloading security, they created a

dependable access control solution based on blockchain technology. This solution can protect cloud resources from unauthorised unloading. They then created a computation offloading issue to deal with both the computational management of authorised MDs, which they jointly improved by optimising autonomous judgments, the allocation of computational power and radio bandwidth, and the usage of smart contracts. The aim of this optimization challenge is to decrease long-term system expenditures like as latency, energy usage, and cryptographic protocol fees across all MDs. To tackle the stated offloading problem, they develop an enhanced deep reinforcement learning method that employs a double-dueling Q-network.

It is proposed in this paper [6] that a blockchain-based transaction provides a pathway be used in a secure distributed Internet of Things network. Additionally, it contains a decentralised transaction (TX) validation technique that is context-aware. A transaction is validated by a miner in line with the priority of a service in this approach. The author has built Software - defined networking Infrastructure (SDN)-enabled ports as an intermediary between both the IoT technology and the Ethereum blockchain, for which the programs have focused including network monitoring are assured on a large scale using SDN technology. Evaluation and comparison of the proposed network model with the Core network have taken place. According to the findings, the supplied prioritization in TX validation is significantly more delayed insensitive than the current approach for delivering networking quality of the service, which is much more sensitive than the current technique.

This research [7] examines a variety of blockchain-based trust techniques and describes their advantages and disadvantages when applied to decentralised IoT communities, as well as their limitations. Then, a trust model with such a multi-layer adaptive and trust-based weighting mechanism is developed, which incorporates the best of both worlds. In addition, many trust metric parameters, as well as the mathematical models that can be used to evaluate trust, are discussed in detail. Furthermore, this study introduces a novel approach for incentivizing processes in the Internet of Things marketplace that makes use of controller parameters and smart contracts, among other things. As a result, individuals are encouraged to make constant improvements in their behaviour. Finally, it is demonstrated that the suggested trust model is trustworthy. The experimental findings obtained from a variety of scenarios demonstrate that the proposed approach is more resilient to diverse attacks than existing approaches.

An article by a researcher in [8] described a unified solution for moving disparate traditional electronic health records to an unified blockchain-based ecosystem. [8] Furthermore, they explore the challenges associated with the differences in data architectures between ordinary relational database systems and blockchain storage databases in more detail. The solution outlines the conversion process as well as the synchronization of data in a centralized database for humongous e-health data storage and transmission. The deployment and analysis have revealed that significant gains in data storage, access control, and seamless transfer may be realized through the use of this technology.

According to [9], the distributed structure of the "ledger," along with Ethereum's capabilities of parallel execution of replicated "smart contracts," give the automation, generality, flexibility, and high availability that have been sought after in a blockchain-based system. A realistic blockchain-based Internet of Things architecture was built, utilising existing technologies while taking into account the characteristics and limits of IoT systems and platforms. Furthermore, they take advantage of the immutability of the blockchain as well as Ethereum's support for custom tokens in order to develop an optimized and accurate token-based access control system. As a consequence of the research's evaluation results, we have determined that our approach is practical and provides considerable security and usage advantages.

The homomorphic hash technique, which is employed to protect data, is the foundation of this study [10]. Furthermore, this enables dynamic operations and block-level customization. When dealing with a large number dynamics, the Merkle Hash Tree is used to help identify the exact location of each dynamic action. The overhead of communication and computation is reduced. The deduplication analysis determines if a file that a user intends to upload in online storage currently exists on the cloud server or if it should be produced. This design is reliable and effective against a hostile server's replace attack, but it has been demonstrated to work.

A novel safe mutual authentication method was developed in this study [11], and according to the authors, it has the potential to be implemented in home automation as well as other applications. The suggested solution, in particular, combines blockchain technology with group signatures and asymmetric cryptography in order to provide accurate investigations of users' access histories, anonymous group member authentication, and efficient verification of the home gateway, among many other things. The authors also demonstrate that the proposed system satisfies the privacy

requirements such as traceability, anonymity, confidentiality and security. For this, they conduct an implementation and evaluation to establish that the system is feasible.

The author of this work [12] focuses on such an access control issue related to the Internet of Things (IoT). In general, we propose a decentralized Internet of Things system based on the blockchain as a starting point. In order to protect users, devices, and data, they develop safe fine-grained access control mechanisms, which they then put into action using smart contracts. We create a number of different transactions in order to trigger the smart contract. Finally, the establishment of access rights is accomplished through the use of a multi-index table struct, and the access rights are stored in a Key-Value database, thereby improving the scalability of the decentralised IoT system. Additionally, in order to strengthen the overall security of the system, the access records were maintained on both the blockchain and the database.

