cryptography

MDPI

Article

Enhanced Authentication for Decentralized IoT Access Control Architecture

Jeong Hwa Kang and Minhye Seo *

Department of Cyber Security, Duksung Women's University, Seoul 01369, Republic of Korea; jhk5242@duksung.ac.kr
* Correspondence: mhseo@duksung.ac.kr

Abstract: The internet of things (IoT) enables a hyperconnected society, offering intelligent services and convenience through various connections between people, objects, and services. However, the current state of the IoT still faces limitations in security. Security issues in the IoT are of significant concern, leading to the proposal of numerous security frameworks and solutions to address these challenges. Authentication and authorization are crucial security requirements in the IoT environment, considering the potential risks posed by inadequate authentication and incorrect authorization. To comprehensively mitigate these issues, we presents a novel IoT access control architecture in this paper. The proposed architecture leverages the OAuth framework for authorization and the decentralized identity technology to enhance the authentication and authorization processes.

Keywords: internet of things (IoT); authentication; authorization management; blockchain; decentralized identity (DID)

1. Introduction

The internet of things (IoT) is a revolutionary technology that enables the connection of physical objects to the internet, bridging the gap between software services and the physical world. It has become an integral part of various industries and businesses, playing a significant role in the fourth industrial revolution. The IoT offers a wide range of capabilities, including detection, identification, information processing, and connectivity, across diverse fields such as healthcare, transportation, industry, agriculture, and urban infrastructure [1]. During the COVID-19 pandemic, the IoT played a crucial role in the healthcare industry. It was utilized for patient investigation and data aggregation, remote monitoring, body temperature measurement, and monitoring quarantine compliance, contributing to the management of the pandemic. The applications of the IoT continue to expand rapidly, encompassing areas such as healthcare, guidance and control systems, trade, and industrial automation [2].

However, the security considerations for IoT deployments have been insufficient, leading to various security threats and incidents as the use of the IoT continues to grow. The IoT operates across three main layers, each susceptible to different types of attacks. At the perception layer, attacks such as denial-of-service (DoS), distributed DoS (DDoS), replay attacks, side-channel attacks, and fake node attacks can occur. In the network layer, attacks such as man-in-the-middle (MITM), DoS, eavesdropping, sniffing, and routing attacks are possible, which can impact data authentication, accessibility, privacy, and application layer efficiency [3]. As such, security threats can appear throughout the framework, from communications among devices to the process of processing and storing data. To address these security threats, IoT architecture incorporates various security requirements. Among these requirements, authentication and authorization are considered fundamental and critical in all layers to prevent a range of attacks [4]. Consequently, solutions that integrate different frameworks have been proposed to enhance authentication, authorization, and access control mechanisms between IoT devices and users.

check for updates

Citation: Kang, J.H.; Seo, M. Enhanced Authentication for Decentralized IoT Access Control Architecture. *Cryptography* **2023**, *7*, 42. https://doi.org/10.3390/cryptography7030042

Academic Editor: Carlo Blundo

Received: 19 June 2023
Revised: 7 August 2023
Accepted: 16 August 2023
Published: 21 August 2023

Various methods have been proposed to authenticate and authorize legitimate users or devices in the IoT environment to ensure effective access control. OAuth, an open standard framework for authorization widely used on the web, has been employed in several studies for authorization delegation in IoT scenarios. IoT-OAuth has demonstrated efficient management of authorization through the use of centralized servers and tokens issued by them. However, the centralized server presents a potential single point of failure susceptible to various security threats. To mitigate this risk, numerous studies have explored the replacement of centralized authorization servers with decentralized systems.

Granting privileges to unauthorized parties within access control mechanisms can create security vulnerabilities, making it crucial to only delegate access to legitimate users and ensure the validity of authentication methods. In the realm of access control management, authentication should be meticulously implemented. Treating authentication as a mere assumption for authorization can lead to significant risks. Therefore, we emphasize the significance of authenticating all entities involved in the framework, alongside the access control mechanisms for authorization. To accomplish this, we adopt a validated authentication method called decentralized identity (DID), which utilizes blockchain technology to ensure integrity and immutability. Moreover, we employ a secure token called the proof of possession (PoP) token to establish ownership and mitigate attacks such as eavesdropping and theft on the network.

1.1. Contributions

In this paper, we propose an IoT authorization management framework based on blockchain and OAuth. The proposed framework utilizes OAuth for authorization, leveraging a decentralized blockchain instead of a centralized server. We also present enhanced authentication as well as authorization delegation by adopting a decentralized (or distributed) identity (DID) system.

The primary contributions of this research are as follows:

- A blockchain-based decentralized OAuth authorization system is presented to address issues with centralized servers.
- Smart contracts on the blockchain are used for automated authentication and authorization performance management.
- A DID system is used to provide strong authentication for all participants involved in access control management.
- By implementing a secure token called the PoP token, proof of user ownership is achieved, which mitigates security threats.

1.2. Organization

The remainder of this paper is organized as follows. In Section 2, we review and compare existing studies on IoT authorization and authentication. Section 3 provides the necessary background knowledge and technology required to comprehend the proposed architecture. Our proposed architecture is presented in detail in Section 4. Section 5 further examines and compares this study, focusing on the underlying techniques. Lastly, Section 6 concludes the paper.

2. Related Work

Various authentication methods, authorization management, framework, and flow have been studied to authenticate and authorize IoT devices which want to access resource, and users (or clients) who want to access IoT devices. We compared related works based on four key technologies: decentralized authentication, smart contracts, secure tokens, and distributed identifiers (DID).

The conventional authentication methods and OAuth perform authentication through a centralized authorization server. This approach offers the advantages of fast and systematic authentication processing through a single authentication server. However, it also presents a critical drawback, where a single point of attack can lead to homogenized

vulnerabilities, and the failure of the server due to attacks or errors can result in the paralysis of the entire authentication system. On the other hand, decentralized authorization disperses the authentication server without centralizing it. This helps to alleviate the critical shortcomings of a centralized server. Moreover, the characteristics of distributed ledgers ensure the integrity and immutability of authentication data, enhancing security measures.

Smart contracts, powered by blockchain technology, enable system automation. They offer the advantage of an automated authentication mechanism, which helps prevent interference from attackers or malicious insiders.

DID (decentralized identifier) serves as a distributed identity management system, utilizing blockchain as the foundation for identity management. Unlike conventional identity management systems, DID enables individuals to manage their identifiers and ensures the integrity of these identifiers through the use of a distributed ledger. Such features of DID offer the advantage of mitigating identifier tampering issues present in traditional identity management models.

A secure token is an enhanced version of the traditional access token, designed to strengthen security and mitigate token-related vulnerabilities at the network layer. The PoP (proof of possession) token, utilized as a secure token, validates the token owner using the PoP key, ensuring that the token is being used by legitimate users.

