Access control offered by blockchain to avoid cyber threats in IoT

Abstract:

The Internet of Things, also abbreviated as IoT and having increasing relevance in today's world due to the rapid development of internet technology, is a concept that is sometimes referred to as IoT. When applied to the structure of a large-scale network that is scattered across several places, the standard ways of restricting access are insufficient. The great majority of them are based on a centralized method, which compels users to consistently employ a trusted third party (TTP) in order to complete their transactions. One of the most major limitations of these systems is that they have this limitation. Researchers have been successful in finding a solution to the problems that have been occurring with the system's security as a direct result of the creation of a technology known as blockchain. This article propose a blockchain-based access control taxonomy in accordance with the nature of access control.

Keywords: Internet of Things (IoT); blockchain; access control; IoT applications;

1.Introduction

The Internet of Things (IoT) has brought about substantial changes both to the ways in which individuals interact with one another and to the topics that are brought up in such interactions. In this respect, the fact that devices connected to the Internet of Things have restricted access to various resources creates a challenge. These solutions, as a result of their reliance, are vulnerable to a wide array of dangers. Blockchain is now the leading choice for permitting safe access control in IoT in order to foil a variety of cyberattacks. This is because blockchain is decentralized, meaning that no third party is required to verify or authenticate transactions. They one day make it possible to ensure users' privacy, data integrity, and safety. However, despite being offered by Satoshi Nakamoto as the central technology behind (Nakamoto 2008), the blockchain did not become widely employed outside of the realm of cryptocurrencies until the release of Ethereum (Buterin 2014). This is despite the fact that Nakamoto offered the blockchain as the central technology behind. Despite the fact that Nakamoto suggested using blockchain technology as the core component of Bitcoin in 2008, this has not come to pass. These requirements and rules can be enforced automatically. Ethereum supports both the construction and execution of smart contracts. Every person who is taking part in the transaction will be able to view and access these rules and guidelines if they are saved on the Ethereum blockchain. The contract requires a number of activities to be carried out, but these activities can only be carried out if all of the rules and restrictions of the contract are satisfied. The contract states that a number of activities are to be carried out. At the moment, a wide variety of blockchain systems offer support for the execution of smart contracts. This is a growing trend. Ethereum and Hyperledger Fabric (Androulaki 2018) are two examples of these kind of systems, although there are a great many more. The development of a wide variety of applications, including smart agriculture, smart grids, and smart cities (Hakak 2020), as well as a huge number of other applications, can make use of blockchain technology that is equipped with smart contracts. One example of an application that could benefit from this is the creation of smart cities (Hakak,2020). This was done so that

new methodologies might be developed and a wide variety of research-related questions could be answered. The format of the Systematic Literature Review (SLR) is consistent with what is outlined in the following paragraphs. A thorough analysis of the studies that were gathered was followed by the preparation of a summary that can be found in the section that is devoted to the findings. An explanation of the many responses to the research questions that were included in this study can be found in the section of this study that is titled "Answers to research questions." In the part that is labeled "Challenges and future work," a number of issues and potential avenues of investigation that are associated with blockchain-enabled secure access management in the Internet of Things (IoT) are investigated.

2. Related Works

Lone and (Naaz 2021) carried out an SLR that centered on the significance of making use of smart contracts and ensuring the safety of the Internet of Things. The findings of their analysis suggest that the implementation of blockchain smart contracts has the potential to make available access to a substantial fraction of the many security services that are already on the market. However, this list is not complete. This was the conclusion reached after the researchers analyzed the data from their tests. This would allow for the development of Internet of Things (IoT) safety measures. (Stojkov 2020) conducted research in which blockchain-driven access control solutions for the Internet of Things (IoT) were compared with others. Utilizing blockchain technology was investigated for the purpose of determining whether or not it is possible to circumvent the difficulties presented by conventional access control methods. We got to the conclusion that it is feasible to make the switch from traditional solutions to those that are based on the technology of blockchain for a variety of applications. Because of this, we arrived at the conclusion that the shift can successfully be made. (Patil 2021) conducted research on the potential security benefits that blockchain technology could provide to the health care industry, supply chain etc., They came to the conclusion that the consortium blockchain approach, when combined with an efficient consensus algorithm, is the best choice for a wide variety of applications. This was one of the reasons why they came to this conclusion. This was one of the findings that led them to come to this conclusion. The researchers (Patel 2020) presented a review on the potential enhancements that might be made to the IoT access control system by utilizing decentralized architecture that makes use of blockchain technology. They arrived to the conclusion that blockchain technology has the ability to make IoT transactions more secure based on their findings, which led them to the conclusion. Based on the findings that they uncovered, they came to this conclusion.

(Osterberg 2021) conducted a study to determine the applicability of traditional and blockchain-enabled access control mechanisms in an Internet of Things environment. The goal of the study was to determine whether or not traditional access control mechanisms can be used in conjunction with blockchain technology. The purpose of the research was to establish whether or not conventional access control techniques are compatible with blockchain technology and to assess whether or not they may be utilized together. The authors arrived at the conclusion that one way in which the security of Internet of Things (IoT) networks might be improved is through the deployment of permissioned blockchains.

This was one of the methods that was considered. This allowed them to circumvent the problem of implementing access control functions in a manner that was more manageable. They were able to circumvent the difficulty of implementing access control mechanisms in permissioned blockchains as a result of this development.

3. Proposed Research Methodology

The strategy that has been advocated for developing an Internet of Things system with access control security that is both lightweight and decentralized is based on a multi-agent system and makes use of a private blockchain. This strategy was developed so that an Internet of Things system could be created. Figure 1 depicts the suggested design, which has a structure for the blockchain that is hierarchical in its very nature. You can get an overall picture of the suggested detailed architecture by looking at it in its whole down below. Each BCM has its own individual contents, which can be broken down into three categories: transactions, block headers, and MAC policy headers. In addition, the Internet of Things has special requirements, such as scalability, distributed nature, and restricted devices; our framework is well-suited to meet these requirements due to its scalability and distributed nature. In conclusion, the architecture that we have presented can be generalized and is appropriate for use in a wide variety of applications that are related to the Internet of Things (IoT).

