





Article

Blockchain-Based Secured Access Control in an IoT System

Sultan Algarni ¹, Fathy Eassa ², Khalid Almarhabi ^{3,*} , Abdullallah Almalaise ¹ , Emad Albassam ²,
Khalid Alsubhi ²  and Mohammad Yamin ⁴ 

- ¹ Department of Information System, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; saalgarni@kau.edu.sa (S.A.); aalmalaise@kau.edu.sa (A.A.)
- ² Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; feassa@kau.edu.sa (F.E.); ealbassam@kau.edu.sa (E.A.); kalsubhi@kau.edu.sa (K.A.)
- ³ Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University, Makkah 24381, Saudi Arabia
- ⁴ Department of Management Information Systems, Faculty of Economics and Administration, King Abdulaziz University, Jeddah 21589, Saudi Arabia; myamin@kau.edu.sa
- * Correspondence: kamarhabi@uqu.edu.sa

Abstract: The distributed nature of Internet of Things (IoT) and its rapid increase on a large scale raises many security and privacy issues. Access control is one of the major challenges currently addressed through centralized approaches that may rely on a third party and they are constrained by availability and scalability, which may result in a performance bottleneck. Therefore, this paper proposes a novel solution to manage the delivery of lightweight and decentralized secure access control of an IoT system based on a multi-agent system and a blockchain. The main objective of the proposed solution is to build Blockchain Managers (BCMs) for securing IoT access control, as well as allowing for secure communication between local IoT devices. Moreover, the solution also enables secure communication between IoT devices, fog nodes and cloud computing.

Keywords: access control; security; blockchain; Internet of Things; fog computing; cloud computing



Citation: Algarni, S.; Eassa, F.; Almarhabi, K.; Almalaise, A.; Albassam, E.; Alsubhi, K.; Yamin, M. Blockchain-Based Secured Access Control in an IoT System. *Appl. Sci.* **2021**, *11*, 1772. <https://doi.org/10.3390/app11041772>

Received: 24 December 2020
Accepted: 9 February 2021
Published: 17 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Internet of Things (IoT) is an extension of Internet power that allows different digital devices to connect to one another in order to send information back and forth. In other words, IoT is a system for connected computing devices. Each of these devices has a unique identifier and can communicate with other devices, which ultimately allows people and businesses to connect with each other and make meaningful strategic decisions.

IoT will not only lead to some revolutionary changes that improve the quality of human life but will also lead to many security challenges in relation to privacy, system configuration, information storage/management and access control, a situation that merits careful consideration [1]. Addressing security and privacy issues is one of the key challenges of IoT. Heterogeneity is also one of the major pillars of IoT that leads to security issues [2].

One of the key aspects of security and privacy issues in resource-constrained IoT devices is designing appropriate authentication and authorization solutions [3]. In this paper, we have proposed an architecture based on a multi-agent system and used a private distributed blockchain to manage the delivery of lightweight and decentralized IoT secure access control. The main objective of the proposed solution is to secure the entire IoT architecture, including communication between IoT devices, fog nodes and cloud computing.

The contributions of this paper can be summarized as follows:

- The primary contribution of this paper is to propose a novel blockchain-based architecture for securing an IoT system. The solution is based on decentralized access

control and uses a multi-agent system. The architecture adopts a private hierarchical blockchain structure to improve the security of the IoT system and to meet the requirements of resource-constrained IoT devices.

- Moreover, our proposed solution uses mobile agent software, which can play a significant role in the reduction of traffic overheads, exemplifying the high level of mobility and intelligence of our solution.
- We designed a generic, lightweight and scalable solution that can be applied to various IoT applications.

As opposed to other solutions, our approaches focus on ensuring the effective and efficient protection of each tier of IoT architecture via a private hierarchical blockchain structure and enable a significant reduction in traffic overheads via the adoption of a lightweight consensus mechanism based on IoT requirements (and using mobile agent software), the addition of mobility and intelligence (via mobile agent software) and the application of Mandatory Access Control (MAC), which is based on a hierarchical security level that works in line with our hierarchical blockchain in order to guarantee our multilevel security (MLS) policy.

The remainder of this paper is structured as follows: Section 2 discusses the existing access control system in IoT. Section 3 provides a brief overview of the blockchain and examines the use of blockchain technology in IoT. Section 4 presents a review of the relevant literature. The proposed architecture is explained in depth in Section 5. Finally, Section 6 concludes the paper and discusses future work.

2. Background of Access Control System in IoT

2.1. Access Control in IoT

Access Control (AC) involves the authentication and authorization of communication rights and resource access with respect to defined security guidelines and policies [4]. AC refers to the granting of permission to authenticated entities so that they can access the resources under predefined conditions.

Applying an optimal access control model to billions of IoT devices is a challenging task. Although authentication and authorization issues have been extensively studied in the literature, these issues in the IoT environment are still in their early stages. Access control List (ACL), Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are some of the most widely used access control mechanisms in IT infrastructure but are not fully appropriate for providing scalable, efficient and easily manageable applicability in an IoT environment [1].

In ACL, access control strategies are implemented in the cloud with better administration and tracking of activities but are constrained by a centralized infrastructure. As the number of IoT devices increases, the complexity of access rules also increases, resulting in confused duty problems. ACL lacks granularity and scalability and is very much prone to a single point of failure due to its centralized infrastructure [5].

The RBAC model provides a resource access authorization mechanism to users based on roles and defined principles, such as priorities, the separation of duties and administrative function partitioning, in order to define access policies for smart devices by capitalizing on the Web of Things (WoTs) approach [6]. These solutions do not fully meet the requirements of access control mechanisms and inter-device communication in a highly distributed network environment. The drawbacks associated with conventional access control models make them unsuitable for an IoT environment, which leads to the use of Capability-Based Access Control (CapAC) systems. To overcome the role explosion problem in RBAC, the ABAC model directly associates attributes with subjects. Access rights are granted based on the user attribute certificate [5]. As the number of IoT devices increases, the ABAC model's complexity increases and policy management becomes a critical issue [2].

A capability model is implemented for large-scale IoT-based systems. In this model, the capability list is associated with each subject, which defines its access rights to the target objects [7]. Despite its large-scale successful deployment, CapAC introduces several

challenges in relation to the propagation and revocation of access rights. Table 1 shows a comparative list of access control limitations in the IoT environment.

Table 1. Access control drawbacks with Internet of Things (IoT) environment.

