future internet

MDPI

Review

SoK: Delegated Security in the Internet of Things

Emiliia Geloczi [1,*], Felix Klement [1], Patrick Struck [2] and Stefan Katzenbeisser [1,*]

[1] Faculty of Computer Science and Mathematics, University of Passau, 94032 Passau, Germany; felix.klement@uni-passau.de
[2] Cryptography and Cyber Security, Department of Computer and Information Science, University of Konstanz, 78464 Konstanz, Germany; patrick.struck@uni-konstanz.de
* Correspondence: emiliia.geloczi@uni-passau.de (E.G.); stefan.katzenbeisser@uni-passau.de (S.K.)

Abstract: The increased use of electronic devices in the Internet of Things (IoT) leads not only to an improved comfort of living but also to an increased risk of attacks. IoT security has thus become an important research field. However, due to limits on performance and bandwidth, IoT devices are often not powerful enough to execute, e.g., costly cryptographic algorithms or protocols. This limitation can be solved through a delegation concept. By delegating certain operations to devices with sufficient resources, it is possible to achieve a high level of security without overloading a device that needs protection. In this paper, we give an overview of current approaches for security delegation in the context of IoT, formalise security notions, discuss the security of existing approaches, and identify further research questions. Furthermore, a mathematical formalisation of the CIA triad (confidentiality, integrity, and availability) is proposed for the predefined application areas, in order to evaluate the different approaches.

Keywords: Internet of Things; delegation; security; access control; authorisation; computation; authentication

Academic Editors: Christos Tryfonopoulos and Nicholas Kolokotronis

Received: 27 March 2025
Revised: 25 April 2025
Accepted: 29 April 2025
Published: 30 April 2025

Citation: Geloczi, E.; Klement, F.; Struck, P.; Katzenbeisser, S. SoK: Delegated Security in the Internet of Things. *Future Internet* **2025**, *17*, 202. https://doi.org/10.3390/fi17050202

1. Introduction

The number of electronic devices in use is steadily increasing [1]. While IoT devices enhance comfort and are attractive for widespread utilisation, they also pose a significant cybersecurity risk [2]. During operation, IoT devices communicate with each other and with the outside world, receiving, transmitting and generating a large amount of data, which can be critical under certain conditions. Critical data in possession of adversaries can cause irreparable damage to individuals or institutions [3]. Beyond unauthorised data access, adversaries can also compromise IoT devices, leading to service disruptions and potential safety risks. For example, in healthcare applications, a compromised medical IoT device, e.g., a connected inhaler, blood sensor, or asthma monitor, could generate false alerts or misleading medical recommendations to patients and doctors, resulting in inappropriate treatment and endangering patient safety [4].

Despite IoT devices providing a wide range of services, their computational and communication resources are constrained, as they are designed to be lightweight, and in many cases battery-powered. As a result, they are often unable to execute complex security mechanisms and protect themselves from cyberattacks [5]. One effective strategy to address this issue and ensure the security of resource-constrained IoT devices is delegation [6,7].

The general idea behind security delegation is that a resource-constrained device, which lacks the computational capacity to perform advanced security measures, outsources them to a more powerful device, called a *delegate*. The *delegate* acts as a trusted entity that

performs security-related functions on behalf of the constrained device, ensuring security and avoiding overloading the limited resources, thereby "encapsulating" the device in a secure environment (see Figure 1).

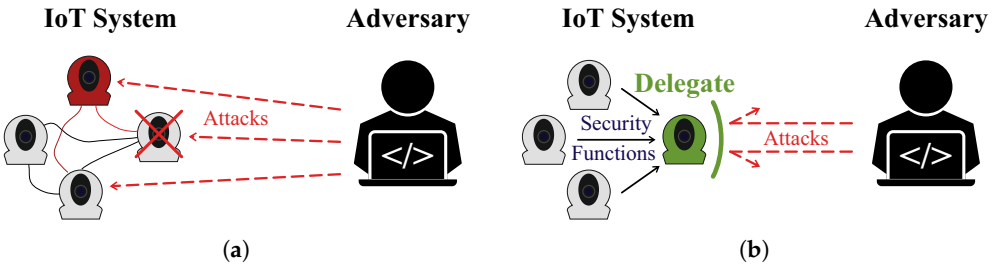


Figure 1. IoT System (**a**) without and (**b**) with security delegation.