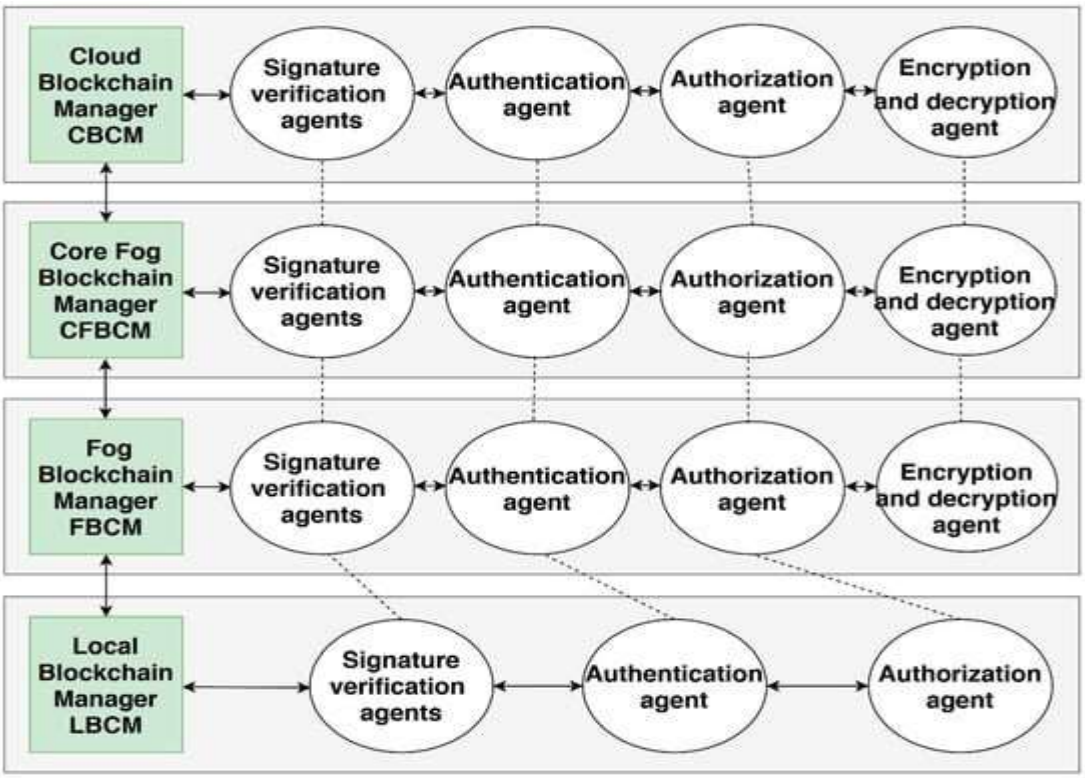

Figure 1: The proposed organizational structure

3.1. Transactions

Any of the following can take part in a transaction: devices connected to the Internet of Things (IoT). Transactions are, essentially, interactions between the aforementioned entities.

Transactions can be arranged in a number of distinct classifications according to the functions that they carry out, which are referred to as Access, Update, Add, Monitor, and Remove respectively. In order for BCMs to obtain access to data, they will first generate what is called as an Access transaction. This transaction is connected with the process of providing authorization to read-only access. Created by devices or nodes in order to update data that has been saved, update transactions are connected to the process of providing permission to read and write. BCMs are granted read and write access, which enables them to generate transactions by making use of the Add, Remove, and/or Monitor capabilities. Add transactions are utilized in the process of adding a new Internet of Things device or node, while Remove transactions are utilized in the process of removing them. Add transactions are also utilized in the process of removing any existing Internet of Things devices or nodes. Monitor transactions allow for the information and status of Internet of Things devices and nodes to be observed. These transactions are what are utilized to keep track of everything.

3.2. Policy of the MAC

The term "Mandatory Access Control" comes from the fact that authorization is required to get entry. This, in turn, has the potential to function as a contributor toward reducing the overall amount of security breaches that occur. The subject's (the user's) security clearance, which can be classified as secret, top secret, or confidential, and the resource classification of an object, which can similarly be classified as secret, top secret, or confidential, are the two criteria that go into defining MAC. The subject's security clearance can be classified as secret, and the user's security clearance can be classified as secret or top secret. There are three levels of secrecy that can be applied to a subject's security clearance: secret, top secret, and confidential. There is information that is pertinent to clearance and classification contained inside the security labels.

When determining whether or not to comply with a request, it is necessary to take into account not only the clearance levels of the individuals involved but also the classification levels of the things in question. This is done so that it can be determined whether or not the subject in question is permitted to access the item in question. In order to carry out this technique in the correct manner, the Bell-LaPadula model is used. In addition to this, it places a significant focus on the maintenance of the confidentiality of user data and ensures that users do not have access to resources that are beyond the scope of their security clearance, as can be seen in Figure 3. In addition to this, it ensures that users do not have access to resources that are beyond the scope of their security clearance.

3.3. Blockchains are managed by BCMs.

Local Blockchain Managers (LBCM), Fog Blockchain Managers (FBCM), basis Fog Blockchain Managers (CFBCM), and Cloud Blockchain Managers (CBCM) are the names given to the Blockchain Control Modules (BCMs) that serve as the foundation of the architecture that we have presented. These Business Communication Managers are accountable for supervising the management of all communications that take place inside

each of the four layers of the framework. Additionally, BCMs are the ones who are responsible for creating the access control policy that will apply to each device and node in each tier. This policy will be applied by the BCMs. A block header and a policy header are included in every single one of the blocks that make up the blockchain. These headers have information about the block that they are heading. Every transaction that is recorded in the blockchain is assigned its own unique MAC policy, which is stored as part of the block structure for that transaction. Because each BCM is furnished with a policy header, it is possible for these devices to exert control over the access permissions associated with each and every transaction. Despite the fact that a policy header must be included for each and every block in a blockchain, the only one that can be accessed in order to verify and alter policies is the most recent policy header, which is always located at the top of the block header in BCMs and is the only one that can be used to check and edit policies. The BCM acts as a stand-in for the miner throughout all of the different layers in the procedure that has been supplied. The BCM is the principal security device that is liable for verifying, approving, and auditing transactions. The BCM is the one who is responsible for carrying out this duty. In addition, when a new block is added to the blockchain, the BCMs construct a pointer to the previous block, copy the policy that was in the header of the previous block to the new block, and then attach the new block to the blockchain. This process happens every time a new block is added to the blockchain. In the event that a new block is added to the blockchain, this procedure will take place.

3.4. Agents of Software

The framework that has been suggested makes use of a software agent that is capable of performing its functions effectively due to the fact that it is mobile, flexible, transparent, ragged, and starts and stops itself on its own accord.

3.4.1. Agent responsible for verifying signatures

This mobile agent can be found in the BCMs, which is where they are kept for your convenience. The agent's principal goal is to ensure that the message's integrity is preserved at all times. This requires confirming that a message was delivered by a user who is known to the system, that the message did not experience any changes while it was in transit, and that the agent is unconcerned with any encrypted data that may be present in the message. In addition, this involves ensuring that the message did not experience any changes while it was in transit. When it comes to LBCM, the only thing that concerns us is making sure that the data have not been tampered with in any manner. This is important in order for symmetric key techniques, which are also known as shared secret keys, to be deployed in order to develop trust between various devices that are part of the Internet of Things (IoT). As a direct result of this, we make use of a simple hashing mechanism in conjunction with verification agents that are appropriate for devices linked to the Internet of Things that have limited capacities for processing data..