Access control is a crucial element in security, and numerous access control frameworks have been researched to enhance security. Among them, role-based access control (RBAC) has been widely used and extensively studied. Sandhu et al. proposed a family of RBAC models based on role hierarchies and constraints [5]. Additionally, Sandhu et al. introduced the NIST RBAC, which integrates RBAC, hierarchical RBAC, constrained RBAC, and symmetric RBAC [6]. Furthermore, Giordano et al. proposed Vicoms, an applicable access control framework for real-world applications [7]. Vicoms implements access restrictions by specifying policies in JEE server environments using the XACML language, designed for enhancing security in access control frameworks. In [8], Zhang et al. further explained how to effectively verify access control frameworks and policies using XACML as used in [7]. Thomas et al. proposed a new approach to access control called task-based authorization controls, which is different from the traditional role-based and policy-based methods [9]. Task-based authorization controls grant permissions at various points during the progression of tasks from a task-oriented perspective. Heydon et al. explain that these tasks are described using easily understandable visual manipulation languages [10]. These studies describe classical access control methods, followed by the development of applicable new access control approaches, and visual manipulation languages that facilitate easy comprehension. Based on these studies, we can understand the advancements and apply them to the framework we intend to propose.

OAuth is an authorization framework which delegates access using tokens. Therefore, studies using OAuth have been proposed to authenticate and authorize users and IoT devices. Kahn et al. [11] presented an IoT authentication protocol using OAuth, and Savio et al. [12] proposed an OAuth-IoT framework for flexible authentication and authorization of IoT devices using OAuth 2.0. The framework proposed an IoT resource access control mechanism and describes the mechanisms on constrained IoT devices. Federico et al. [13] also introduce an IoT access control architecture using OAuth 2.0. The as-a-service access control architecture introduced in [13] has an identity provider for authentication and delegation of authority. Oh et al. [14], who proposed an IoT access control framework based on expanded OAuth 2.0 and Role, controlled access by limiting the scope of authority based on Role, similar to [13]. Oh et al. [15] used OAuth for authorization, not only for users but also for devices in heterogeneous domains. However, since all of those [11–15] who designed IoT access control management based on OAuth using centralized servers to manage authorization and set scope for permissions, there are limitations to threats caused by centralized servers such as DDoS, DoS, insider attacks, and data forgery problems.

In order to solve the problem caused by using the centralized server, studies have been presented to solve the problem by replacing the centralized server with a distributed ledger. Qian et al. [16] proposed data security management through device authentication excluding third parties and recording data in distributed ledgers using blockchain distributed ledgers. As the distributed ledger and its functions developed, smart contracts that automatically record and verify transactions were used in various blockchain systems and were also introduced in blockchain-based IoT authentication and access control management frameworks. Li et al. [17] gave each IoT a unique ID and recorded it in a distributed ledger to explain a framework that can authenticate and authorize IoT through smart contracts, and similarly, Gong et al. [18] created and authenticated device fingerprints for device authentication inside the blockchain. Subsequently, Ferreira et al. [19] used a blockchain to identify, register, and authenticate IoT devices, and developed an API for the blockchain. Furthermore, Tahir et al. [20] described a framework for accessing data by performing authentication and authorization of fog IoT data on the blockchain through smart contracts based on certificates and keys granted to each user. Ayoade et al. [21] also proposed an IoT smart contract architecture that serves as an authorization for information stored safely in TEE storage by recording and tracking access from third parties in a distributed ledger through smart contracts. In addition, a system that provides interaction in a secure and distributed manner by applying blockchain algorithms to IoT has also been proposed [22]. Blockchain uses hash operations to provide strong integrity and immutability, but IoT access management frameworks that have replaced the permission server with the proposed blockchain must go through authentication and authorization procedures each time and perform operations to record in a distributed ledger. Above all, there is a disadvantage that it is difficult to verify access rights in a resource server if there is a separate resource server that stores the user's data from the authorization blockchain.

To simplify the problem of inconvenient user authorization by specifying authorization, an authorized tokens or tickets may be issued [4]. A framework can be designed that provides authorization to improve the weakness of a distributed ledger by borrowing the previously proposed token technology of OAuth. Therefore, several studies have published designs and architectures that overcome the limitations of the two technologies by delegating OAuth's authority and decentralizing the (centralized) servers. Ourad et al. [23] proposed a blockchain-based OAuth solution that enables authentication and secure communication for IoT devices, and Siris et al. [24,25] use an authorization server to authorize requests, but it is recorded in the blockchain to ensure integrity and traceability, and can be applied in practice. Subsequently, research was also conducted to verify IoT devices through smart contracts with blockchain-based OAuth by completely replacing the authorization servers with a blockchain-based OAuth, and to issue authorization tokens [26]. In addition, an authorization architecture also has been proposed that allows contextual flexibility in providing access to resource [27], using context-aware security services that can determine detailed authority such as roles, as shown in [14].

Most works have mainly proposed management, frameworks, and architectures that delegate authorization through authentication, that is, control access. Therefore, authentication was treated as an assumption, or the authentication method (certificates, public keys, etc.) of parties such as users and IoT devices were not significantly defined. That is, many parts of the enrollment process for authentication in the framework, which is important in delegation of authority, are omitted or passed over. However, the assumption of authentication is a very strong assumption because it is very important to verify whether it is a legitimate party or a legitimate authentication method, and false authentication can pose a threat to empowering the non-legitimate party. Therefore, in this paper, we propose an authorization framework using smart contracts based on OAuth and blockchain and authentication of parties with DIDs guaranteed integrity and immutability as an authentication method.

DID is an identity management technology that enables verification of forgery by storing documents including authentication methods such as public keys and certificates

in a distributed storage. Several studies have been presented that have adopted authentication using DIDs with guaranteed integrity and legitimacy of the authentication methods. Fotiou, Nikos et al. [28] adopted DID for guests' IoT access permission and performed authentication and authorization. This paper proposes granting access to IoT devices by utilizing DID for authentication in multi-tenant IoT hubs. An OAuth-based study using verifiable credentials (VC), that add personal identification to DIDs for user authentication and IoT access, has also been conducted [29]. In this framework, the issuer issued the VC, and authentication and authorization were performed in the AS using the VC's certification. Subsequently, Dixit et al. [30] proposed a device-to-device connection framework for IoT in the industry through SSI authentication based on DID and VC.

However, most studies using DID for authentication rely on centralized authorization servers, which share the limitations that come from centralized servers, as shown in [11–15]. Therefore, we would like to propose an OAuth-based DID certification and blockchain access control management framework that compensates for the shortcomings of each technology that has not yet been proposed. Table 1 summarizes the comparison of the tasks examined for IoT authentication and access control management.

Table 1. Comparison of IoT access control architecture tasks.