For example, Saied et al. propose a collaborative approach to key establishment based on delegation [8]. In the proposed scenario, a highly resource-constrained sensor intends to exchange data with an external server securely. Since the sensor is unable to perform costly computations, it delegates the establishment of a session key with the external server to a group of proxy nodes. The proxies complete key agreement with the server on behalf of the sensor using Diffie–Hellman key exchange and submit the resulting session key to the sensor. Thus, all heavy computations are performed by proxies, while the sensor only needs to handle the lightweight secret key. This approach results in lower costs compared to a TLS handshake. Additionally, one could argue that it shifts the adversary's target from the "weak" device to the "strong" one, which can be better protected. Hence, we can hope that delegation in IoT systems also enhances security. However, delegation may introduce other attack vectors and complicate security models as well as security properties due to the introduction of the delegate.

Several studies have been carried out on security delegation, exploring different techniques and implementations. However, most works use different adversary models and assumptions [9,10]. In some cases, solutions are even proposed without security arguments or proofs [11–13]. Some works focus more on performance improvements [14,15], while others prioritise enhancing security [16,17]. Furthermore, the role of the *delegate* varies, with some approaches relying on centralised authorities [18,19], while others distribute security tasks among multiple entities [8,20]. The listed reasons make a direct comparison of delegating approaches challenging, a difficulty further exacerbated by the lack of a standardised evaluation framework.

1.1. Contributions of This Paper

In this SoK paper, the following key contributions are presented:

- A review of existing works on security delegation in IoT, including the identification of common characteristics and the derivation of generalised architectures for four application domains.
- A flexible adversary model and a formalisation of security properties relevant to the identified application domains.
- An evaluation of the security of approaches described in the literature using the presented security models.
- An identification of the limitations of security delegation in IoT environments and suggestions for future research directions.

1.2. Organisation of This Paper

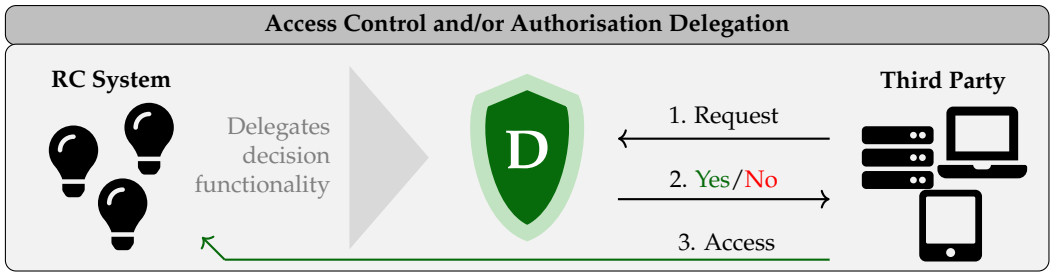
The rest of this paper is organised as follows. Section 2 presents a classification of existing works that introduce delegation-based security solutions in IoT, according

to their application domains. A formal definition of the adversary model is provided in Section 3. Section 4 introduces sound formalisations of security properties for the identified application domains. In Section 5, the existing delegation solutions are evaluated with respect to the proposed security model. The results of the evaluation are discussed in Section 6. Potential future research directions are outlined in Section 7, and the paper is concluded in Section 8.

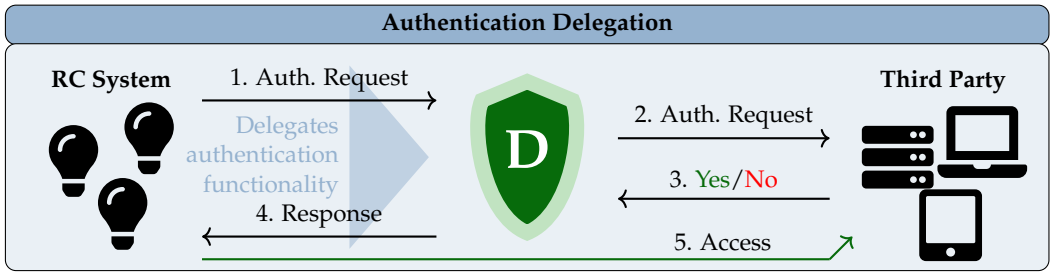
2. Application Domains of Security Delegation

In this paper, we conduct a review of 254 existing research works related to security delegation in the context of the IoT. The methodology used to identify and select these works is described in Appendix A.