Access Control Models	Limitations with IoT Environment
ACL	Lack of granularity and scalability. Prone to a single point of failure due to its centralized infrastructure.
RBAC and ABAC	Lack of complexity. Not supporting user-driven. Policy management becomes a critical issue.
CapAC	Propagation issue. Lack of context consideration.

2.2. Access Control Challenges in IoT

The main challenges of applying existing access control mechanisms in the IoT environment are as follows:

1. Reusability of existing solutions.

Access control mechanisms have been extensively studied in the literature and successfully deployed but these solutions cannot be applied directly to an IoT infrastructure, as they are complex and do not fit IoT requirements. Building a solution from scratch takes time to implement, deploy and adopt [1].

2. Centralized vs. distributed access control mechanisms

Centralized solutions provide control policies that are easily accessible but which possess a single point of failure. Centralized state-of-the-art security frameworks that are not suitable for the IoT environment are constrained by scalability issues [8]. In a centralized end-to-end mechanism, the user is not involved in the access control of their data. The distributed solution ensures privacy at a low cost and does not involve third-party trust. These distributed solutions are difficult to manage and require device-side access control policy updates.

3. Scalability

Interconnected devices are increasing at a significant speed, which, in turn, increases their management workload. A decentralized and distributed access control mechanism must provide scalability in order to accommodate the ever-growing number of homogeneous and heterogeneous IoT devices [9].

4. Heterogeneity

IoT infrastructure is distributed and incorporates multiple heterogeneous, interconnected devices with different underlying technologies, originating from multidisciplinary domains [1]. These technologies, under each domain, have different underlying authentication and authorization policies that make heterogeneity a major hindrance to providing a scalable, robust and secure IoT environment.

5. Resource constraints

IoT devices are bound by computation and storage capabilities and are connected via low-power and loss-prone networks. The access control system must provide an easy solution to address the abovementioned challenges within the resource constraints [10].

Consequently, the IoT environment required additional requirements to be considered in the access control mechanism, particularly distribution, scalability, heterogeneity and lightweight architecture.

3. The Use of Blockchain in IoT

A blockchain (a chain of linked blocks) is a distributed ledger with a list of linked data records or blocks, which are linked and secured by cryptographic hashes. Each block contains a set of new data records or transactions, as well as the hash value of the previous block, along with a timestamp that verifies the transactions at the time of the creation of the block, making the modification of records difficult, as they are dependent on prior records, as shown in Figure 1. Blockchain is characterized by the fact that data cannot be modified because they are copied and stored in a distributed and dependent manner [10].

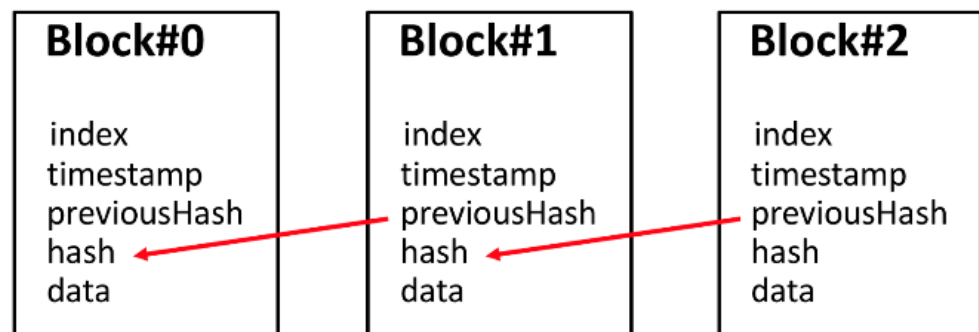


Figure 1. The components and basic architecture of the blockchain.

Blockchain is a highly transparent access control technology that provides end-to-end decentralized security and reduces the risk of human error. It provides solid protection against hacker attacks and can be of ultimate importance to access control systems. It was introduced in 2008 as a core framework of Bitcoin and it allows data to be recorded, stored and updated in a distributed way [11]. Blockchain is a decentralized approach that maintains the integrity of data by using a consensus mechanism. A third-party intermediary is not required and trust is developed through a public ledger stored in a decentralized manner in order to ensure secure distributed transactions in a trustless environment. The blockchain protocol is a potential candidate that may bring some evolutionary changes to traditional IT security technologies due to its decentralized infrastructure and anonymity maintenance [12].

Traditional security measures and access control mechanisms require a centralized trusted entity that ultimately compromises end-to-end security properties. Applying a centralized access control mechanism to an ever-growing number of IoT devices can complicate the process of trust management and affect the scalability of the system. Using blockchain can help the development of a fair authorization framework to address the abovementioned IoT access control challenges. The Ethereum blockchain is used to authenticate the server introduced by Auth0 [3] by using the challenge–response method. This model uses the decentralized approach of a blockchain but is also dependent on a third-party authentication server. This centralized infrastructure is one of the major drawbacks (single point of failure; single point of trust) of this method. Ourad et al. [3] proposed a blockchain-based IoT access control and secure authentication mechanism for users to connect securely to IoT devices by providing accountability (achieved through tamperproof records) and availability.

While a public blockchain brings numerous benefits, it is not suitable for resource-constrained IoT devices due to its high bandwidth overheads, delays and utilization of a large amount of computation resources [11]. Therefore, to address these challenges, our proposed solution uses a private blockchain, which provides light and decentralized IoT access control security.

4. Related Work

The related work in this paper can be classified into three main categories, with slight overlap between them: current security control solutions in IoT [1,2,5,13–26]; multi-agent systems for access control [27]; and blockchain-based access control for IoT [3,7–12].

Ouaddah et al. [1] presented a comprehensive review of the current access control solutions in IoT based on Objectives, Models, Architecture and Mechanisms (OM-AM). Moreover, the paper proposed a taxonomy based on the authors' comprehensive review. The paper analyzed the strengths and weaknesses of access control models and protocols regarding the IoT environment. Furthermore, they presented a decentralized access control framework called FairAccess [10] for IoT, based on a blockchain. The framework used the Pseudonymous technique to ensure the privacy of the users. They proposed a new type of transaction that is used to grant, obtain, delegate and revoke access based on access tokens. This is based on an Attribute-Based Access Control model. The authorization mechanism of FairAccess is based on authorization tokens, which provide access rights to a specific resource, identified based on its address and smart contract expressing its access control policies, to the requester or receiver. Nevertheless, this framework may cause a delay due to owner communication, authorization through tokenization only and terminating a token or requesting new access from the owner.