After successfully decrypting the message with the private key that is owned jointly by both parties, the verification agent is able to validate the contents in the LBCM layer. This is possible because the private key is kept jointly by both parties. In order to carry out this verification, the value that was derived from the hash that was sent is compared to the value that was generated.

The production of a hash value of the original message and the attachment of the sender's private key to each message that is signed is seen in Figure 4. This is the method through which digital signatures function. The verification agent first decrypts the message by using the sender's public key, and then validates the contents by comparing the hash value that was received with the hash value that was created. The reliability of the contents is ensured by going through this process. If both numbers are the same, this implies that the message has not been altered in any manner, which in turn proves the identity of the sender. If both values are different, however, this does not imply that the message has not been altered. When both of these values are different from one another, it suggests that the message has been changed in some way.

3.4.2. Authenticator

This agent is accountable for determining whether or not the credentials presented by a user are genuine, as well as ensuring that they are accurate and up to date. In order for the network as a whole to operate correctly, each individual device and node in the network needs to have access to the same secret key. Every BCM miner contains a component known as an Authentication Agent, the sole function of which is to verify that a user is authentic and authorized to use the miner. The BCM miner that is situated at each tier is the one who is accountable for the distribution of a shared secret key. In order to keep their communications secure, two parties who are not familiar with one another might use this method to generate a secret key that they can both keep to themselves and use to encrypt their messages. There is the possibility that the communication between the two parties will take place across a channel that is not encrypted. The Diffie-Hellman key exchange method serves as the foundation for the shared secret key that must be protected in any and all circumstances.
If an agent finds out that two Internet of Things devices or nodes on the same layer want to connect with one another, it will first investigate those devices or nodes to see if they have the appropriate shared key or not. In the event that, on the other hand, the nodes of the Internet of Things are scattered throughout several tiers, then public key cryptography will be utilized for the communication between the BCMs in each tier. The communication will be thrown away if the agent is unable to verify the identities of the individuals involved in it. They will be able to speak with one another and will proceed to the subsequent phase, which is the Authorization Agent, if the agent arrives at the conclusion that their identities can be trusted. It is the responsibility of the Authorization Agent to determine which resources users are allowed to access in accordance with the parameters that are defined in the MAC policy..

3.4.3. Authorization Officer

After the requester has been authenticated, this agent is tasked with the responsibility of enforcing access control policies and giving authorization privileges to the requester depending on the digital identification (ID) of the requester. This agent also has the responsibility of supplying authorization privileges. It gives the BCM miner the power to precisely identify what IoT devices and nodes are permitted to accomplish in accordance with the MAC regulations. This is done in order to protect the resources. The current search follows directly on the heels of the one that came before it. The MAC policy file utilized by the BCM miner is the one that underwent the most recent round of editing, and the modification date is derived from the block header that was generated most recently. This agent puts into practice the idea of the MAC policy, which determines the kind of authorization (read; write) depending on the security classification level of the information that is being accessed. The MAC policy establishes that the type of authorization (read; write) depends on the information. In addition to this, the Authentication Agent keeps track of the activities that the devices and nodes connected to the Internet of Things (IoT) are participating in and assigns a trust value to each individual Internet of Things device and node. In addition to this, it implements the access control policy by determining which resources the users are allowed to access by following the Bell-LaPadula model as a reference. This is done in order to maintain security. This is done by determining which resources the users are allowed to access.

3.4.4. Encrypt/Decrypt Agent

This mobile agent ensures that data are kept confidential and that only authorized users and agents are able to access and comprehend these data. In addition, this agent restricts who may read and understand the data. This agent further ensures that only authorized users and agents are able to view and comprehend the data by restricting access to it. This particular agent can be found in CBCM, FBCM, and CFBCM in that order. We function under the presumption that there is no demand for the privacy of data transmissions between IoT devices in LBCM. On the other hand, there is a requirement for the privacy of data transmissions between any BCMs. The agent is able to encrypt and decrypt any and all of the data as well as the access control policies that are transmitted between BCMs. This capability extends to both the data and the rules. An asymmetric algorithm is utilized by this agent.

A sequence diagram, such as the one that is displayed in Figure 5, can be used to illustrate the interaction that takes place. This interaction is depicted in a sequence diagram. This interaction is shown to take place when the user makes a request to change the data in a resource. After all of the tasks that came before it have been finished, we will now discuss how a user can edit data in accordance with our infrastructure. If a user wants to make changes to data that already exists, the application must first submit a request to the Authentication Agent, and the Authentication Agent will then check the user's identity before allowing the changes to take effect. Within the context of this transaction, the user is in possession of a private shared key that can be utilized. An investigation of the user's claim of identification is carried out by the Authentication Agent. Once the Authentication Agent determines that the user's claim is true since it is in possession of a valid key, it issues an

identification card to the user. The following step that needs to take place is for the user to make use of the ID that was provided to them in order to submit a request to the Authorization Agent. The Authorization Agent is the individual who is responsible for carrying out the MAC procedure in its entirety. In order to identify whether or not the user is authorized to access the resource, it performs a check against the MAC policies of both the user and the resource. Access has been provided to the user in this scenario since they are unable to read or write information that is either higher or lower than the categorization level that they now possess. After that, the user is only able to carry out actions that are permitted by the MAC policy, and they are required to directly submit a request to the authorized resource in order to update the data. Following the modification of the resource, an updated transaction including a revised value for the blockchain hash is transmitted to the LBCM. The final step of the procedure involves the LBCM submitting an updated transaction to the Authorization Agent in order to inform them of the changed resource and to bring the hash value that is stored on the blockchain up to date. This part of the procedure is called the "confirmation phase."

4. Results and Discussion

This highlights not only the way for enabling distributed access control but also the secure flow of information from devices that are connected to the internet of things. The blockchain-based secure access control system that was built was assisted in its deployment by using the NS2 simulation tool as one of the tools that contributed to its development. Throughout the entirety of this procedure, we made use of an Intel i3 central processing unit (CPU) that was equipped with 2 gigabytes of random access memory (RAM) and ran the Ubuntu operating system. Additionally, in the course of constructing a mechanism that assures the safe transmission of data, an i7-4510U central processing unit (CPU) and 8 gigabytes of random access memory (RAM) were deployed. As data-sharing technologies have gradually gotten more advanced over the past few years, a growing number of businesses have gradually adopted them. As a direct result of this, the only way to effectively extract the value of the data is through the utilization of data exchanges that are encrypted. However, the first architecture for data interchange does not provide an easy mechanism of monitoring how digital data is employed. This is a limitation of the architecture. One further problem is that the people who are providing the data are reluctant to reveal the information that they know, which is something that should not be the case. This research was carried out with the goal of coming up with a plan for data sharing that makes use of the blockchain technology that is already accessible. Because of the steps that were taken to achieve this goal, the research was effective in resolving the challenges of safety and control that are inherent in traditional types of centralized data sharing and administration. This was possible as a result of the actions that were done to achieve this goal. In addition to that, the researchers investigated whether or not the model was secure and whether or not it was practicable. This piece presented a paradigm for the exchange of data that is based on blockchain technology and showed that it is viable, secure, easy to regulate, and very effective. Additionally, the paradigm was shown to be viable, secure, and successful. In addition to this, it provided evidence that demonstrates the viability of this paradigm. The ACE-BC framework was utilized to construct this architecture, and the blockchain served as the foundation for the decentralized information

security access that the architecture provides. Additionally, the entire database was encrypted synchronously, which not only serves as the connecting link for the entire design but also protects the data from having its integrity compromised in the event of a hacking attempt. This is due to the fact that centralized storage can give rise to issues. The simulation's parameters were connected to a graphical representation of the security criteria, which may be found in Table 1 of the reference materials.