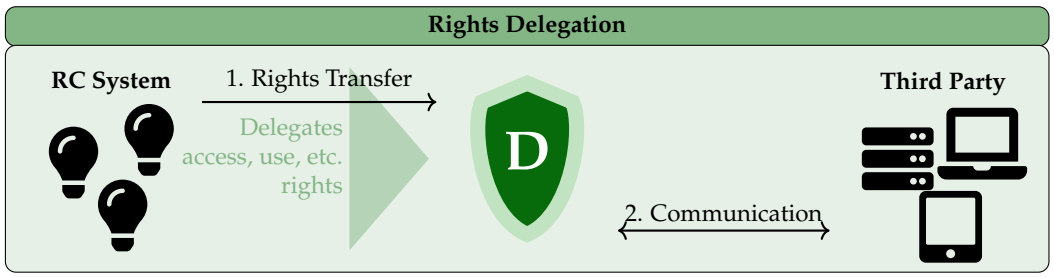
During the analysis of the selected works, it was observed that they focus on four application domains: access control and/or authorisation delegation, authentication delegation, rights delegation, and computation delegation. Within these domains, the proposed solutions exhibit similar architectural patterns, allowing us to identify generalised system architectures presented in Figure 2. These architectures and their illustrative examples are described in detail in this section.



(a)

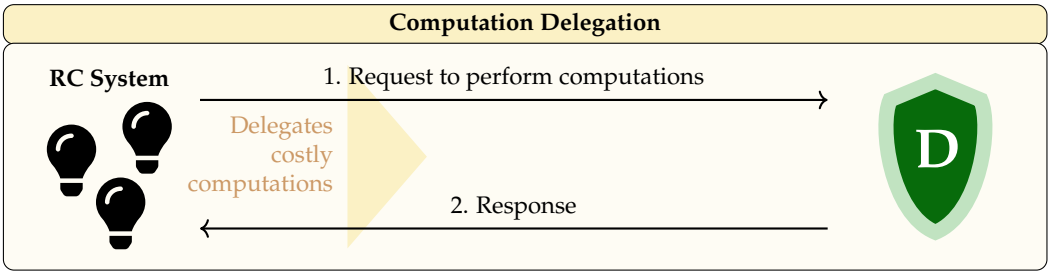


(b)



(c)

Figure 2. *Cont.*



(**d**)

Figure 2. The generalised schemes of the system architectures based on the application domains: (**a**) Access Control and/or Authorisation Delegation; (**b**) Authentication Delegation; (**c**) Rights Delegation; and (**d**) Computation Delegation.

The identified system architectures include the following parties:

- *Resource-constrained (RC) System:* This party wants to benefit from security delegation. It can be a single device (e.g., a light bulb, a smart vacuum cleaner, a sensor, etc.) or several networked IoT devices. It is assumed that the RC system does not have enough resources to perform some security functions on its own.
- *Delegate:* A device that has sufficient resources to perform resource-intensive cryptographic operations, maintain necessary security and communication protocols, etc. The delegate performs these operations on behalf of the RC system.
- *Third Party:* Any party that interacts with the RC system via the delegate is called a third party. For example, the RC system may want to access resources or services of the third party, or the third party requires access to the RC system.

2.1. Access Control and/or Authorisation Delegation

Access control or authorisation allows or denies access to certain elements of the RC system requested by the third party, based on a security policy. Such policies can be complex decisions that need to be delegated. Through our selection procedure, 47 publications were identified that deal with this domain (see Table A1).

In these applications, the RC system delegates the evaluation of the security policy regarding access control and authorisation to the delegate. The third party first requests access via the delegate, who then verifies the request, makes a decision, and forwards the response to the third party. In case of a positive verdict, the third party obtains access to the RC system (see Figure 2a).

Example

Park and Park present a delegated group-oriented access control security mechanism based on DTLS, which reduces the total computational burden [21]. The proposed system includes the RC system consisting of sensors, a client acting as a third party, and a Security Proxy (SP), which acts as a delegate and manages access control on behalf of the RC system (see Figure 3). During the first step of the proposed protocol, SP forms a list of approved sensor devices and issues a capability ID to each authorised client. Subsequently, the client can directly perform a DTLS handshake and communicate with the desired sensor device from the list. The authors conclude that their mechanism is superior to performing standard approaches without access control delegation in terms of execution time and security.

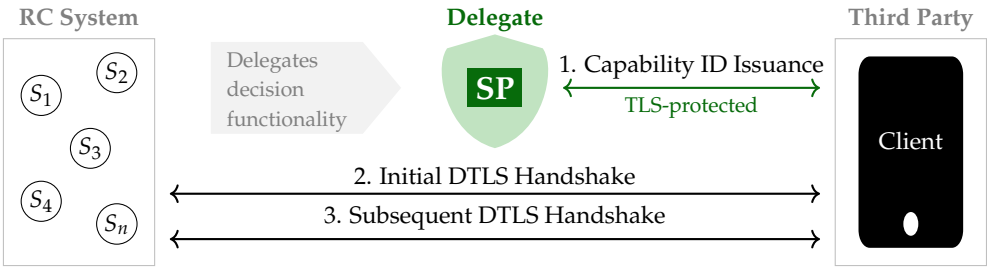


Figure 3. Architecture of the group-oriented end-to-end security mechanism based on DTLS [21]. SP is the Security Proxy that serves as a delegate. S_n is a sensor device.