	Decentralized Authorization	**Smart Contract**	**Secure Token**	**DID Authentication**
[5–9]	N	N	N	N
[11–15]	N	N	Y	N
[16]	Y	N	N	N
[17–23]	Y	Y	N	N
[24,25]	N	Y	Y	N
[26,27]	Y	Y	Y	N
[28]	N	N	N	Y
[29]	N	N	Y	Y
[30]	N	Y	N	Y
Ours	**Y**	**Y**	**Y**	**Y**

3. Background

3.1. IoT

The IoT is a ubiquitous sensor internet connection system proposed by Kevin Ashton in 1999, short for internet of things. The IoT can be simply defined as a variety of objects connected to internet networks. Objects have embedded communication functions and wirelessly transmit and receive information obtained through sensors or computers [31]. All objects and structures with embedded sensors and communication functions are IoT, and various embedded objects can be IoT devices, from simple sensor equipment to home appliances such as smart refrigerators and smart TVs, mobile equipment such as smartphones and Wi-Fi, and wearable equipment such as smartwatches.

The network formed by connecting various IoT devices that wirelessly transmit and receive information and apply it according to their purpose is called an IoT network, and IoT networks are also growing with the development of the internet. These open and comprehensive IoT networks can share information, data, and resources, and respond and act according to changes in contexts and environments [32].

3.2. Blockchain

Blockchain is a distributed computing ledger technology that provides data integrity and immutability. The nodes of the blockchain environment have a distributed ledger, and transaction data that has undergone a consensus process at the blockchain node is recorded in the distributed ledger as a 'block' and cannot be modified or changed. Blockchain guarantees integrity and immutability through a hash function, and links blocks into chains. The block constituting the blockchain is a set of data stored in the ledger and consists of

a block header and block data. The block header includes a hash of the previous block header, a time stamp, a nonce, and a hash of the entire block, and the block data includes a list of transactions [33]. The blockchain is recorded in a distributed ledger through a block header connected to the previous block in the form of a chain.

Blockchain is decentralized technology, that is because the blockchain uses the P2P method and all nodes propagate recorded transactions with a distributed ledger, and decentralization is one of the strong attributes that can solve the problem of centralized servers [34]. Blockchain provides integrity, immutability, and decentralization, making it impossible to falsify data, and enabling safe transactions and data processing without using intermediaries or trust agencies. Therefore, blockchain is used as a key technology in cryptocurrency, finance, medical care, SNS, and identity verification systems.

Smart Contract

The technology proposed with the development of blockchain is a technology that programs the contents of the contract and embeds the contract in the blockchain to automatically execute it when the contract conditions are met, proposed by Nick Szabo in 1994 and applied by Vitalik Buterin in 2015 simultaneously with the development of Ethereum [35]. Smart contracts allow developers to write their own contract contents and conditions and can implement any contract based on such programmed contracts. In addition, smart contracts are very efficient because they automatically sign contracts and record transactions when conditions are met, and have the advantage of minimizing the risk of third-party intervention and exceptions [36]. Therefore, signing transactions through smart contracts that execute on the blockchain and recording transactions on the blockchain can ensure stronger integrity and immutability. Smart contracts with these advantages are used for various financial, real estate, insurance transactions, digital rights management, and notarization [37].

3.3. OAuth

OAuth is open authorization, commonly referred to as OAuth 2.0 authorization framework technology. OAuth is an open standard technology that delegates access to limited user information to clients using a trust certification authority. It can delegate access without exposing IDs or passwords to third parties by using tokens to delegate authority [38].

The OAuth framework consists of a resource owner (user), resource server, client, and authorization server. The resource owner is the owner of the protected resource and the user who can grant access, and the resource server is the server that stores the protected user's resources. The client is an application that accesses resources on behalf of the user, and the authorization server is a server that authorizes the resource owner by authenticating and issuing tokens to the client. In OAuth, the resource owner sends a request to the application (client) that they want to use, and the application requests it again from the permission server to authenticate the user and issue a permission token. The application receives an authorized token from the authority server and accesses the information of the protected user on the resource server [39].

Secure Token

OAuth uses access tokens to delegate access to clients. An access token is a string containing information about authorization, such as scope and period, and no specific format is specified. Therefore, in OAuth, the server may select various types of access tokens. However, access tokens issued by all authorization servers cannot be interpreted by the client and have the property of not containing user information [39].

Many commercial implementations utilize JSON Web Token (JWT) as an access token in OAuth 2.0. The JWT may include authentication and authorization information as a JSON object and may ensure integrity through a digital signature [40]. However, in constrained devices such as IoT devices, bearer tokens including JWT have the disadvantage of being overcalculated and being able to steal tokens through attacks such as eavesdropping and

hijacking. Therefore, a proof of possession key for CWT was proposed as an improved technology. CWT, a compromise of inefficient JWT in the IoT, is a compact means of encoding small data to deliver claims. In CWT, valid claim sets include issuers, subjects, audience, expiration, not before, issued at, and cwt id, and claim sets have different coverage depending on the situation [41].

The proof of possession (PoP) token proves that the token's presenter is a legitimate user who owns the key through a specific PoP key. The PoP key can be used in both a symmetric key and a private key method that can confirm the ownership of the key in an encrypted method. Symmetric keys are exchanged privately, and asymmetric keys are exchanged for public keys and used for proof of ownership [42]. In addition, PoP token using the CWT token format has been proposed because PoP token is not limited to the format of the token. The token proves the ownership of the key, including a confirmation cnf claim in the issuer iss, the recipient aud, and the expiration time exp claim. PoP token using CWT format is efficient for limited environments using less data, while providing security through proof of possession through the PoP key [43].

3.4. DID

Decentralized identity is a blockchain-based identity management system that allows individuals to manage their IDs, unlike other identifiers [44]. Unlike the existing server–client identity management model and the trust agency identity management model, DID allows users to manage their identifiers, and because it uses a distributed ledger as a storage, it can access unforged identifiers without a trust agency.

The DID consists of DID identifiers and a DID document with a key and value structure. A DID identifier is an address that refers to a DID document recorded in a distributed ledger in the form of a url and consists of scheme, method, and method specific identifier. The DID document stored at the address indicated by the DID identifier is a document containing the user's authentication means and identifiers, including id, public key, authentication method, and other details. The user may develop various services by adding detailed items. Members who want to access the DID document through the DID identifier can see the DID document using the DID resolver [45].

4. System Architecture

In this section, we propose OAuth-based blockchain for IoT access control management, which uses DID to authenticate the parties, and a smart contract to automate verification and recording. The proposed architecture is described in Figure 1. The elements of the proposed architecture are as follows:

- User: Service users who want to register and access the IoT to use IoT devices and multiple applications on IoT devices (e.g., e-health, smart home, auto driving car, etc.). It is the owner of the resources that the IoT wants to access.
- IoT device: This is an IoT device that a user wants to access, and the access authority is delegated from the user to access and use the user's information on the resource server. Various IoT devices such as wearable devices such as smartwatches, self-driving cars, and smart home systems are included.
- Blockchain and smart contract: Blockchain nodes use smart contracts to authenticate and authorize users and IoT devices. Users and IoT devices verified through smart contracts are submitted transactions on the distributed ledger, and blockchain issues tokens for access, and records them on the ledger. The secure token key, requested by the resource server, is also verified, and recorded to serve as an authentication server.
- DID resolver: A DID document containing the authentication keys and authentication methods of users and the IoT is found through DID and delivered to the blockchain.
- Resource Server: This stores and manages the user resource. When IoT accesses it through tokens, it calls smart contracts on the blockchain to verify the integrity and possession of the tokens and delivers protected user resource to the IoT.