Simulation parameters, Table 1.

Parameter	Description
Block size	1 MB
Transmission Range	300 m
Message Size	1.5 GB
Total Number of Nodes	Random (10,000–30,000)
Number of Blocks	Random (100–250)
Security Protocols	AP, CKP
Traffic Type	Constant Bit Rate
Timestamp	128 bit

4.1. The percentage of secrecy afforded to the data.

The platform that blockchain technology provides for the flow of data is not only one that is secure, but also one that is very effective in its operation. The solution that was presented makes use of label data to categorize individuals for the purpose of delivering more granular data sharing services with the intention of preserving data confidentiality. The protection of sensitive information was the motivation behind this action. Before the transfer may be regarded successful, this step must first be completed. Because of this, the data will be able to be transferred without having its integrity compromised in any way. The detection server is the central component of the system for sharing information. In this configuration, label data from all clients is gathered and processed by a centralized server. The server then uses cosine similarity to determine which communities exist and then publishes the results of this analysis on a blockchain. Through the use of the blockchain client, users are offered access to the aggregated statistics as well as the opportunity to collaborate on the aggregated data. It has been demonstrated that the proposed framework offers significant performance advantages in contrast to the approaches that are currently being used, both in terms of the amount of time and expense that are required and the amount of throughput that is produced. These benefits came to light as a consequence of the experiments that were conducted. Additionally, it was found that the advised method, when put through its paces in experimental simulations, resulted in a significant increase in the efficiency of information transfer. This was established after the strategy was put through its paces. Figure 2 presents

an illustration of the extent to which the ACE-BC design, which is currently the topic of debate, safeguards the confidentiality of data.

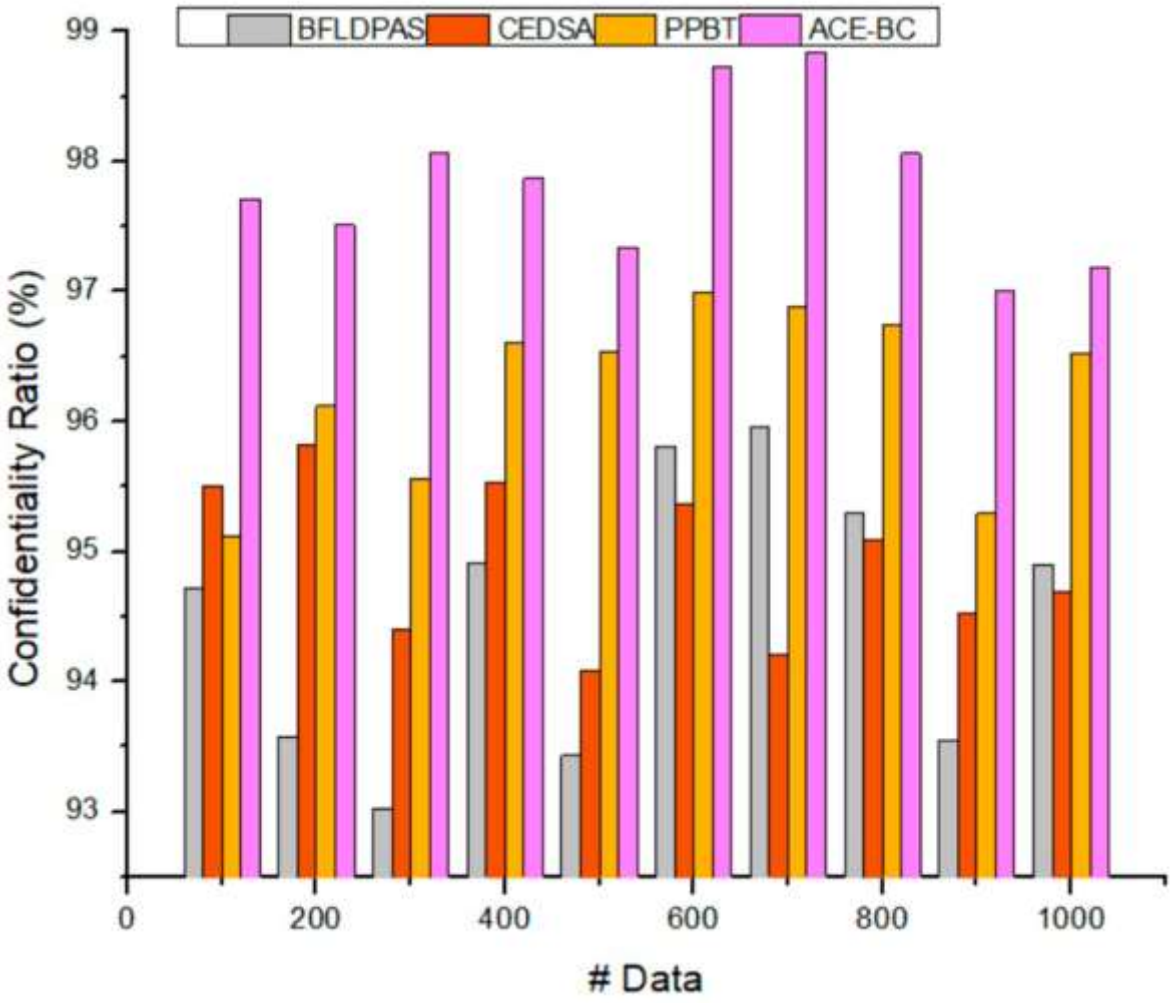

Figure 2 Rate of data secrecy

4.2. Ratio of throughput

After dividing the size of the file by the amount of time it took to achieve the throughput, which was then given as the number of megabits, kilobits, or bits per second, the throughput could be determined. The throughput of the network refers to the rate at which data may be transferred from one point on the network to another. This rate can vary depending on the type of data being transferred. It is common practice to express the speed of a network in terms of the number of bits that are transferred in a given amount of time, such as megabits or gigabits. This is because it is easier to measure and understand. This is due to the fact that it is simpler to measure the amount of data that is transmitted in a certain amount of time. This is due to the fact that it is simpler to both measure and comprehend. The amount of data as well as its speed were taken into consideration for this throughput analysis. The throughput statistic was utilized so that a justification could be made regarding how successfully the information was transferred in a secure manner to the end user. To begin, attribute-based encryption is a costly form of cryptographic primitive, which makes it difficult to satisfy the