Novo [8] proposed scalable decentralized access management based on blockchain technology for IoT devices. The architecture excluded IoT devices from the blockchain network in order to overcome network overheads. The system has several advantages in relation to access control in IoT, namely mobility, accessibility, concurrency, lightweight architecture, scalability and transparency. This framework has managers that enable the registering of IoT devices and their verification. Even though this solution gains scalability as a result of distributing query permissions via management hubs, it could encounter security threats if the manager is malicious.

Dorri et al. [12] proposed a lightweight architecture for securing IoT using private blockchain technology. The proposed solution uses an access control list for ensuring authorization and their architecture encompasses three main models, namely smart homes, an overlay network and cloud storage. This solution stores the access control policies in the policy header of a local blockchain and does not use a Proof of Work (PoW) consensus to validate blocks as all IoT devices in the smart home tier are controlled by the miner. They argued that the overheads of the solution are insignificant compared to its security gains. However, the proposed architecture is a smart home application-based solution, which is not a generic solution and may not apply to other IoT domains. Moreover, this mechanism does not support self-enforced access control policies.

Almarhabi et al. [27] proposed a framework based on a multi-agent system for access control in the cloud and bring your own devices (BYODs) environments by addressing several security and privacy issues related to BYODs, such as the leakage of sensitive information and unauthorized policy changes. They proposed an architecture to address security and privacy issues by incorporating Mandatory Access Control policies in the cloud and BYOD environments delicately and securely with an independent platform.

Liu et al. [13] proposed an authentication and access control mechanism for an IoT infrastructure by establishing an ECC (Elliptic Curve Cryptosystem)—based security key and using an RBAC authorization method based on the user's role. The proposed solution is not scalable in an IoT environment due to the large number of users and the inability of RBAC to assign permission in advance. The proposed protocol requires frequent message exchanges and the security assessment is not strong. Ndibanje et al. [14] improved the efficiency at a minimal communication cost by incorporating secure session key establishment, maintaining user anonymity and mutual authentication. However, this solution is lacking in terms of its protection of the integrity of the transmitted messages.

Both role- and credential-based access control models cannot be directly applied to IoT due to their inherited disadvantages, as discussed before. However, using the strengths of these models and combining them with other models can overcome their

weaknesses. Moreover, Kaiwen et al. [15] proposed a hybrid role- and Attribute-Based Access Control model to target large-scale dynamic users by keeping policy integrity intact. They also proposed a mechanism to resolve policy conflicts and redundancy. Granting permissions and role management are still the responsibilities of the administrator in the proposed model.

Touati et al. [16] proposed an activity control mechanism (a generalized version of context-aware access control) by focusing on user and system preferences to grant or deny access. They used Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and a finite state machine for dynamic access policy adaptation. Touati et al. [17] also targeted the key/attribute revocation problem by proposing a Batch-Based CP-ABE method. The proposed mechanism does not require extra nodes for processing and reduces the overall complexity and overheads.

The Cap-BAC model is based on the least privileged principle for access service management. The service provider requires an authorization certificate from the user to give access to the required resources.

Sicari et al. [18] proposed a Unified Modeling Language (UML) conceptual model to define privacy policy definitions and data quality assessment in order to lay the foundation for the development of a secure and private IoT-based environment. Moreover, Goncalves et al. [19] proposed a secure architecture to establish and manage medical prescriptions in a mobility context by using Radio Frequency Identification (RFID) technology.

Gusmeroli et al. [20] proposed a capability-based approach to address IoT access control issues with low computation and storage capabilities, which requires lightweight secure control access policies. Moreover, Bernabe et al. [21] proposed a trust-aware lightweight access control mechanism to provide a reliable and secure link between connected devices in an IoT environment. They proposed a novel trust model based on the trust values accumulated from Quality of Service (QoS), security measures and reputation. As the identities of devices are not known in a distributed and decentralized IoT environment, this makes trust management a core issue to address.

Mahalle et al. [22] proposed an energy-efficient trust-based dynamic access control framework by capitalizing on the fuzzy approach to trust calculation from linguistic information gained from IoT devices. In Mandatory Access Control (MAC), an individual or a group with the authority to grant access rights to a resource grants access control. This is mostly implemented in government organizations and access is granted based on the sensitivity label associated with that particular resource.

Nippon Telegraph and Telephone (NTT) Innovation Institute [23] proposed a Mandatory Access Control mechanism for securing an IoT framework and hosting policy administration points by forcing unauthorized communications to shut down. They eased the administration of policies by incorporating attribute-based control policies.

Seitz et al. [24] proposed a distributed authorization framework by keeping the number of messages exchanged between resource-constrained devices to a minimum.

Naedele et al. [25] proposed a public key-based protocol to gain secure access and communication between embedded devices by specifying numerous authentication and access control policies. The proposed protocol requires frequent message exchange to make a secure connection and it does not conform to industry standards. The device's local condition and status are also not taken into consideration.

Zhang et al. [26] proposed a distributed privacy-preserving access control scheme specifically for sensor networks. It asks users to buy a token from the network owner and request the sensor data, which are delivered after the verification of the token. They use a distribution token reuse detection mechanism to avoid the reuse of tokens, which would enable unauthorized access. Their main work focused on privacy preservation and did not consider fine-grained access control policies for end devices. Table 2 shows the advantages and drawbacks of the related works.

Table 2. Summary of the advantages and drawbacks of the related works.