2.2. Authentication Delegation

Authentication protocols authenticate subjects and distribute secret keys for future communication. A total of 21 papers addressing the delegation of authentication were identified during our literature search (see Table A1).

In this application, the RC system wants to authenticate to a third party. It delegates this process to the delegate who performs authentication on behalf of the RC system and returns the result. Consequently, the RC system obtains credentials to access the third party directly (see Figure 2b).

Example

A delegation-based DTLS framework for Cloud-based IoT Services, called D2TLS, has been proposed by Cho et al. D2TLS allows for establishing secure communication while ensuring secure storage of private keys [22]. Unlike DTLS, D2TLS contains a Security Agent (SA), which does not have access to IoT devices' private keys in order to avoid key escrow problems. The presented solution contains three entities (see Figure 4): a client (RC system), the SA (delegate), and a cloud server (third party). First, the client sends a delegation request to the SA. Then, the SA performs a DTLS handshake with the server on behalf of the client in two steps. Finally, the SA sends the client credentials to access the resources of the server. To evaluate the proposed framework, the authors compare D2TLS with DTLS with respect to delays, energy consumption, code size, memory requirements, and session overhead. In terms of delay and energy consumption, the D2TLS shows significantly better results.

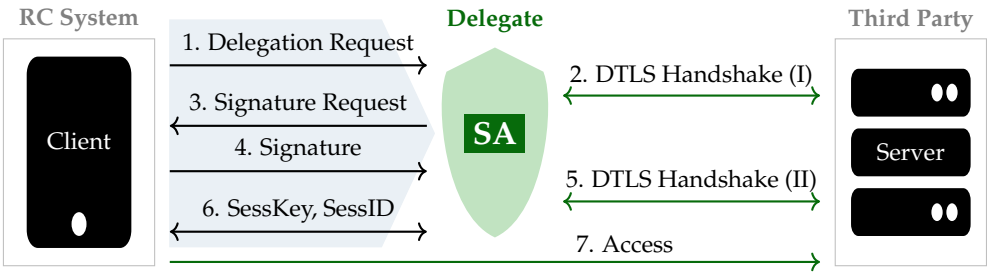


Figure 4. The D2TLS protocol of [22]. SA is a Security Agent.

2.3. Rights Delegation

This category includes papers that address the delegation of various rights (e.g., access, usage, actions, etc.). In total, 123 papers from our literature study targeted this domain (see Table A1).

At first glance, the general architecture of this application domain is similar to authentication delegation. However, there is one significant difference. In authentication delegation, the RC system delegates only the authentication procedure. After its completion, upon receiving the credentials, the RC system independently continues communication with the

third party. In rights delegation, the RC system transfers all its rights related to some third party (e.g., access, use, action, etc.) to the delegate. The delegate is thus able to operate on its own during interaction with the target third party and completely substitute the RC system (see Figure 2c).

Example

Identity-less, asynchronous, and decentralised delegation for IoT based on blockchain technology is presented in [23]. The solution consists of brokers (RC system), buyers (delegate), and a resource manager acting as a third party that offers specific services and resources. All components interact via the blockchain network with smart contracts (see Figure 5). During the preparatory phase, the resource manager registers the offered resources on the blockchain network. The broker has the right to access these resources and can also delegate these rights to the buyer on demand. The buyer requests access rights to the desired resource by triggering a transaction to a delegation smart contract. If the transaction is valid, a new event in the blockchain is generated, and the buyer can request the resource directly. After the first request, the buyer is verified, and only if the verification is successful, the buyer obtains full access to the resource. In comparison with other existing approaches that are not based on blockchain, the described system is asynchronous, decentralised, monotonic, and auditable.