In [13], the author proposes a blockchain-based Internet of Things communication system. Researchers use an Ethereum smart contact for combine IoT devices into "bubbles" of trust, which they call "bubbles of trust." Each bubble is overseen by a "master," who determines which devices are permitted to enter the bubble. In order for a device to become a member of a bubble, it must first give a "lightweight certificate" signed by the bubble master to the smart contract. After becoming a member of a bubble, an interface to communicate with the other members of the bubble. A smart contract is required for communication since it determines whether or not the transmitting and receiving devices are located within the same bubble of devices.

The researchers in [14] presents a blockchain based framework for controlling access to IoT devices. The proposed method is based on an Ethereum smart contract where “managers” may define the IoT resources which another device can access. Resource requests are handled by gateway nodes, sometimes known as "management hubs," which take into account the policies contained in the blockchain when making decisions about how to allocate resources.

In [15], the author proposes an Internet of Things-based access management system based on smart contracts. An "access control contract" is used to record the activities that a "subject" can do on a "object," as well as the permissions that are granted to them, during the creation process. In the context of access control contracts, a "register contract" is in charge of maintaining a mapping between subject-object identifier pairs and access control contract addresses. An Internet of Things gateway is in charge of processing resource requests and enforcing the access control policies stated in the related access control smart contract, among other things. A common theme among these solutions is that they employ smart contracts to store the activities that a single user can execute on a certain Internet of Things device or resource. The token amount of individuals is taken into account in the access control settings in our system, which goes beyond previous techniques. With another way of saying it, their solutions are analogous to an access control system that is based on user names and passwords, whereas our approach is analogous to a role-based access control system. Our technique also allows for certain innovative structures by exploiting the token handling capabilities of the Ethereum platform. For more information, please see our website.

Earlier this year, the research published in [16] investigated the possibility of smart contracts in the context of machine-to-machine (M2M) communications. In order to accomplish this, they created and analysed an Internet of Things system for automated, M2M fuel purchases that utilised Ethereum smart contracts to complete the transactions. This is also the direction in which our work is going. However, in addition to merely utilising smart contracts to facilitate message transfer and payment, our solution also helps to incorporate interaction and network management features as standard.

The section provides an overview of the present status of security mechanisms in the Internet of Things, as well as the need for further development. The results of the poll provide us with information on a variety of security problems that are associated with blockchain and IoT networks. It highlights the many approaches that have been developed by various researchers to address the difficulties that have been encountered. The poll inquires as to what actions may be made to address the situation. Due to the dispersed structure of IoT networks and the limited resources available to IoT devices, current security solutions are not completely appropriate for IoT deployment. Energy consumption and computational overhead expenses associated with traditional access control systems are considerable, resulting in a hefty cost. Furthermore, public blockchains are not ideal for IoT devices with limited resources since they require a large amount of computing power for the mining operations.

II. BLOCKCHAIN BASED IOT ARCHITECTURE

We will explore a typical smart home scenario in which a user, Alice, has outfitted her house with a variety of Internet of Things devices, such as a smart thermostat, smart lights, an

https://doi.org/10.46335/IJIES.2022.7.8.22 **e-ISSN: 2456-3463**
Vol. 7, No. 8, 2022, PP. 1-6
International Journal of Innovations in Engineering and Science, www.ijies.net

IP camera, and a number of other sensors. Specifically, the suggested architecture depicted in Figure 1 consists of three layers, which are the smart home (or, to put it a bit more broadly, the local network), the relation to a wide, and the cloud services.

We explore the following data storage and access scenarios: Alice should be able to get data from her smart home from a distance, for example, the current temperature in her bedroom, if she has a smartphone. Furthermore, intelligent technologies should really be able to transfer information on storage devices that can be accessed by a third party, such as a smart thermostat provider, in order to take use of certain services. Prior to delving into the specifics of the proposed design, we'll take a quick look at the various network tiers:

- Integrated Smart Home: The integrated smart home is broken down into the following three components:
- Gadgets: Any and all smart devices that are found in the house.
- Local BC: A safe and private BC that is generated and maintained by just one (or more) source of energy device(s) that is constantly online and has access to the internet. As an illustration, consider a smart hub or a home computer.

As illustrated in the smart house in Fig.2, local storage is an optional feature that may be included in each home to allow for the storage of data locally. This may be a backup disc on your computer's local network.