Reference	Advantages	Limitations
FairAccess [10]	The Pseudonymous technique is used to ensure the privacy of the users.	Produces possible delays due to owner communication as authorization occurs through tokenization.
Novo [8]	It utilizes managers, who are responsible for registering IoT devices and verifying them.	Even though this solution gains scalability as a result of distributing query permissions via management hubs, it could encounter security threats if the manager is malicious.
Dorri [12]	It does not use Proof of Work (PoW) consensus validation blocks as all IoT devices in the smart home tier are controlled via the miner. It is argued that the overheads of the solution are insignificant compared to its security gains.	The proposed architecture is smart home application based, not a generic solution and may not be well suited to other IoT use cases. Moreover, this mechanism does not support self-enforced access control policies.
Almarhabi [27]	The architecture addresses security and privacy issues by incorporating Mandatory Access Control policies in the cloud and BYOD environments delicately and securely with an independent platform.	It does not protect the integrity of the transmitted messages.
Liu [13]	The infrastructure established an ECC-based security key and uses the RBAC authorization method based on the user's role.	The solution is highly centralized and therefore is not well suited to the IoT environment due to the distributed nature of IoT networks. The protocol requires frequent message exchanges and its security assessment is weak.
Ndibanje [14]	It improved efficiency at a minimal communication cost by incorporating secure session key establishment, maintaining user anonymity and mutual authentication.	Role-Based Access Control and credential-based access control models cannot be directly applied to IoT due to their inherited disadvantages.
Kaiwen [15]	It uses hybrid Role-Based Access Control and Attribute-Based Access Control models to target large-scale dynamic users. It resolves policy conflicts and redundancy.	Granting permissions and role management is still the responsibility of the administrator in the proposed model.
Sicari [18]	It is based on a UML conceptual model to define privacy policy definitions and data quality assessment in order to lay the foundation for the development of a secure and private IoT-based environment.	The data integrity and security of the transmitted messages must be ensured.
NTT Innovation Institute [23]	It used a Mandatory Access Control mechanism for securing an IoT framework and hosting policy administration points by forcing unauthorized communications to be shut down. It eases the administration of policies by incorporating attribute-based control policies.	The integrity of transmitted messages is not fully protected.
Seitz [24]	It enables keeping the number of messages exchanged to a minimum between resource-constrained devices.	Transmitted messages are not fully protected (in terms of their integrity) against illegal modifications.
Zhang [26]	It requests users to purchase a token from the network owner in order request the sensor data, which are delivered after the verification of the token. It uses a distribution token reuse detection mechanism to avoid the reuse of tokens, which would enable unauthorized access.	The main work focused on privacy preservation and did not consider fine-grained access control policies for end devices.

Nevertheless, current security solutions are not fully suited to IoT due to the distributed nature of IoT networks and the limited resources of IoT devices. Traditional access control methods are costly in terms of their high power consumption and processing

overheads. Furthermore, public blockchains are not suitable for resource-constrained IoT devices, as they demand high computational power for mining processes.

Unlike traditional access control methods, our proposed architecture provides the following:

- Ensuring effective and efficient protection for each tier of the IoT architecture via a private hierarchical blockchain structure.
- Enabling a significant reduction in traffic overheads by adopting a lightweight consensus mechanism based on IoT requirements and using mobile agent software.
- Incorporating mobility and intelligence via mobile agent software.
- Applying MAC, which is based on a hierarchical security level, to work in line with our hierarchical blockchain architecture and guarantee MLS protection.
- Designing a generic, lightweight and scalable solution that can be applied to various IoT applications.

5. Proposed Solution

The proposed solution is based on a multi-agent system and uses a private blockchain, which provides lightweight and decentralized access control security for an IoT system. The proposed architecture is shown in Figure 2 and relies on a hierarchical blockchain structure, consisting of a Local Blockchain Manager (LBCM), which includes IoT devices at the bottom of our proposed architecture, a Fog Blockchain Manager (FBCM), which includes fog/edge nodes, a Core Fog Blockchain Manager (CFBCM), which includes core fog nodes and a Cloud Blockchain Manager (CBCM), which represents cloud blockchain storage. Each BCM has a block header, MAC policy header and transactions. Our framework meets the requirements of the CIA (Confidentiality, Integrity and Availability) security triad and is well-suited to the specific requirements of IoT in terms of its scalability, distributed nature, constrained devices and defense against various security issues, such as single points of failure. Finally, our proposed architecture is generalizable and can be applied to various IoT applications.

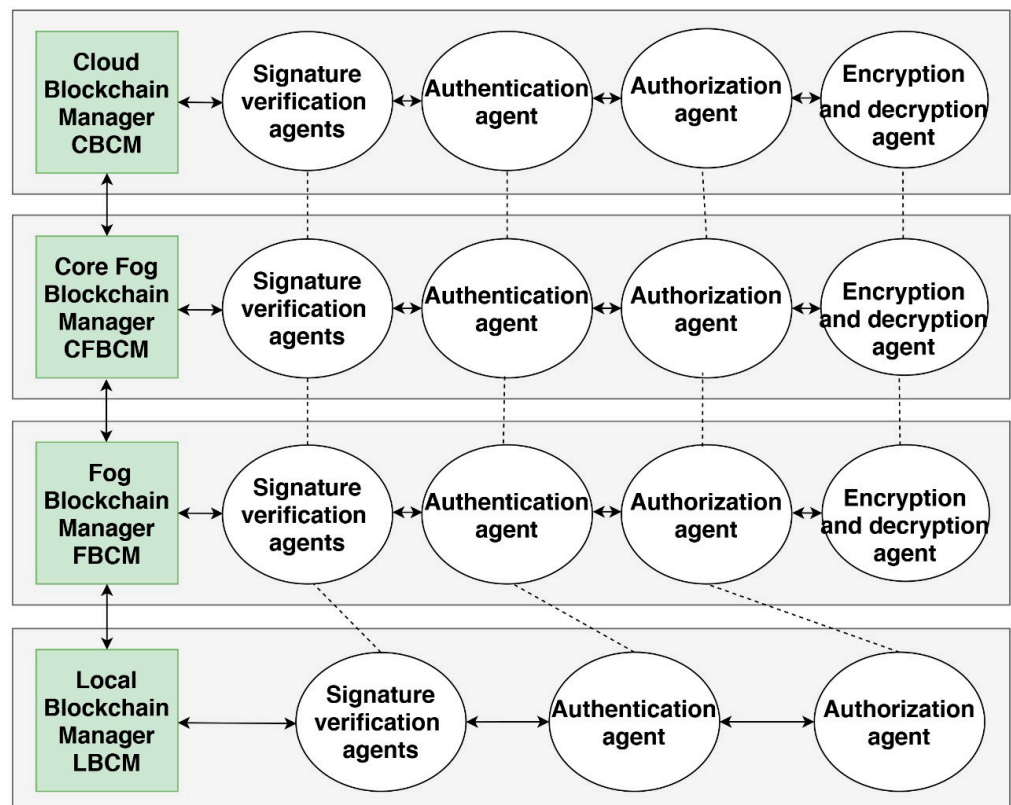


Figure 2. Proposed blockchain-based framework for secure Internet of Things (IoT) access control.