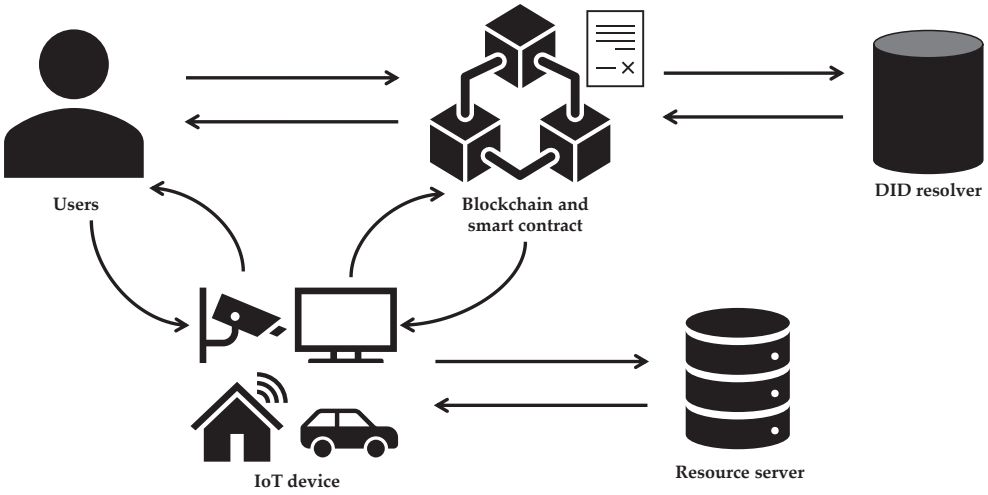

Figure 1. The proposed architecture.

In real-life scenarios, the IoT is widely used not only in industries but also in our daily lives. Some of the most prominent IoT devices closely integrated into our daily routines are wearable IoT devices, with smartwatches being a leading example. In this architecture, users connect to their smartwatches (IoT) through their smartphones (clients). The user and the smartwatch are authenticated using decentralized identifiers (DID) through a blockchain, and the authentication status is recorded on the blockchain. The blockchain issues an access token, known as a PoP (proof of possession) token, to the authenticated smartwatch, granting it access to the resource server where the user's biometric information, such as height, weight, heart rate, and activity level, is stored. The resource server verifies the PoP key provided by the blockchain to validate the legitimacy of the smartwatch and subsequently delivers encrypted biometric data.

Similarly, with the commercialization of autonomous vehicles, which have been steadily developed in recent years, the importance of authentication and access control is becoming evident. In this architecture, users connect to autonomous vehicles (IoT) using their smartphones (clients), where their authentication credentials (DID) are stored. The connected user and autonomous vehicle are authenticated through decentralized identifiers (DID) using blockchain technology to access and communicate user information and location data. The blockchain issues an access token, known as a PoP (proof of possession) token, to the authenticated autonomous vehicle and records the authentication process. The autonomous vehicle utilizes the PoP token to access the resource server, and upon verification of the PoP key by the resource server against the blockchain, encrypted user information and location data are transmitted if deemed legitimate.

4.1. Security Requirements

Several requirements are needed for this framework to serve as an access control environment for IoT. Therefore, we would like to propose a framework that satisfies the following requirements. The detailed requirements are as follows:

- Flexibility: In the IoT authentication environment, users should possess compatibility and scalability, enabling them to freely register and access any IoT device while appropriately managing their permissions. Additionally, IoT devices should exhibit flexibility in accommodating users' resource usage and support various authentication methods tailored to both users and IoT devices. The proposed framework effectively leverages decentralized identifiers (DID) and OAuth-based secure tokens to perform authentication and access control at a superior level.
- Authentication: Whether a legitimate user enrolls in an access control framework or whether a legitimate IoT device uses the user's resources is very important. The proposed framework goes through an authentication process through smart contracts

on the authentication blockchain to see if both users and IoT devices who want to enroll are legitimate.

- Integrity: The integrity of the authentication information of the user requesting authentication or IoT is very important. Since the proposed framework uses DID, authentication credential information for users and IoT can be recorded in blockchain to ensure integrity, and other authentication and authorization information can also be hashed and recorded on the authentication blockchain.
- Data confidentiality: The user's critical data should be encrypted, safely stored, and safely transmitted to the authenticated IoT. The user's data to be accessed by the IoT is encrypted in the resource server and stored safely. In addition, the resource server can maintain the confidentiality of the data by providing protected information after verifying the ownership proof of the access authority token using the key contract of the authentication blockchain of IoT.
- Key agreement: Access control management uses encryption keys for encryption, authentication, and authorization. In the proposed framework, users and IoT proceed with signatures using public key algorithms to authenticate each other, and also use security tokens to prove ownership using symmetric keys. Public keys for authentication are exchanged using DID, and symmetric keys for token ownership proof are encrypted and delivered using public keys of authenticated users and IoT by the authentication blockchain.
- Decentralization: Various security threats from authentication servers that perform authentication of users and IoT devices can be prevented by decentralizing the server. In the proposed framework, blockchain, a decentralized authentication server, can eliminate the threat of a centralized authentication server.
- Traceability: Access control management using blockchain, a distributed ledger, should be able to record and track logs for users and IoT devices to access and users and devices to authenticate and enroll. The proposed framework provides traceability to accessors by recording values encrypted with public keys of authenticated and registered users and IoT devices.

4.2. The Proposed Protocol

Figure 2 describes the OAuth-based blockchain for IoT access framework flow. We construct and describe only the user and IoT registration and authentication, authorization, and RS access phases of the framework using OAuth and blockchain. The detailed flow and description of the framework flow is as follows. Note that the cryptographic notations in the protocol is explained in Table 2.

1. User sends a request message, denoted as $\{(User'sDID), Sign_{SK_C}(H(User'sDID))\}$, to the IoT device. The request includes the user's DID and the signed hash of the DID using the user's secret key.
2. When the IoT device receives the request, it adds its own DID and the signed hash of its DID using the IoT's secret key to the user's request. Subsequently, the IoT device sends the resource access request transaction, denoted as $\{(User'sDID, IoT'sDID), Sign_{SK_{IoT}}(Sign_{SK_C}(H(User'sDID))||H(IoT'sDID))\}$, to the blockchain. In this transaction, the IoT device includes the user's DID, the IoT device's DID, and the signature of the set comprising the signed hash of the user's DID and the hash of the IoT device's DID.
3. After receiving the transaction, the IoT authentication contract code is executed by blockchain nodes. The IoT authentication contract uses DID documents from the IoT DID identifier addresses through DID resolver to authenticate the IoT device. The IoT device's DID document includes the authentication methods; the IoT authentication is performed using the IoT device's public key. The IoT authentication contract authenticates the IoT by verifying the signature of the request through the public key of the IoT device. If the DID hash of the signed IoT device matches, the verification is successful.