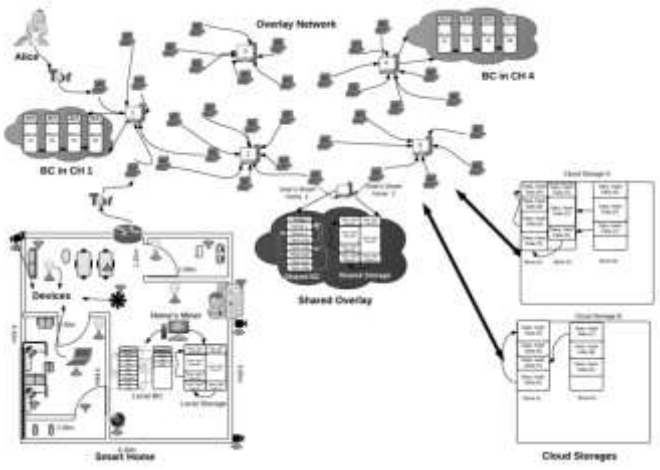

Fig 2- Schematic Architecture for Blockchain Based IoT Architecture

In addition to these components, each house's miner maintains a list of public key identifiers (PKs) that are used to grant people permission to view the smart home data.

III. CONCLUSION

The present Internet of Things-enabled technologies are confronted with a slew of difficulties, including privacy concerns and security concerns. Blockchain technology offers optimism that it would be able to overcome the difficulties described above without the need of a trusted third party. Throughout this paper, we have explored the necessity of blockchain in the Internet of Things and given state-of-the-art research.

Despite the numerous benefits of blockchain technology, it is not without its drawbacks as well. As previously mentioned, Ethereum (and most blockchain systems) incur a monetary penalty as well as a slight delay in the processing of transactions. Unluckily, and because Ethereum is still considered an innovative protocol, the financial cost of operations is subject to significant fluctuations.

The blockchain is the only means through which clients may communicate with IoT devices in the construction described in this article. Cases in which a customer comes into direct contact with an IoT gateway, of course, can be taken into consideration. Because of the distributed nature of blockchain technology, we have been able to develop an event-based system for controlling Internet of Things devices that are linked to Web of Things gateways. In addition, we improved our architecture by implementing a network management solution is based on bespoke blockchain tokens created just for us. Blockchain and smart agreements are an exciting and rapidly growing technology that has virtually limitless potential. As a result, our system may be customised in a variety of ways. In this article, we provide the outstanding research topics as well as our findings that may be helpful in the development of ethereum - based Internet of Things systems.

REFERENCES

[1] *Ouaddah, A.; Mousannif, H.; Ouahman, A.A. Access control models in loT: The road ahead. In Proceedings of the 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, Morocco, 17–20 November 2016; pp. 272–277.*

[2] *G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, 2014.*

[3] *A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in 2017 IEEE International Conference on*

Pervasive Computing and Communications Workshops (PerCom Workshops), March 2017, pp. 618–623.

[4] *D. Nguyen, P. Pathirana, M. Ding and A. Seneviratne, "Secure Computation Offloading in Blockchain based IoT Networks with Deep Reinforcement Learning," in IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2021.3106956.*

[5] *A. S. M. S. Hosen et al., "Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network," in IEEE Access, vol. 8, pp. 117266-117277, 2020, doi: 10.1109/ACCESS.2020.3004486.*

[6] *B. Shala, U. Trick, A. Lehmann, B. Ghita and S. Shiaeles, "Blockchain and Trust for Secure, End-User-Based and Decentralized IoT Service Provision," in IEEE Access, vol. 8, pp. 119961-119979, 2020, doi: 10.1109/ACCESS.2020.3005541.*

[7] *S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere and S. P. Mohanty, "Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1363-1376, Nov. 2020, doi: 10.1109/TEM.2020.2989779.*

[8] *N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris and G. C. Polyzos, "Secure IoT Access at Scale Using Blockchains and Smart Contracts," 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2019, pp. 1-6, doi: 10.1109/WoWMoM.2019.8793047.*

[9] *R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.*

[10] *C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," in IEEE Internet of Things Journal, vol. 7, no. 2, pp. 818-829, Feb. 2020, doi: 10.1109/JIOT.2019.2944400.*

[11] *S. Sun, S. Chen, R. Du, W. Li and D. Qi, "Blockchain Based Fine-Grained and Scalable Access Control for IoT Security and Privacy," 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), 2019, pp. 598-603, doi: 10.1109/DSC.2019.00097.*

[12] *M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," Computers and Security, vol. 78, pp. 126 – 142, 2018.*

[13] *O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, April 2018.*

[14] *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, pp. 1–1, 2019.*

[15] *Y. Hanada, L. Hsiao, and P. Levis, "Smart contracts for machine-to-machine communication: Possibilities and limitations," in 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS), Nov 2018, pp. 130–136.*