Taking into account the limited resources of IoT devices and the high computational overheads for solving cryptographic puzzles such as Proof of Stake (PoS), it is not straightforward to adopt blockchain technology in IoT devices. Regarding the miners in our proposed solution, each Blockchain Manager (BCM) is equipped with an online, high-resource device, identified as a miner, which is responsible for controlling all communications within and outside of each Blockchain Manager (BCM). Moreover, the BCM has the responsibility of removing or adding IoT devices and possesses a policy header, which is a MAC policy that enables the BCM to control all of the transactions inside each BCM and between BCMs. Furthermore, each Blockchain Manager (BCM) has the following mobile agents: Signature Verification Agent, Authentication Agent, Authorization Agent, Encryption and Decryption Agent. However, the Local Blockchain Manager (LBCM) does not contain an Encryption and Decryption Agent due to the existence of resource-constrained IoT devices, as encryption and decryption algorithms are computationally expensive, which would be unsuitable for the limited resources of IoT devices.

Regarding the applicable consensus mechanisms in our proposed solution, consensus mechanisms in public blockchains require costly mining methods, such as Proof of Work (PoW), which are not suitable for IoT networks for various reasons. For instance, public blockchains allow any nodes in the blockchain network to participate in the consensus process and transactions can be seen publicly, which is not desirable to many business blockchain solutions, as their sensitive data may be revealed and their privacy can be compromised. Moreover, public blockchains are vulnerable to the effects of a 51% attack. Hence, we use private (or permissioned) blockchains [28] to address the abovementioned challenges within IoT resource constraints and we use a lightweight consensus mechanism. In permissioned blockchains, the mining processes are managed via authenticated participants and are not open to the public. We will illustrate the main components of the proposed framework in the following sections.

5.1. Transactions

Communications among IoT devices, fog nodes, core fog nodes, and/or cloud computing are known as transactions. Transactions can be classified based on their specific functions, namely Access, Update, Add, Monitor and Remove. An Access transaction is created by BCMs to access data and is associated with granting read-only permission. Update transactions are created by devices/nodes to update stored data and are associated with granting read-and-write permission. BCMs can create Add, Remove, or/and Monitor transactions and BCMs have read/write permissions. Add transactions are used to add a new IoT device/node, while Remove transactions are used to remove them. Monitor transactions are used to monitor IoT devices/nodes' information and status.

5.2. MAC Policy

MAC stands for Mandatory Access Control and offers tighter security because only Blockchain Managers (BCM) can access or modify the access control policy, which can, in turn, reduce security errors. MAC is based on the security clearance of a subject (user), such as secret, top secret or confidential and an object's resource classification, such as secret, top secret or confidential. Clearance and classification data are stored in the security labels.

The determination of granting access to a request is based upon the clearance levels of subjects and the classification levels of objects. MAC policy is enforced by comparing the clearance of the subject to that of the object according to the Bell-LaPadula model, which is used for enforcing access control based on multilevel security policies [29]. Moreover, it focuses on maintaining data confidentiality and guarantees that users do not acquire access to resources above their security clearance, as shown in Figure 3.



Figure 3. Bell-LaPadula model.

5.3. Blockchain Managers (BCMs)

BCMs are the core of our proposed framework and they manage all communications in four layers: Local Blockchain Manager (LBCM), Fog Blockchain Manager (FBCM), Core Fog Blockchain Manager (CFBCM) and Cloud Blockchain Manager (CBCM). Furthermore, BCMs are responsible for setting the access control policy for each device/node in each layer. Each block in the blockchain comprises two headers: a block header and a policy header. The MAC policy is inserted into the block structure of each blockchain transaction. The BCMs have a policy header that allows them to control access permission for all transactions. Although all blocks in a blockchain have a policy header, the most updated one at the head of the block header in BCMs is used for checking and changing policies. The miner in the proposed solution is the BCM in each layer, which is the central security device responsible for authenticating, authorizing and auditing transactions. Moreover, when a block is added, BCMs create a pointer to the prior block, copy the policy in the prior block header to the new block and attach the block to the blockchain.

5.4. Software Agent

The proposed framework uses a software agent that can work effectively due to its mobility, adaptability, transparency, raggedness and self-starts and stops. Furthermore, the software agent can enable resource-constrained IoT devices to reduce costs and resources during coordination with other machines. The following subsections illustrate each software agent of the proposed framework.

5.4.1. Signature Verification Agent

This mobile agent is located in BCMs. The agent aims to ensure message integrity to guarantee that a message was sent by a known user and was not modified in transit and that it is not concerned with encrypted data. In LBCM, we are only concerned with ensuring that the data were not modified to ensure trust between IoT devices via symmetric key algorithms (shared secret keys). Therefore, we run a lightweight hashing function and verification agents, which are suitable for resource-constrained IoT devices.

For LBCM layer, each sender generates a hash value of the original message and assigns the sender's shared secret key to each message they send. The verification agent verifies the data in the LBCM layer by decrypting the message using the shared secret key and comparing the received hash value to the generated hash value.

However, as FBCM, CFBCM and CBCM have more computing power, these agents use digital signatures, as shown in Figure 4, which generates a hash value of the original message and assigns the sender's private key to each message they send. The verification agent verifies the data by decrypting the message using the sender's public key and comparing the received hash value to the generated hash value. If the values are equal, this means that the message has not been modified and the identity of the sender is confirmed.

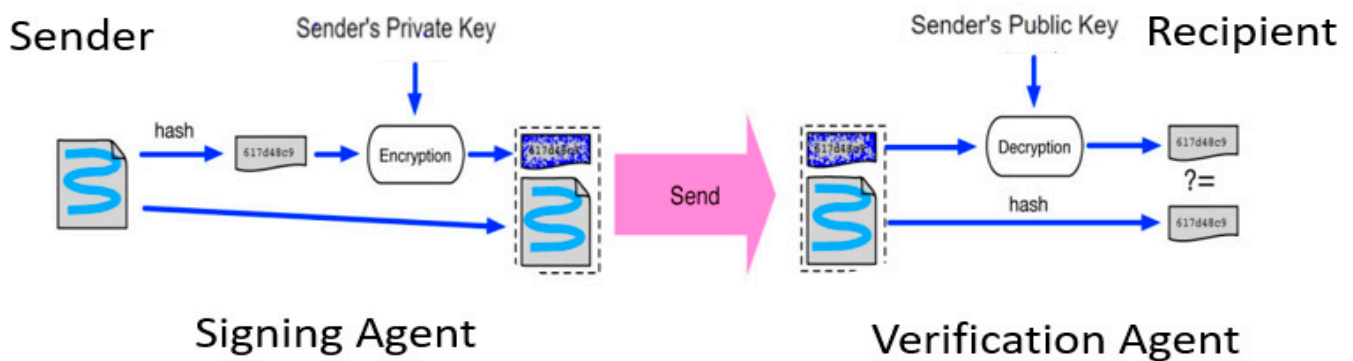


Figure 4. Signing Agent and Verification Agent for Fog Blockchain Manager (FBCM), Core Fog Blockchain Manager (CFBCM) and Cloud Blockchain Manager (CBCM).