good throughput need of time series Internet of Things data in a business scenario due to the fact that the required throughput is too high. The approach that was explained in this article was able to circumvent the problem of relying on a single point of failure, as was discussed previously in the passage. This was accomplished by greatly decentralizing the system. To begin, the distributed ledger technology, also known as blockchain, along with shared data storage devices served as the foundation for the foundation of this method of information exchange. The decentralized nature of the blockchain extends to both the protection of its integrity and the distribution of its data. As a direct result of this, the vulnerability of the network as a whole will not be affected even if a single node in the network loses its functioning. Second, using this paradigm makes it possible for diverse attribute management authorities to coordinate their efforts, which is something that would not be attainable by any other method. This is something that would not be possible without using this paradigm. The system is more resistant to the failure of any of the distinct attribute authorities as a result of the functions of the distinct attribute authorities being divided. In addition to this, the system is improved in its ability to avoid service disruptions caused by illicit actions. In addition, in contrast to the alternative scenario, in which the owner is accountable for the management of the attribute, the data owner in this study was in no way involved in the upkeep of the attribute in any manner. This is in contrast to the alternative scenario, in which the owner is responsible for maintaining the attribute. This occurs as a result of the attribute being severed from its connection to the data owner. Because the data owner is unable to respond quickly, data unavailability can be avoided by limiting the data owner to the job of data manager and banning them from carrying out any other user-managed actions. This will prevent the data owner from making the data unavailable. We were successful in achieving a throughput ratio of 98.2% with the help of the model that was suggested. Figure 3 provides an illustration of the suggested throughput ratio for the ACE-BC framework. This ratio was mentioned earlier.

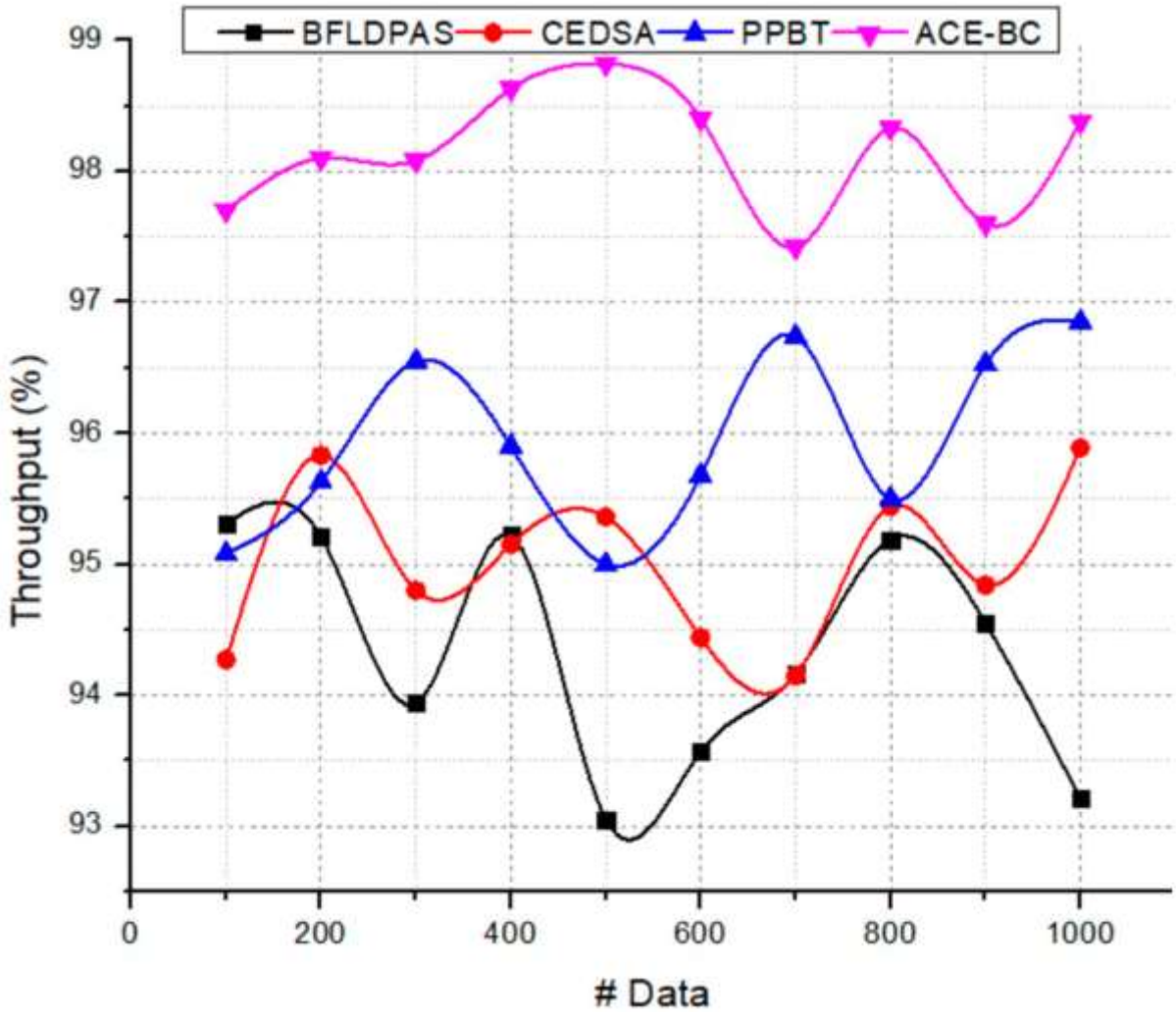

Figure 3 The ratio of throughput.

4.5. Computation Time

During the course of this study, the amount of time that was needed by each user in order to successfully complete a number of various encryption procedures was measured and analyzed. This research was carried out in order to answer the following question:. According to the conclusions of this research, a sizeable fraction of the overall amount of time was taken up by the amount of time spent computing that was required for blockchain operations. It is important that you take note of the fact that the data access key on blockchains has been granted to this study as part of the protocol. Because of this, the amount of time necessary to complete the computation was not directly impacted by the volume of data that was being processed. Additionally, the time spent on blockchain operations accounted for the vast majority of the total amount of operating time that was utilized by each user. This was the case even though each user only had a limited amount of time available to devote to blockchain operations. This is as a result of the fact that in order to show that they behaved themselves in a trustworthy manner, it was necessary for both the recipient and the sender to carry out verification procedures. In other words, both parties were required to verify each

other. In particular, when the blockchain was operating, it took the receiver only 0.6 milliseconds to figure out the data access key for the data that belonged to the recipient. Figure 4 presents the total amount of time consumed by computer activities.