4. If the IoT device's validation is successful, the blockchain nodes execute the next user authentication contract code to verify the user. The same as the IoT authentication contract, the user authentication contract obtain the user's DID document via DID resolver, and then verifies the user. The user authentication contract authenticates the user by verifying the signature of the request through the public key of the user. If the DID hash of the signed user matches, the verification is successful. Based on OAuth 2.0, the proposed framework uses tokens for delegation of authority. Thus, the user authentication contract code also generates the random PoP key, access token, random session ID r, and user's public key encryption of r. The access token (CWT), which is the payload of the PoP token, must have four fields: issuer (ISS), audience (AUD), expiration time (EXP), and confirmation (CNF). The framework uses the PoP key to make a secure token that proves ownership, to delegate authority, and to access resources. Access through PoP tokens, which are security tokens using access tokens and PoP keys, can achieve security on constrained IoT devices because they require PoP keys as well as tokens.
5. If the user's validation is successful and all the authentication contracts are closed, the node submits the transaction $\{E_{PK_C}(Acc.token||PoP\ key), E_{PK_{IoT}}(Acc.token||PoP\ key), h(r), h(PoP\ key)\}$ to the blockchain. This transaction includes the user's public key encryption of the access token and PoP key, the IoT's public key encryption of the access token and PoP key, the hash of the access token, the hash of r, and the hash of the PoP key.
6. After the transaction recording is complete, the node sends a response message to the IoT device. The response message $E_{PK_{IoT}}(PoP\ key||Acc.token||r||E_{PK_C}(r))$, contains the encryption of PoP key, access Token, r, and the user's public key encryption of r.
7. The IoT can decrypt and obtain the access token, PoP key, and session ID r if the IoT device is a legitimate device. The IoT device sends an authorization granted reply and encrypted r, $E_{PK_C}(r)$, to notify the user that authentication and authorization were successful.
8. The IoT device makes the PoP token using the access token and the PoP key obtained, that is made up of the access token and encrypts the access token with the PoP key. The encryption parts of the PoP token assure the integrity and authentication of the access token. In the IoT system, to access the resource, a proof of possession (PoP) token $\{Acc.token, E_{PoP}(Acc.token)\}$ and $E_{PK_{RS}}(PoP\ key)$ are sent to the resource server. The PoP token comprises an access token and an encrypted access token with the PoP key. The PoP key is further encrypted with the resource server's public key.
9. When the RS receives the PoP token and the RS's public key encryption of the PoP key, the hash of the PoP key, the RS can obtain the PoP key and send the key verify request transaction to blockchain.
10. The RS only sends the hash of the PoP key, and requests the transaction to execute the key contract to verify the PoP key.
11. The key contract checks the previous transaction record on blockchain to verify the PoP key. If key validation is successful, the node submits the hash of the PoP key $H(PoP\ key)$, transaction.
12. The RS sends the protected resource to the IoT device.

Table 2. Cryptographic notation.

	Description
$Sign_{SK_C}$	Signature of user (client) using user's secret key
$Sign_{SK_{IoT}}$	Signature of the IoT using user's secret key
E_{PK_C}	Encryption using the user's public key
$E_{PK_{IoT}}$	Encryption using the IoT's public key
E_{PoP}	Encryption using the PoP key
$E_{PK_{RS}}$	Encryption using the resource server's public key

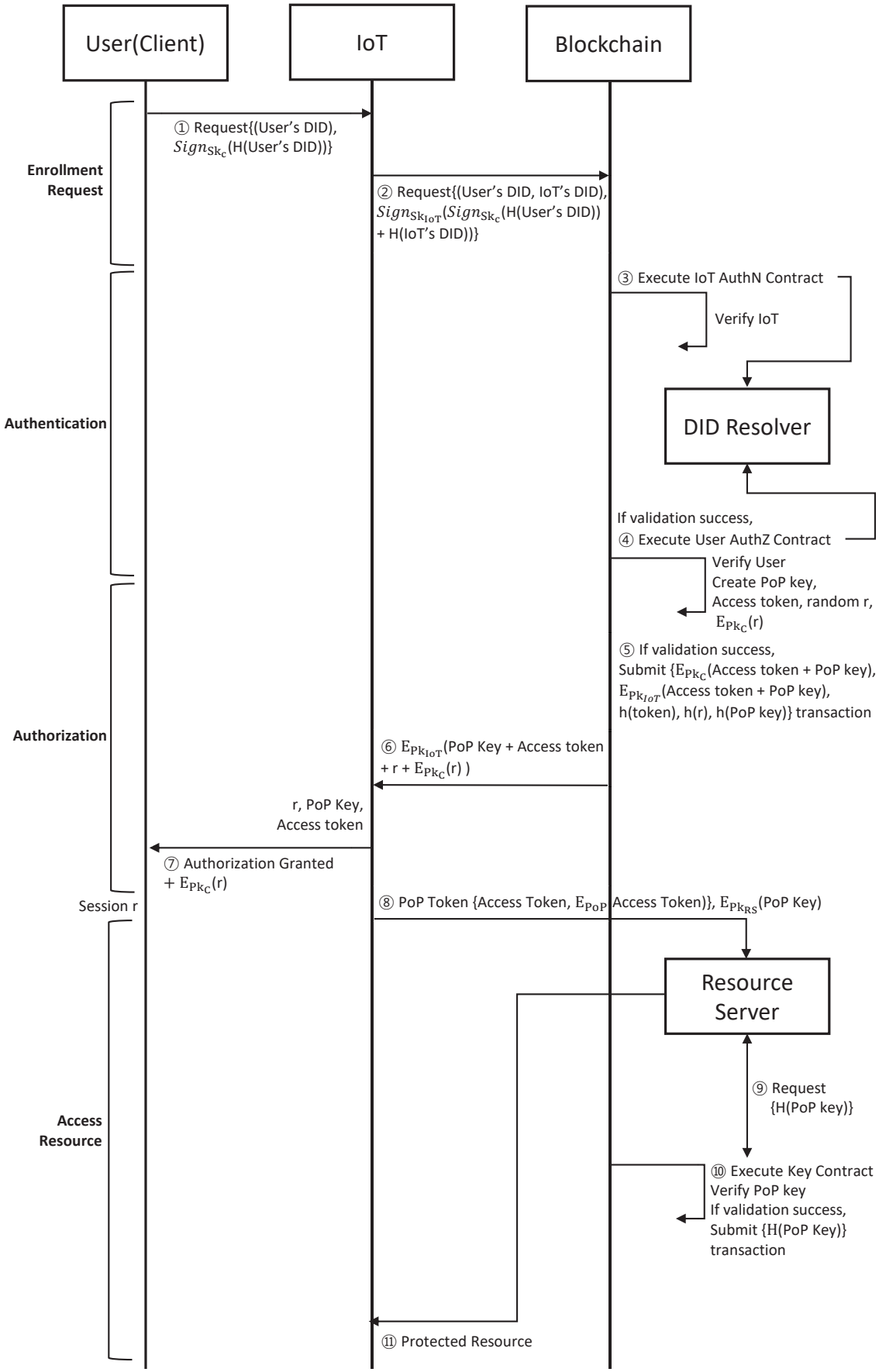

Figure 2. The proposed protocol.