5.4.2. Authentication Agent

This agent is responsible for ensuring that a user is valid and authenticated. Each device/node must share a secret key. Each BCM miner has an Authentication Agent, which ensures that a user is valid and authenticated. The Authentication Agent authenticates IoT devices/nodes based on a shared secret key, which is issued by the BCM miner in each layer. The shared secret key is based on the Diffie-Hellman key exchange algorithm, which enables the generation of a shared secret key between two parties that have not previously know each other over a non-secure channel in order to secure their communications [30].

When two IoT devices/nodes want to communicate with each other in the same layer, the agent first checks if they have the right shared key. However, if the IoT nodes are in different layers, the communication takes place between the BCMs in each layer using public key cryptography. If the agent does not approve their identities, then the communication is discarded. If the agent approves their identities, then they can communicate and move on to the next step, which is the Authorization Agent, to determine which resources can be accessed based on the MAC policy.

5.4.3. Authorization Agent

This agent is responsible for enforcing access control policies and granting permission rights to the requester based on its digital identity (ID) after authentication. It enables the BCM miner to determine exactly what IoT devices/nodes are allowed to do based on the MAC policy. Although the Authentication Agent approves the communication, this agent takes the ID of the connected party from the Authentication Agent. Then, it searches for user security clearance and resource classification based on the stored MAC policy in the BCM. The BCM miner uses the most updated MAC policy file based on the last block header. This agent implements the concept of the MAC policy, which includes the security classification level, to determine the type of permission (read; write). Furthermore, the Authentication Agent monitors the behavior of IoT devices/nodes and assigns a trust value for each IoT device/node. Moreover, it enforces the access control policy to determine which resource the users can access based on the Bell-LaPadula model.

5.4.4. Encryption and Decryption Agent

This mobile agent assures the confidentiality of data and guarantees that only approved users and agents can read and understand these data. This agent is located in FBCM, CFBCM and CBCM. While we assume that data confidentiality is not needed between IoT devices in LBCM, it is needed between any BCMs. The agent can encrypt and decrypt all access control policies and data transmitted between BCMs. This agent uses an asymmetric algorithm (public cryptography), which encrypts the message with the receiver's public key and the message can be decrypted by the receiver's private key.

A sequence diagram, as shown in Figure 5, illustrates the interaction between various software agents, specifically the Authentication Agent, Authorization Agent, resource and BCM for a user who requests a modification of the data in a resource. Now, we will illustrate how a user can modify data based on our framework. When the user wants to modify existing data, it sends a request to the Authentication Agent, which checks the identity of the user. In our case, the user has a secret shared key. The Authentication Agent checks the identity of the user and approves it, as it has a valid key and provides the user with an ID. Then, the user uses the provided ID and sends a request to the Authorization Agent, which implements the MAC mechanism. It checks the MAC policy for the user and the resource; in our case, the user is granted access, as the user can neither write nor read above or below its classification level. Then, the user directly sends a request to modify the data to the authorized resource and can only perform authorized actions based on the MAC policy. After the resource has been modified, it sends an updated transaction with an updated blockchain hash value to the LBCM. Finally, the LBCM sends an updated transaction to inform the Authorization Agent and update the blockchain hash value for the updated resource.

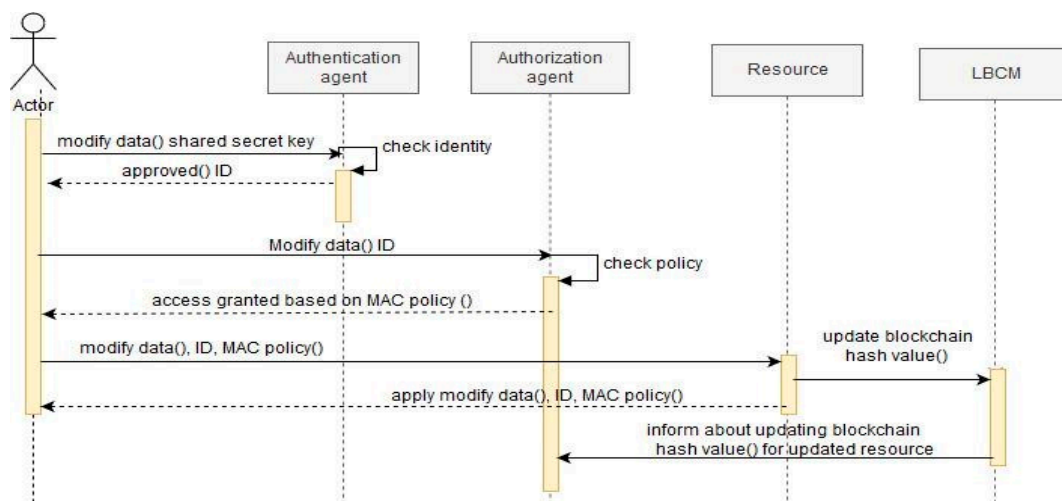


Figure 5. Sequence diagram for Authentication and Authorization Agents.

5.5. Results and Discussion

The result of this paper is that current security solutions are not fully suited to IoT due to the distributed nature of IoT networks and the limited resources of IoT devices. Traditional access control methods are costly in terms of their high power consumption and processing overheads. Furthermore, public blockchains are not suitable for resource-constrained IoT devices as they demand high computational power for mining processes. Therefore, there is a need to design distributed and lightweight secure access control for an IoT network. The paper's contribution is the proposal of a novel architecture based on a multi-agent system, which uses a private distributed blockchain, providing a lightweight architecture and decentralized access control security for the IoT system. The framework relies on a hierarchical blockchain structure and consists of a Local Blockchain Manager (LBCM), which includes IoT devices, a Fog Blockchain Manager (FBCM), which includes fog/edge nodes, a Core Fog Blockchain Manager (CFBCM), which includes core fog nodes and a Cloud Blockchain Manager (CBCM), which is a cloud computing node. Our framework meets the requirements of the CIA security triad and is well-suited to the specific requirements of IoT in terms of its scalability, distributed nature, constrained devices and defense against various security issues, such as single points of failure. The limitations will appear clearly after the implementation and testing of the proposed architecture. However, it may be deduced that they will involve performance and convenience issues. Finally,

the objectives of the proposed solution are achieved in the framework by enhancing the security of the access control mechanisms among IoT devices, as well as enabling secure communication between IoT devices, fog nodes and cloud computing.