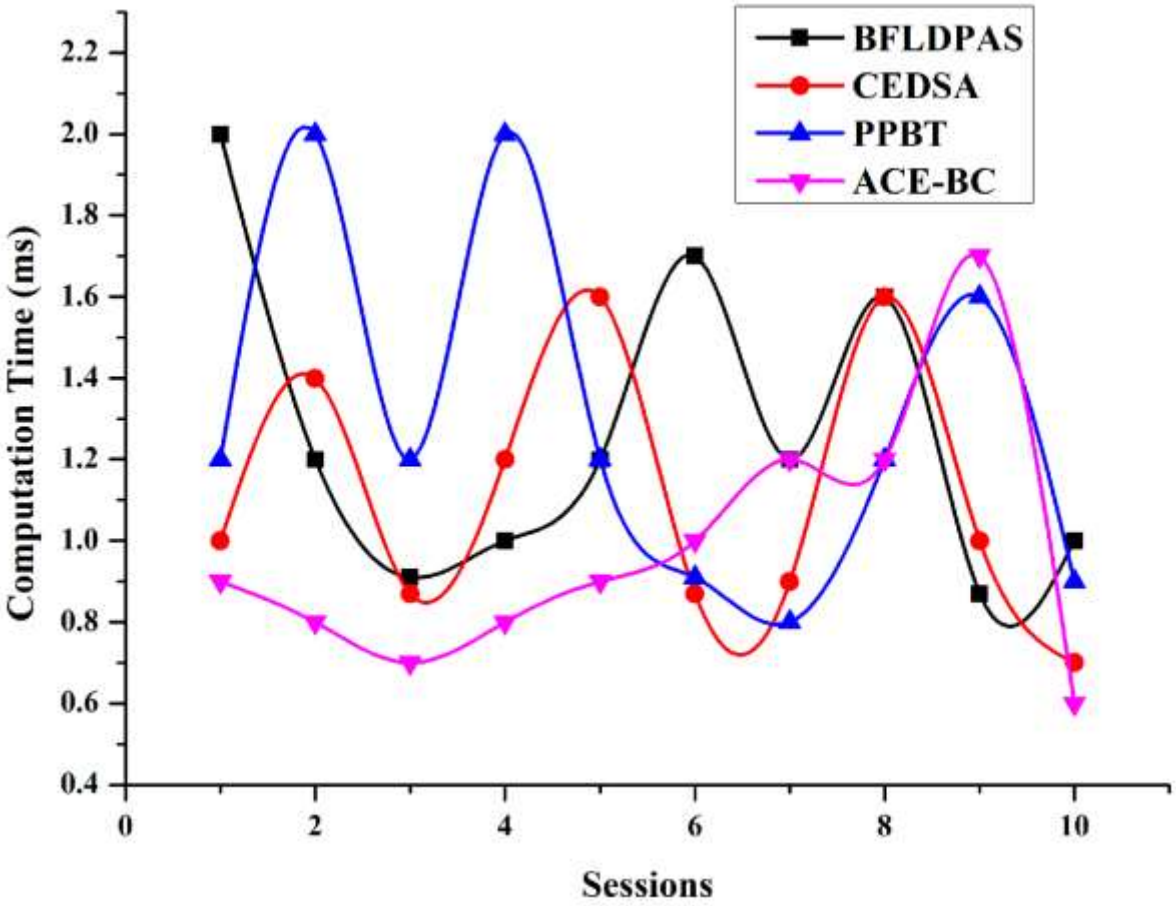

Figure 4 Calculation Time

5. Conclusion

The Internet of Things (IoT) system presents an exceptionally wide variety of potential dangers to the users' personal information as well as their physical safety. As a result, careful thought is required in this area. Both centralized and decentralized methods of problem solving come with their own individual sets of benefits and drawbacks, respectively. While centralized solutions are limited in their ability to scale, decentralized approaches suffer limitations such as delays, computational overheads, and energy limits. Centralized solutions are limited in their ability to scale. The ability to scale that centralized solutions have is severely restricted. We offered a multi-agent system as a means of achieving our goal of providing effective and decentralized methods of access control security for the Internet of Things (IoT). Additionally, it is the responsibility of BCMs to ensure that the necessary level of security is in place at all times. The architecture that has been provided is a solution that can be generalized and employed for a wide variety of Internet of Things applications in their many different forms. This was accomplished by utilizing a solution that can be applied for generalization. In addition, the problems that are caused by the Internet of Things have not been well addressed in the study that has been done previously. This is because the majority of these studies have concentrated on the problems that are produced by access control in a

particular Internet of Things application, such as a smart house, rather than the problems that are generated by the Internet of Things itself. This is why we have this situation. The writers are well aware of the fact that the evaluation of research needs to be based on phases of implementation and testing in order to determine the applicability and efficacy of the solution in comparison to other research. However, this research is still in the process of being carried out, and the authors are of the opinion that the findings of these two phases ought to be released in a paper that is independent from the rest of the discoveries that have been found in this investigation. This is due to the fact that it is anticipated that, in addition to fresh contributions, a huge number of particulars would need to be taken into consideration. This is owing to the fact that it is anticipated that additional donations would be made, which is the cause for this situation.

In further study, the suggested framework will be applied to a real-world setting in order to conduct an investigation on the degree to which the primary security goals with regard to integrity have been attained. This evaluation will be carried out with the purpose of establishing whether or not the primary security goals have been accomplished successfully. This will be completed through the use of a digital signature, authentication will be performed through the utilization of shared secret keys, authorization will be performed through the utilization of the MAC policy, and confidentiality will be performed through the utilization of public key encryption. In order to address the issue of the enormous header size in the blockchain, we will investigate a wide range of potential solutions from a variety of different angles. Both of these locations would be unique from the blockchain itself. In this specific area, the proposed architecture will be improved, and a case study will be conducted on applications for the internet of things (IoT) that call for an exceptionally high level of security. For the deployment of the solution, a RaspberryPI Internet of Things device will be used, and a private blockchain platform will be used for the dissemination of the solution. When they are ultimately brought out into the world, the next works are going to, once again, supply additional knowledge.