5. Discussion

In this section, the techniques used in this paper were compared based on each criterion.

5.1. Using Decentralized Authorization

Authorization services, including OAuth, which are widely used in various systems, including various clouds, the web, and IoT, perform authentication and authorization using a centralized server. Centralized servers have the advantage of being easy to manage, fast to process transactions, and efficient, but there are various vulnerabilities that threaten the confidentiality and integrity of the data. However, most of these security problems can be solved through decentralization of the centralized servers.

First, a typical threat that threatens the server may be an attack by a malicious hacker. Hackers can perform brute force, DoS, DDoS, and various injection attacks, including malware, and SQL, paralyzing the server, causing system failures, or leaking sensitive information [46]. However, decentralized systems such as blockchain are distributed, so attacks are very difficult because they can cause system failures only when more than a majority of nodes are attacked, and the structure of the distributed ledger itself makes an injection attack impossible. In addition, blockchain, that relies on hash, an encryption technology, guarantees the integrity and immutability of the data to prevent data deletion, forgery, and tampering [47].

Furthermore, there may be attacks by malicious insiders inside the server, not by malicious hackers outside [48]. Distributed systems, including blockchain, are meaningless, because multiple participants manage the system, not an authorized administrator. Therefore, in addition to the problem of malicious insiders, security problems caused by managers' mistakes can also be prevented.

5.2. Using Smart Contract

A distributed ledger that replaces an authentication server can be used as a storage for simply recording and storing authentication and authorization results, but a distributed ledger can be used more efficiently and safely by using a smart contract running on a blockchain. Since smart contracts can implement any contract, they can perform tasks such as party verification that are difficult to perform on the blockchain, allowing the blockchain to play the role of an authentication server instead [49]. In addition, smart contracts automatically collect contracts when conditions are met, so without using smart contracts, verification through third-party trust agencies such as authentication centers can be omitted, and network attacks such as eavesdropping or MITM can be reduced. In addition, the above smart contract's behavior is free from insider attacks because there is no intervention from managers or third parties involved in the contract.

5.3. Using Secure Token

A PoP token, a secure token, is a proof of ownership token that requires a PoP key to prove the validity of the token. PoP tokens issue an asymmetric or symmetric PoP key to the owner and require proof of ownership by encrypting the token using the PoP key. This means that an attacker or eavesdropper must steal not only the token but also the PoP token bound to the token in order to access the resource server. This provides stronger security than bearer tokens, which do not prove ownership of the key material in OAuth. PoP tokens are also token-agnostic, meaning that you can choose token formats that are appropriate for your environment and framework. This flexibility of PoP tokens allows you to build token security using the more efficient CWT token format for limited IoT environments.

5.4. Using DID for Authentication

DID has the advantage of being able to manage the public information of the document directly and easily, accessing the DID document through the DID identifier, as it stores its public key, authentication method, and identifier in a distributed ledger. This provides the

advantage of being able to perform authentication without going through a third agency or a trust agency. In addition, since it is recorded in the distributed ledger, the integrity of the identifier inside the document can be guaranteed.

Various clients and users use OAuth for authentication and authorization and verify through an authorization server. When the authorization server is replaced with a decentralized blockchain, blockchain nodes that verify clients and users are not suitable for storing and managing all identifiers. Therefore, DID, which allows access to securely stored identifiers to perform authentication, can be an effective solution to this problem. Except for the identifier management aspect, the use of DID is very efficient in that it guarantees the integrity of the identifier and omits a third trust agency.

6. Security Analysis

The proposed framework satisfies seven security requirements, and a detailed evaluation of each security requirement is provided below.

- Flexibility: The flexibility of the IoT authentication and authorization system should ensure compatibility and scalability within a narrow scope, as well as appropriate authorization and resource accessibility, along with support for various authentication methods in a broader context. The proposed framework utilizes decentralized identifiers (DID), allowing all IoT devices to authenticate and establish connections with users, thus guaranteeing compatibility and scalability. Moreover, the authentication identifiers for IoT are encrypted and recorded within the DID, ensuring data integrity, while IoT devices only store the DID identifier. This approach enhances security measures significantly compared to conventional authentication environments. Furthermore, as DID enables owners to manage authentication identifiers, diverse authentication methods can be supported. Additionally, the adoption of OAuth-based proof of possession (PoP) tokens in the framework enables granting precise authorization and secure resource access.
- Authentication: In the proposed framework, both IoT and user authentication credentials are securely managed within decentralized identifiers (DID), ensuring tamper resistance. The authentication process is securely conducted using automated mechanisms, such as smart contracts within the blockchain nodes, preventing any intervention by attackers or malicious insiders. With vulnerabilities in the authentication process also adequately protected, the proposed framework guarantees reliable authentication.
- Integrity: The authentication credentials used in the framework are recorded on the blockchain, ensuring integrity and immutability. Furthermore, all authentication and authorization processes are recorded on the blockchain, guaranteeing the integrity of the authentication.
- Data confidentiality: In the proposed framework, the user's sensitive data are securely stored in an encrypted form on the resource server. However, during the transmission process to the authenticated IoT devices, the confidentiality of the user's information may be compromised. To address this issue, the framework ensures that only authorized IoT devices, which have undergone thorough authentication processes, can access the resource server. Authorization is achieved using secure tokens, specifically PoP (proof of possession) tokens. These tokens are verified using PoP keys to confirm the ownership and legitimacy of the token holder. Upon receiving the token, the resource server further validates the IoT device's authorization status through the authentication blockchain's key contract, ensuring that the IoT device has been granted appropriate privileges. As a result, the resource server provides the encrypted user data only to the legitimate IoT devices, effectively preventing security incidents where sensitive information is exposed to malicious attackers. Through the implementation of encryption techniques and rigorous authorization management, the proposed framework ensures data confidentiality.
- Key agreement: The proposed framework aims to generate the necessary secret keys for encrypted communication of devices in IoT access control management. This

framework allows owners to directly manage authentication identifiers and utilizes decentralized identifiers (DID) generated through key agreement to enable registered IoT devices and users to create and manage keys for communication. DID leverages distributed ledger technology to enhance the reliability of keys and enables efficient and stable key exchange. This framework is expected to contribute to improved security and performance of IoT systems through fast responsiveness and secure communication.