The Internet of Things has many uses. Such uses are still increasing and a promising future for the Internet of Things is expected. With this increase, however, there have been cases and incidents that have revealed the weaknesses of the Internet of Things and the extent of its threat to users' rights and freedoms [31]. It is imperative to develop technologies and solutions that reduce these effects and allow users to benefit from the advantages of the IoT. One of the most widespread examples of the Internet of Things is smart home devices, which may be the next arena for attacking and influencing individuals [32]. An attacker could take control of the victim's home and enter it by remotely opening the front door or opening windows and damaging the home devices. Cameras can be hacked, access to sensitive data and household appliances can be controlled and destroyed or fires can threaten residents. This type of attack poses a new threat to smart home device users. The risks in smart homes fall into five classes: technical vulnerabilities, user data risk, a lack of encryption, privacy issues and increased complexity of the system [33]. On October of 2016, in one of the worst breaches, Mirai botnet attacked IoT, which affected the control of the world's Domain Name Server (DNS) infrastructure. As a result, many IoT devices, such as DVR players and digital cameras as well as many websites including Netflix and CNN, were affected and turned off. The attacker used default authentication data to log in to victims' IoT devices. The estimated number of targeted devices was approximately 100,000 [34].

In our proposed solution, we provide different levels of blockchain managers that manage the IoT's entire system. In the case of smart homes, the Local BlockChain Manager (LBCM) works as a miner. It is installed in the home hubs or on a personal computer and is directly connected to and manages the IoT devices located in a smart home, such as smart TVs, lights and refrigerator devices. Each smart home has various IoT devices managed via LBCM. A group of neighboring smart homes or a specific smart home owned by someone can be managed and connected to each other by Fog BlockChain Manager (FBCM) through LBCM. Core Fog BlockChain Manager (CFBCM) can manage different groups of FBCMs in a wide area such as a city to increase scalability and for security purposes. Finally, these groups of CFBCMs are connected to different Cloud BlockChain Managers (CBCM) so that data can be stored and retrieved. The communication only takes place between BCMS. All these managers perform as discussed in Section 5. Appropriate measures such as these must be taken to make smart homes safer and more livable.

Smart home devices are a potential target of various security attacks due to the availability of data and communication resources. Tampering and malicious code are some of the common cyber-attack challenges for smart home devices. In these attacks, they refer to a piece of software designed intentionally to inflict serious damage to a targeted device to modify data and breach the integrity of the system. The primary target of the attacker, after scanning the network of smart home, is to gain access to these devices and maintain access to compromise the whole system. When attackers tamper with a smart home system by adding a code or function on IoT devices to access and modify sensitive data, it leads to system reliability being compromised. If our research proposal faces this kind of attack, it will not function in some parts of the framework. In the proposed solution, firstly, an authentication agent can distinguish between authorized and unauthorized access. Secondly, the authorization agent is applied to the MAC policy, which limits the access and searches for the security classification label. In addition, the compartmentalization approach is applied. Finally, the signature verification agent ensures the reliability against the change of data which leads to maintaining the integrity and safety of the system.

Distributed Denial of Service (DDoS) attack is one of the most threatening security challenges for the IoT environment. In a DDoS attack, the attackers overwhelm a target network resource with a large volume of fake requests to make the resource or service unavailable for legitimate users. In the context of IoT environment, the DDoS attack can be

launched by malicious smart home devices that flood the LBCM with a large number of fake transactions. Our proposed solution is based on a hierarchical security level which can reduce the possibility of DDoS attacks. As a result, malicious devices will not be able to access the LBCM, as each smart home device needs to be authenticated before communicating with the LBCM. The Authentication Agent ensures that each smart home device has a valid shared secret key. Let us suppose that an adversary compromised smart home devices. The next level of security can prevent this attack, which is based on a multilevel security (MLS) policy in the Bell-LaPadula model. The Authorization Agent applies a security classification level for each smart home device which limits the access of each smart home device. In the worst case, let us suppose that the attacker gains access to smart home devices, gains access and starts sending unnecessary transactions to overwhelm the LBCM. In such an event, the Authorization Agent would assign a trust value to each smart home device and update them periodically. This trust value is based on the behavior of smart home devices and as a result, the compromised devices would be blocked when the attackers conduct malicious activities such as unnecessary transactions to the LBCM.

6. Conclusions and Future Works

The issues related to the security and privacy of the IoT system are immense and require careful consideration. There are some pros and cons to both centralized and decentralized solutions. Centralized solutions are constrained by scalability, while decentralized approaches are bound by delays, computational overheads and energy constraints. We proposed a multi-agent system to provide lightweight, decentralized IoT access control security mechanisms. Blockchain Managers (BCMs) are responsible for providing the necessary security for access control, securing communication between local IoT devices, fog nodes, core fog nodes and cloud computing.

The proposed architecture is a generalizable solution that can be applied to various IoT applications. Furthermore, IoT's issues are not fully addressed in prior studies, as most studies focus on addressing access control issues in a specific IoT application such as a smart home.

The authors understand that research evaluation is must be based on implementation and testing phases that specify the solution's applicability and effectiveness compared to related research. However, this research is still in progress and the authors believe that the results of these two phases should be published in a separate paper due to the expectation that a great number of details will need to be discussed, as well as new contributions.

In future research, the proposed framework will be implemented in a real environment to measure the achievement of the fundamental security goals in relation to integrity by applying the digital signature, authentication via shared secret keys, authorization via the MAC policy and confidentiality via public key encryption.

We will examine various solutions to solve the big header size problem in the blockchain. A possible solution is to separate the header block access control policy from the block structure in the blockchain and place the access control policy in a separate policy file blockchain or in a separate encrypted text file. The proposed architecture will be enhanced in this domain and we will apply a case study for IoT applications that requires a high level of security. The RaspberryPI IoT device will be used for the deployment of the solution and we will use a private blockchain platform in its deployment. Further details will be included in future works.