References

Ahmed, M. T., Al Hashim, F., Hashim, S. J., and Abdullah, A. (2022). Hierarchical blockchain structure for node authentication in IoT networks. Egypt. Inform. J. 23, 345–361. doi: 10.1016/j.eij.2022.02.005

Alharbi, A. Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System. *Sensors* **2023**, *23*, 3020. https://doi.org/10.3390/s23063020

Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K., et al. (2021). Blockchain-based secured access control in an iot system. Appl. Sci., 11, 1–16. doi: 10.3390/app11041772

Ali, G., Ahmad, N., Cao, Y., Asif, M., Cruickshank, H., Ali, Q. E., et al. (2019). Blockchain based permission delegation and access control in Internet of Things (BACI). Comput. Secur. 86, 318–334. doi: 10.1016/j.cose.2019.06.010

Androulaki, E, Barger, A., Bortnikov, V., Cachin, C., Christidis, K., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. EuroSys. 18 Proc. Thirteenth EuroSys Conf. 30, 1–15. doi: 10.1145/3190508.3190538

Bera, B., Chattaraj, D., and Das, A. K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. Comput. Commun. 153, 229–249. doi: 10.1016/j.comcom.2020.02.011

Bera, B., Saha, S., Das, A. K., and Vasilakos, A. V. (2021). Designing blockchain-based access control protocol in iot-enabled smart-grid system. IEEE Internet Things J. 8, 5744–5761. doi: 10.1109/JIOT.2020.3030308

Breiki, H., Al Qassem, L., Al, S.alah, K., Ur Rehman, M. H., and Sevtinovi, D. (2019). "Decentralized access control for IoT data using blockchain and trusted oracles," Proceedings - IEEE International Conference Ind. Internet Cloud, ICII 2019, no. ICII 248–257.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Etherum, 1–36. Available online at: http://www.buyxpr.com/build/pdfs/EthereumWhitePaper.pdf

Butun, I., and Osterberg, P. (2021). A review of distributed access control for blockchain systems towards securing the internet of things. IEEE Access 9, 5428–5441. doi: 10.1109/ACCESS.2020.3047902

Dadhania, A. J., and Patel, H. B. (2020). "Access control mechanism in internet of things using blockchain technology: A review," Proceedings of the 3rd International Conference Intellectual Sustainable System ICISS 2020. New York, IEEE, 45–50.

Ding, S., Cao, J., Li, C., Fan, K., and Li, H. (2019). A novel attribute-based access control scheme using blockchain for IoT. IEEE Access. 7, 38431–38441. doi: 10.1109/ACCESS.2019.2905846

Dukkipati, C., Zhang, Y., and Cheng, L. C. (2018). "Decentralized, blockchain based access control framework for the heterogeneous internet of things," ABAC 2018 - Proc. 3rd ACM Work. Attrib. Access Control. Co-located with CODASPY, 61–69.

El Kalam, A. A., Outchakoucht, A., and Es-Samaali, H. (2018). “Emergence-based access control: New approach to secure the Internet of Things,” in Proceedings of the 1st International Conference on Digital Tools & Uses Congress, 1–11.

Google Scholar

Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., and Guizani, N. (2020). Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. IEEE Netw. 34, 8–14. doi: 10.1109/MNET.001.1900178

CrossRef Full Text | Google Scholar

Han, D., Zhu, Z., Li, D., Liang, W., Souri, A., Li, K. C., et al. (2022). A blockchain-based auditable access control system for private data in service-centric IoT environments. IEEE Trans. Ind. Informatics. 18, 3530–3540. doi: 10.1109/TII.2021.3114621

CrossRef Full Text | Google Scholar

Hwang, D., Choi, J., and Kim, K. H. (2018). “Dynamic Access Control Scheme for IoT Devices using Blockchain,” 2018 International Conference on Information and Communication Technology Convergence (ICTC)2018, 713–715.

Google Scholar

Iftekhar, A., Cui, X., Tao, Q., and Zheng, C. (2021). Hyperledger fabric access control system for internet of things layer in blockchain-based applications. Entropy. 23, 1054. doi: 10.3390/e23081054

PubMed Abstract | CrossRef Full Text | Google Scholar

Islam, M. A., and Madria, S. (2019). “A permissioned blockchain based access control system for IOT,” Proceedings 2nd IEEE International Conference Blockchain, Blockchain. 469–476.

Google Scholar

Kitchenham, B. A., and Charters, S. (2007). “Guidelines for performing systematic literature reviews in software engineering,” EBSE Technical Report EBSE-2007-01. School of Computer Science and Mathematics, Keele University, 1–57.

Google Scholar

Kukreja, D., Dhurandher, S. K., and Reddy, B. V. R. (2019a). Securing ad hoc networks using energy efficient and distributed trust-based intrusion detection system. Int. J. Adv. Intell. Parad. 13, 430–448. doi: 10.1504/IJAIP.2019.101990

CrossRef Full Text | Google Scholar

Kukreja, D., Sharma, D. K., Dhurandher, S. K., and Reddy, B. V. R. (2019b). GASER: genetic algorithm-based secure and energy aware routing protocol for sparse mobile ad hoc networks. 13, 230–259. doi: 10.1504/IJAIP.2019.099953

CrossRef Full Text | Google Scholar

Li, D., Han, D., Crespi, N., Minerva, R., and Li, K. C. (2022). A blockchain-based secure storage and access control scheme for supply chain finance. J Supercomput. 78, 1–30 doi: 10.1007/s11227-022-04655-5

CrossRef Full Text | Google Scholar

Li, T., Wang, H., He, D., and Yu, J. (2022). Blockchain-based Privacy-preserving and Rewarding Private Data Sharing for IoT. IEEE Internet Things J. 9, 15138–15149. doi: 10.1109/JIOT.2022.3147925

CrossRef Full Text | Google Scholar

Li, Z., Hao, J., Liu, J., Wang, H., and Xian, M. (2021). An IoT-applicable access control model under double-layer blockchain. IEEE Trans. Circuits Syst. II Express Briefs 68, 2102–2106. doi: 10.1109/TCSII.2020.3045031

CrossRef Full Text | Google Scholar

Liu, H., Han, D., and Li, D. (2020). Fabric-iot: a blockchain-based access control system in IoT. IEEE Access. 8, 18207–18218. doi: 10.1109/ACCESS.2020.2968492

CrossRef Full Text | Google Scholar

Liu, Y., Lu, Q., Chen, S., Qu, Q., Choo, K. K. K., O'Connor, H., et al. (2021). Capability-based IoT access control using blockchain. Digit. Commun. Networks. 7, 463–469. doi: 10.1016/j.dcan.2020.10.004

CrossRef Full Text | Google Scholar

Lone, A. H., and Naaz, R. (2021). Applicability of Blockchain smart contracts in securing Internet and IoT: a systematic literature review. Comput. Sci. Rev. 39, 100360. doi: 10.1016/j.cosrev.2020.100360

CrossRef Full Text | Google Scholar

Ma, M., Shi, G., and Li, F. (2019). Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. IEEE Access.7, 34045–34059. doi: 10.1109/ACCESS.2019.2904042

CrossRef Full Text | Google Scholar

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Bus. Rev. 21260, 1–221. Available online at: https://bitcoin.org/bitcoin.pdf

PubMed Abstract | Google Scholar

Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet Things J. 5, 1184–1195. doi: 10.1109/JIOT.2018.2812239

CrossRef Full Text | Google Scholar

Novo, O. (2019). Scalable access management in IoT using blockchain: A performance evaluation. IEEE Internet Things J. 6, 4694–4701. doi: 10.1109/JIOT.2018.2879679

CrossRef Full Text | Google Scholar

Oktian, Y. E., and Lee, S. G. (2021). Border chain: blockchain-based access control framework for the internet of things endpoint. IEEE Access 9, 3592–3615. doi: 10.1109/ACCESS.2020.3047413

CrossRef Full Text | Google Scholar

Ouaddah, A., AbouElkalam, A., and AitOuahman, A. (2017a). FairAccess: a new Blockchain-based access control framework for the Internet of Things. Secur. Commun. Netw. 9, 5943–5964. doi: 10.1002/sec.1748

CrossRef Full Text | Google Scholar

Ouaddah, A., Elkalam, A. A., and Ouahman, A. A. (2017b). "Harnessing the power of blockchain technology to solve IoT security and privacy issues," Proceedings of the Second International Conference Internet things, Data Cloud Comput. 1–10.