- Decentralized: Identity verification, authentication information encryption, and log auditing are crucial elements in the authentication and authorization processes. Decentralizing the authentication server helps to protect these vital elements and mitigates various security threats that may arise during the authentication and authorization procedures. This framework leverages distributed identifiers (DID), a decentralized ledger technology, to ensure identity verification and safeguard authentication information against tampering through encryption. Additionally, the authentication and authorization logs are recorded on a decentralized authentication blockchain, preventing log tampering, modifications, or deletions, and enabling transparent log auditing. Moreover, traditional centralized authentication systems suffer from a critical flaw, as a single vulnerability or system failure can render the entire authentication system inoperative. Conversely, a decentralized authentication system such as the authentication blockchain operates in a distributed manner, thus mitigating such vulnerabilities. Furthermore, by utilizing smart contracts functioning on the distributed ledger, the authentication process can be automated without requiring the involvement of third-party trust entities. This automation eliminates security threats that may arise from third-party involvement, facilitating efficient authentication procedures.
- Traceability: The proposed framework records all processes in the authentication system's log for access control management through the authentication blockchain and smart contracts, enabling the traceability of incidents. The authentication contract, authorization contract, and key contract thoroughly document all relevant information, including users and IoT devices as authentication subjects. Sensitive information is securely protected by being encrypted with public keys or hashed and stored on the blockchain, ensuring its safety from external threats. Additionally, the blockchain's immutable nature guarantees the integrity of the logged data, preventing any tampering attempts. As a result, the framework ensures accurate and reliable traceability, enhancing preparedness against potential security incidents. Access control management plays a pivotal role as a core element of the framework, reinforcing data security and trustworthiness.

The security analysis of IoT access control architectures in the literature is given in Table 3.

Table 3. Security analysis of IoT access control architectures.

	Flexibility	**Authentication**	**Integrity**	**Data Confidentiality**	**Key Agreement**	**Decentralized**	**Traceability**
[5–9]	N	Y	N	Y	Y	N	Y
[11–15]	Y	Y	N	Y	Y	N	Y
[16]	N	N	Y	Y	Y	Y	Y
[17]	N	Y	Y	Y	Y	Y	Y
[21]	N	N	Y	Y	Y	Y	Y
[23]	Y	N	Y	Y	Y	Y	Y
[18–20]	N	Y	Y	Y	Y	Y	Y
[22]	Y	Y	Y	Y	Y	Y	N
[24,25]	Y	N	N	Y	Y	N	Y
[26,27]	Y	N	Y	Y	Y	Y	Y
[28,29]	Y	N	Y	Y	Y	N	Y
[30]	N	Y	Y	Y	Y	Y	Y
Ours	Y	Y	Y	Y	Y	Y	Y

7. Conclusions

We propose a decentralized OAuth access control framework utilizing DID for enhanced authentication and authorization in IoT environments. We incorporate improved authentication and authorization procedures from previous OAuth-based access control frameworks. By analyzing existing OAuth-based frameworks, we identify issues associated with centralized authorization servers, such as single-point-of-failure problems and inadequate authentication methods. To address these issues, we decentralize the centralized authorization server in our proposed architecture and employ an efficient and enhanced authentication method called DID. Furthermore, we automate smart contracts on the blockchain to prevent third-party interference, and implement secure tokens at the network layer of the IoT for authorization.

We present the flow of our proposed architecture in detail, strengthened by the aforementioned technologies, and discuss the improvements compared to existing research in accordance with each technology. The paper presents a new framework as the theoretical basis and structure for an improved IoT authentication and authorization architecture. Although scientific evaluation encompassing a performance assessment of the proposed framework is essential, the complexity of the experimental environment poses challenges in conducting the framework evaluation. As future work, we acknowledge the need for more flexible access control despite the enhanced authentication. Therefore, incorporating context-aware capabilities to recognize and adapt to different situations within the architecture can enable more appropriate access control measures. In future research, we will strive to overcome these challenges and conduct additional studies to scientifically appraise and enhance the performance of the proposed framework.

Author Contributions: Conceptualization, J.H.K.; methodology, J.H.K.; validation, J.H.K. and M.S.; formal analysis, J.H.K.; investigation, J.H.K.; writing—original draft preparation, J.H.K.; writing—review and editing, J.H.K. and M.S.; supervision, M.S.; project administration, M.S.; funding acquisition, M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Duksung Women's University Research Grants 2021.

Data Availability Statement: The data is collected from the sources: Elsevier's Library, IEEE Xplore, IET Digital Library, The Institute of Electronic, Information and Communication Engineers (IEICE), ACM Digital Library, Springer and Web of Science (WoS).

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

References

1. Hosseini, S.M.; Ferreira, J.; Bartolomeu, P.C. Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations. *Electronics* **2023**, *12*, 1283. [CrossRef]
2. Salih, K.O.M.; Rashid, T.A.; Radovanovic, D.; Bacanin, N. A comprehensive survey on the Internet of Things with the industrial marketplace. *Sensors* **2022**, *22*, 730. [CrossRef] [PubMed]
3. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
4. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
5. Sandhu, R.; Coyne, E.; Feinstein, H.; Youman, C. Role-based access control models. *Computer* **1996**, *29*, 38–47. [CrossRef]
6. Sandhu, R.; Ferraiolo, D.; Kuhn, R. The NIST model for role-based access control: Towards a unified standard. In Proceedings of the ACM Workshop on Role-Based Access Control, Berlin, Germany, 26–28 July 2000; Volume 10.
7. Giordano, M.; Polese, G. Visual computer-managed security: A framework for developing access control in enterprise applications. *IEEE Softw.* **2012**, *30*, 62–69. [CrossRef]
8. Zhang, N.; Ryan, M.; Guelev, D.P. Synthesising verified access control systems in XACML. In Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering, Washington, DC, USA, 29 October 2004; pp. 56–65.
9. Thomas, R.K.; Sandhu, R.S. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In *Database Security XI: Status and Prospects*; Springer: Boston, MA, USA, 1998; pp. 166–181.
10. Heydon, A.; Maimone, M.W.; Tygar, J.; Wing, J.M.; Zaremski, A.M. Miro: Visual specification of security. *IEEE Trans. Softw. Eng.* **1990**, *16*, 1185–1197. [CrossRef]