Author Contributions: Conceptualization, S.A., F.E. and K.A. (Khalid Almarhabi); methodology, S.A.; validation, K.A. (Khalid Almarhabi), F.E. and M.Y.; writing—original draft preparation, S.A. and K.A. (Khalid Almarhabi); writing—review and editing, M.Y.; supervision, F.E.; project administration, F.E. and A.A.; funding acquisition, A.A., E.A. and K.A. (Khalid Alsubhi) All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. (RG-18-611-38). The authors, therefore, gratefully acknowledge the DSR technical and financial support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. *Comput. Netw.* **2017**, *112*, 237–262. [[CrossRef](#)]
2. Aldowah, H.; Rehman, S.U.; Umar, I. Security in Internet of Things: Issues, Challenges and Solutions. In *International Conference of Reliable Information and Communication Technology*; Springer: Cham, Switzerland, 2018; pp. 396–405.
3. Ourad, A.Z.; Belgacem, B.; Salah, K. Using blockchain for IOT access control and authentication management. In *International Conference on Internet of Things 2018 June*; Springer: Cham, Switzerland, 2018; pp. 150–164.
4. Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. *J. Netw. Comput. Appl.* **2019**, *144*, 79–101. [[CrossRef](#)]
5. Ouaddah, A.; Mousannif, H.; Ouahman, A.A. Access control models in IoT: 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.
6. Jia, J.; Qiu, X.; Cheng, C. Access control method for web of things based on role and SNS. In Proceedings of the 2012 IEEE 12th International Conference on Computer and Information Technology, Chengdu, China, 27–29 October 2012; pp. 316–321. [[CrossRef](#)]
7. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1027–1034. [[CrossRef](#)]
8. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [[CrossRef](#)]
9. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in Internet of Things: Challenges and Solutions. *Yingyong Kexue Xuebao/J. Appl. Sci.* **2020**, *38*, 22–33. [[CrossRef](#)]
10. Gao, W.; Hatcher, W.G.; Yu, W. A survey of blockchain: Techniques, applications, and challenges. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018. [[CrossRef](#)]
11. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623. [[CrossRef](#)]
12. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*; Springer: Cham, Switzerland, 2017; pp. 523–533. [[CrossRef](#)]
13. Liu, J.; Xiao, Y.; Chen, C.L.P. Authentication and access control in the Internet of things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592. [[CrossRef](#)]
14. Ndibanje, B.; Lee, H.J.; Lee, S.G. Security analysis and improvements of authentication and access control in the internet of things. *Sensors* **2014**, *14*, 14786–14805. [[CrossRef](#)] [[PubMed](#)]
15. Kaiwen, S.; Lihua, Y. Attribute-role-based hybrid access control in the internet of things. In *Asia-Pacific Web Conference*; Springer: Cham, Switzerland, 2014; Volume 8710, pp. 333–343. [[CrossRef](#)]
16. Touati, L.; Challal, Y. Poster: Activity-based access control for IoT. In Proceedings of the 1st International Workshop on Experiences with the Design and Implementation of Smart Objects, Paris, France, 7–11 September 2015; pp. 29–30. [[CrossRef](#)]
17. Touati, L.; Challal, Y. Batch-based CP-ABE with attribute revocation mechanism for the Internet of Things. In Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 16–19 February 2015; pp. 1044–1049. [[CrossRef](#)]
18. Sicari, S.; Rizzardi, A.; Coen-Porisini, A.; Cappiello, C. A NFP model for internet of things applications. In Proceedings of the 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Larnaca, Cyprus, 8–10 October 2014; pp. 265–272. [[CrossRef](#)]
19. Goncalves, F.; Macedo, J.; Nicolau, M.J.; Santos, A. Security Architecture for Mobile E-Health Applications in Medication Control. In Proceedings of the 2013 21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2013), Primosten, Croatia, 18–20 September 2013.
20. Gusmeroli, S.; Piccione, S.; Rotondi, D. IoT Access Control Issues: A Capability Based Approach. In Proceedings of the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Palermo, Italy, 4–6 July 2012; pp. 787–792. [[CrossRef](#)]
21. Bernabe, J.B.; Ramos, J.L.H.; Gomez, A.F.S. TACIoT: Multidimensional trust-aware access control system for the Internet of Things. *Soft Comput.* **2016**, *20*, 1763–1779. [[CrossRef](#)]

22. Mahalle, P.N.; Thakre, P.A.; Prasad, N.R.; Prasad, R. A fuzzy approach to trust based access control in internet of things. In Proceedings of the Wireless VITAE 2013, Atlantic City, NJ, USA, 24–27 June 2013; pp. 1–5. [CrossRef]
23. NTT Innovation Institute. Mandatory Access Control over IoT Communications. Available online: https://labevent.ecl.ntt.co.jp/forum2017/elements/pdf_eng/03/C-18_e.pdf (accessed on 16 November 2020).
24. Seitz, L.; Selander, G.; Gehrmann, C. Authorization framework for the Internet-of-Things. In Proceedings of the 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Madrid, Spain, 4–7 June 2013. [CrossRef]
25. Naedele, M. An access control protocol for embedded devices. In Proceedings of the 2006 4th IEEE International Conference on Industrial Informatics, Singapore, 16–18 August 2006; pp. 565–569. [CrossRef]
26. Zhang, R.; Zhang, Y.; Ren, K. Distributed privacy-preserving access control in sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1427–1438. [CrossRef]
27. Almarhabi, K.; Jambi, K.; Eassa, F.; Batarfi, O. An evaluation of the proposed framework for access control in the cloud and BYOD environment. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 213–221. [CrossRef]
28. Zheng, Z.; Xie, S.; Dai, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
29. Sahafizadeh, E.; Parsa, S. Survey on access control models. In Proceedings of the 2010 2nd International Conference on Future Computer and Communication, Wuha, China, 21–24 May 2010; Volume 1, pp. 1–3. [CrossRef]
30. Li, N. Research on Diffie-Hellman key exchange protocol. In Proceedings of the 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 16–18 April 2010; Volume 4, pp. 634–637. [CrossRef]
31. Narendra, M. Research Reveals the Most Vulnerable IoT Devices. Available online: <https://gdpr.report/news/2019/06/12/research-reveals-the-most-vulnerable-iot-devices/> (accessed on 11 January 2021).
32. Denning, T.; Kohno, T.; Levy, H.M. Computer security and the modern home. *Commun. ACM* **2013**, *56*, 94–103. [CrossRef]
33. Vojković, G.; Milenković, M.; Katulić, T. IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. *Bus. Syst. Res. Int. J. Soc. Adv. Innov. Res. Econ.* **2020**, *11*, 167–185. [CrossRef]
34. Cvitić, I.; Peraković, D.; Periša, M.; Botica, M. Smart home IoT traffic characteristics as a basis for DDoS traffic detection. In Proceedings of the 3rd EAI International Conference on Management of Manufacturing Systems 2018, Dubrovnik, Croatia, 6–8 November 2018.