Google Scholar

Ouaddah, A., Elkalam, A. A., and Ouahman, A. A. (2017c). Towards a Novel Privacy-Preserving access control model based on blockchain technology in IoT. Eur. MENA Coop. Adv. Inf. Commun. Technol. 520, 103–112. doi: 10.1007/978-3-319-46568-5_53

CrossRef Full Text | Google Scholar

Ourad, A. Z., Belgacem, B., and Salah, K. (2018). Using blockchain for IOT access control and authentication management, vol. 10972 LNCS. Berlin, Germany: Springer International Publishing.

Google Scholar

Outchakoucht, A., Samaali, H., and Philippe, J. (2017). Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things. Int. J. Adv. Comput. Sci. Appl. 8, 417–424. doi: 10.14569/IJACSA.2017.080757

CrossRef Full Text | Google Scholar

Patil, P., Sangeetha, M., and Bhaskar, V. (2021). Blockchain for IoT access control, security and privacy: a review. Wirel. Pers. Commun. 117, 1815–1834. doi: 10.1007/s11277-020-07947-2

PubMed Abstract | CrossRef Full Text | Google Scholar

Pinno, O. J. A., Gregio, A. R. A., and De Bona, L. C. E. (2017). "Control chain: blockchain as a central enabler for access control authorizations in the IoT," in IEEE Glob. Commun. Conf. GLOBECOM 2017 - Proc. New York, IEEE, 1–6.

Google Scholar

Putra, D. R., Anggorojati, B., and Hartono, A. P. P. (2019). "Blockchain and smart-contract for scalable access control in Internet of Things," Proceeding - 2019 International Conference ICT Smart Soc. Innov. Transform. Towar. Smart Reg. ICISS 2019. New York, IEEE.

Google Scholar

Putra, G. D., Dedeoglu, V., Kanhere, S. S., Jurdak, R., and Ignjatovic, A. (2021). Trust-based blockchain authorization for IoT. IEEE Trans. Netw. Serv. Manag. 18, 1646–1658. doi: 10.1109/TNSM.2021.3077276

CrossRef Full Text | Google Scholar

Saha, S., Sutrala, A. K., Das, A. K., Kumar, N., and Rodrigues, J. P. C. (2020). "On the design of blockchain-based access control protocol for IoT-enabled healthcare applications," IEEE International Conference Commun. New York, IEEE, 1–6.

Google Scholar

Shafagh, H., Burkhalter, L., Hithnawi, A., and Duquennoy, S. (2017). "Towards blockchain-based auditable storage and sharing of iot data," CCSW 2017 - Proc. Cloud Comput. Secur. Work. co-located with CCS 2017. New York, IEEE, 45–50.

Google Scholar

Stojkov, M., Simic, M., Sladi,ć, G., and Milosavljevic, B. (2020). "Traditional and blockchain - based access control models in IoT: A Review," in ICIST 2020 Proceedings, eds. M. Zdravković, Z. Konjović, and M. Trajanović, M. New York, IEEE,51–55.

Google Scholar

Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., Javaid, N., et al. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. Appl. Sci. 10, 488. doi: 10.3390/app10020488

CrossRef Full Text | Google Scholar

Sun, S., Du, R., Chen, S., and Li, W. (2021). Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain. IEEE Access. 9, 36868–36878. doi: 10.1109/ACCESS.2021.3059863

CrossRef Full Text | Google Scholar

Tao, X., Liu, Y., Wong, P. K. Y., Chen, K., Das, M., Cheng, J. C. P., et al. (2022). Confidentiality-minded framework for blockchain-based BIM design collaboration. Autom. Construct.136, 104172. doi: 10.1016/j.autcon.2022.104172

CrossRef Full Text | Google Scholar

Tapas, N., Longo, F., Merlino, G., and Puliafito, A. (2020). Experimenting with smart contracts for access control and delegation in IoT. Futur. Gener. Comput. Syst. 111, 324–338. doi: 10.1016/j.future.2020.04.020

CrossRef Full Text | Google Scholar

Wang, P., Yue, Y., Sun, W., and Liu, J. (2019). "An attribute-based distributed access control for blockchain enabled IoT," in 2019 International Conference Wirel. Mob. Comput. Netw. Commun. New York, IEEE, 1–6.

Google Scholar

Xiang, W., and Yuanyuan, Z. (2021). Scalable access control scheme of internet of things based on blockchain. Procedia Comput. Sci. 198, 448–453. doi: 10.1016/j.procs.2021.12.268

CrossRef Full Text | Google Scholar

Xu, H., He, Q., Li, X., Jiang, B., and Qin, K. (2020). BDSS-FA: a blockchain-based data security sharing platform with fine-grained access control. IEEE Access. 8, 87552–87561. doi: 10.1109/ACCESS.2020.2992649

CrossRef Full Text | Google Scholar

Xu, R., Chen, Y., Blasch, E., and Chen, G. (2018). “Blendcac: A blockchain-enabled decentralized capability-based access control for iots,” Proceedings. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree. New York, IEEE, 1027–1034.

Google Scholar

Yu, G., Zha, X., Wang, X., Ni, W., Yu, K., Yu, P., et al. (2020). Enabling attribute revocation for fine-grained access control in blockchain-IoT systems. IEEE Trans. Eng. Manag. 67, 1213–1230. doi: 10.1109/TEM.2020.2966643

CrossRef Full Text | Google Scholar

Yutaka, M., Zhang, Y., Sasabe, M., and Kasahara, S. (2019). “Using ethereum blockchain for distributed attribute-based access control in the internet of things,” in Proceedings 2019 IEEE Glob. Commun. Conf. GLOBECOM 2019. New York, IEEE.

Google Scholar

Zhang, Y., Li, B., Liu, B., Wu, J., Wang, Y., Yang, X., et al. (2020). An attribute-based collaborative access control scheme using blockchain for IoT devices. Electron. 9, 285. doi: 10.3390/electronics9020285