11. Khan, J.; Li, J.P.; Ali, I.; Parveen, S.; ahmad Khan, G.; Khalil, M.; Khan, A.; Haq, A.U.; Shahid, M. An authentication technique based on oauth 2.0 protocol for internet of things (IoT) network. In Proceedings of the 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 14–16 December 2018; pp. 160–165.
12. Sciancalepore, S.; Piro, G.; Caldarola, D.; Boggia, G.; Bianchi, G. OAuth-IoT: An access control framework for the Internet of Things based on open standards. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 676–681.
13. Fernández, F.; Alonso, Á.; Marco, L.; Salvachúa, J. A model to enable application-scoped access control as a service for IoT using OAuth 2.0. In Proceedings of the 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 7–9 March 2017; pp. 322–324.
14. Oh, S.R.; Kim, Y.G.; Cho, S. An interoperable access control framework for diverse IoT platforms based on oauth and role. *Sensors* **2019**, *19*, 1884. [CrossRef]
15. Oh, S.R.; Kim, Y.G. AFaaS: Authorization framework as a service for Internet of Things based on interoperable OAuth. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720906388. [CrossRef]
16. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards decentralized IoT security enhancement: A blockchain approach. *Comput. Electr. Eng.* **2018**, *72*, 266–273. [CrossRef]
17. Li, D.; Peng, W.; Deng, W.; Gai, F. A blockchain-based authentication and security mechanism for IoT. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–6.
18. Gong, L.; Alghazzawi, D.M.; Cheng, L. BCoT sentry: A blockchain-based identity authentication framework for IoT devices. *Information* **2021**, *12*, 203. [CrossRef]
19. Ferreira, C.M.S.; Garrocho, C.T.B.; Oliveira, R.A.R.; Silva, J.S.; Cavalcanti, C.F.M.d.C. IoT registration and authentication in smart city applications with blockchain. *Sensors* **2021**, *21*, 1323. [CrossRef] [PubMed]
20. Tahir, M.; Sardaraz, M.; Muhammad, S.; Saud Khan, M. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. *Sustainability* **2020**, *12*, 6960. [CrossRef]
21. Ayoade, G.; Karande, V.; Khan, L.; Hamlen, K. Decentralized IoT data management using blockchain and trusted execution environment. In Proceedings of the 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, USA, 6–9 July 2018; pp. 15–22.
22. Ahsan, T.; Iqbal, Z.; Ahmed, M.; Alroobaea, R.; Baqasah, A.M.; Ali, I.; Raza, M.A. IoT devices, user authentication, and data management in a secure, validated manner through the blockchain system. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8570064. [CrossRef]
23. Ourad, A.Z.; Belgacem, B.; Salah, K. Using blockchain for IOT access control and authentication management. In Proceedings of the Internet of Things–ICIOT 2018: Third International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, 25–30 June 2018; Proceedings 3; Springer: Berlin/Heidelberg, Germany, 2018; pp. 150–164.
24. Siris, V.A.; Dimopoulos, D.; Fotiou, N.; Voulgaris, S.; Polyzos, G.C. OAuth 2.0 meets blockchain for authorization in constrained IoT environments. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 364–367.
25. Siris, V.A.; Dimopoulos, D.; Fotiou, N.; Voulgaris, S.; Polyzos, G.C. Decentralized authorization in constrained IoT environments exploiting interledger mechanisms. *Comput. Commun.* **2020**, *152*, 243–251. [CrossRef]
26. Riabi, I.; Ayed, H.K.B.; Zaghdoudi, B.; George, L. Blockchain based OAuth for IoT. In Proceedings of the 2021 10th IFIP International Conference on Performance Evaluation and Modeling in Wireless and Wired Networks (PEMWN), Ottawa, ON, Canada, 23–25 November 2021; pp. 1–7.
27. Sylla, T.; Mendiboure, L.; Chalouf, M.A.; Krief, F. Blockchain-based context-aware authorization management as a service in iot. *Sensors* **2021**, *21*, 7656. [CrossRef] [PubMed]
28. Fotiou, N.; Pittaras, I.; Siris, V.A.; Polyzos, G.C. Enabling opportunistic users in multi-tenant IoT systems using decentralized identifiers and permissioned blockchains. In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things, London, UK, 15 November 2019; pp. 22–23.
29. Lagutin, D.; Kortesniemi, Y.; Fotiou, N.; Siris, V.A. Enabling decentralised identifiers and verifiable credentials for constrained IoT devices using OAuth-based delegation. In Proceedings of the Workshop on Decentralized IoT Systems and Security (DISS 2019), in Conjunction with the NDSS Symposium, San Diego, CA, USA, 24 February 2019; Volume 24.
30. Dixit, A.; Smith-Creasey, M.; Rajarajan, M. A Decentralized IIoT Identity Framework based on Self-Sovereign Identity using Blockchain. In Proceedings of the 2022 IEEE 47th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 26–29 September 2022; pp. 335–338.
31. Gokhale, P.; Bhat, O.; Bhat, S. Introduction to IOT. *Int. Adv. Res. J. Sci. Eng. Technol.* **2018**, *5*, 41–44.
32. Madakam, S.; Ramaswamy, R.; Tripathi, S. Internet of Things (IoT): A literature review. *J. Comput. Commun.* **2015**, *3*, 164. [CrossRef]
33. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
34. Antonopoulos, A.M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2014.
35. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
36. Kolvart, M.; Poola, M.; Rull, A. Smart contracts. In *The Future of Law and Etechnologies*; Springer: Cham, Switzerland, 2016; pp. 133–147.

37. Mohanta, B.K.; Panda, S.S.; Jena, D. An overview of smart contract and use cases in blockchain technology. In Proceedings of the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 10–12 July 2018; pp. 1–4.
38. Fett, D.; Küsters, R.; Schmitz, G. A comprehensive formal security analysis of OAuth 2.0. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1204–1215.
39. Hardt, D. *The OAuth 2.0 Authorization Framework (No. rfc6749)*; Technical Report; IETF: Wilmington, DE, USA, 2012.
40. Bertocci, V. *RFC 9068 JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens*; IETF: Wilmington, DE, USA, 2021 .
41. Jones, M.; Wahlstroem, E.; Erdtman, S.; Tschofenig, H. *Cbor Web Token (cwt) (No. rfc8392)*; Technical Report; IETF: Wilmington, DE, USA, 2018 .
42. Jones, M.; Bradley, J.; Tschofenig, H. *Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs) (No. rfc7800)*; Technical Report; IETF: Wilmington, DE, USA, 2016 .
43. Jones, M.; Seitz, L.; Selander, G.; Erdtman, S.; Tschofenig, H. Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs). IETF Draft, February 2019. Available online: https://www.ietf.org/proceedings/103/slides/slides-103-ace-pop-key-semantics-for-cwts-00.pdf (accessed on 7 August 2023).
44. Kwon, J.W.; Sep, S.H.; Lee, K.H. Understanding and Applications of Blockchain-based Decentralized Identity. In Proceedings of the Korea Information Processing Seciety Conference, Online, 14–15 May 2021; Volume 28, pp. 309–312.
45. Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M.; Holt, J. *Decentralized Identifiers (dids) v1.0: Core Architecture, Data Model, and Representations*; W3C Working Draft; W3C: Wakefield, MA, USA, 2020.
46. Chou, T.S. Security threats on cloud computing vulnerabilities. *Int. J. Comput. Sci. Inf. Technol.* **2013**, *5*, 79. [CrossRef]
47. Gamage, H.; Weerasinghe, H.; Dias, N. A survey on blockchain technology concepts, applications, and issues. *SN Comput. Sci.* **2020**, *1*, 114. [CrossRef]
48. Ashktorab, V.; Taghizadeh, S.R. Security threats and countermeasures in cloud computing. *Int. J. Appl. Innov. Eng. Manag. (IJAIEM)* **2012**, *1*, 234–245.
49. Kemmoe, V.Y.; Stone, W.; Kim, J.; Kim, D.; Son, J. Recent advances in smart contracts: A technical overview and state of the art. *IEEE Access* **2020**, *8*, 117782–117801. [CrossRef]