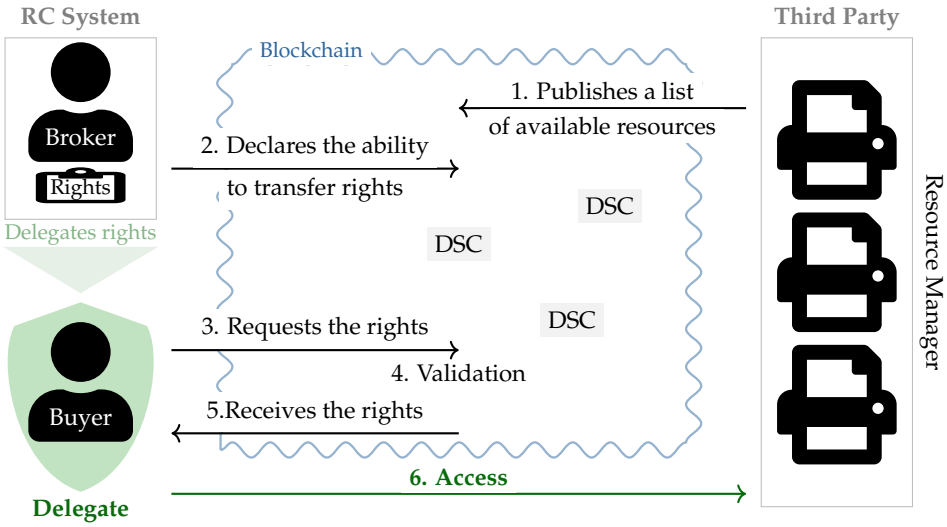


Figure 5. Blockchain-based delegation process of [23]. DSC is a delegation smart contract.

2.4. Computation Delegation

In this application domain, the delegation of computationally intensive cryptographic or computational operations is addressed. Sixty-three papers from our literature review are classified under this domain (see Table A1).

Here, the RC system queries the delegate to perform necessary mathematical computations or cryptographic operations such as key generation, encryption or filtering. After finishing the requested operations, the delegate returns the results to the RC system (see Figure 2d).

Example

In [15], a lightweight revocable hierarchical attribute-based encryption (LW-RHABE) scheme is presented that combines efficient encryption/decryption, flexible key delegation, and revocation.

The solution consists of five main components (see Figure 6). Central and Domain Authorities (CA and DA, respectively) do not participate in delegation directly but generate

system parameters and user secret keys and maintain revocation lists. A Cloud Service Provider (CSP) serves as a delegate that provides storage and computational resources. Data owners and users form the RC system: while data owners are smart IoT devices that collect and encrypt data, users consume data. The workflow of the proposed LW-RHABE system has several steps. First, the CA generates the system's public parameters (a master secret key) and initialises several DAs. Then, the DAs generate secret keys for the users based on their attributes and secret/public keys for data owners. In the next step, data owners create an access control policy, encrypt collected data, and outsource it to the CSP. When the data users want to obtain some data collected by the data owners, they request it and the decryption from the CSP. According to the authors, LW-RHABE allows flexible key delegation and user revocation as well as lightweight encryption and decryption. Based on the results of the performance analysis, the described scheme is significantly more efficient than approaches without delegation.

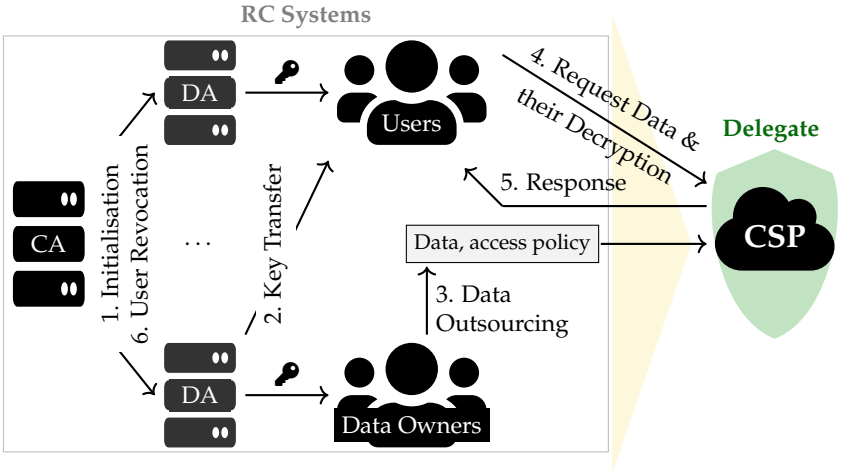


Figure 6. Architecture of the LW-RHABE scheme [15]. CA is Central Authority, DA is Domain Authority, CSP is a Cloud Service Provider.

3. Adversary Model

In order to formulate sound attack models for security delegation in the different application domains mentioned in Section 2, a generalised adversary model is developed, which we believe can provide a possibility to define the different types of adversaries with various capabilities, and thus can be applied even beyond the scope of our study. First, the characteristics and goals of potential adversaries are identified. This leads to a mathematical adversary mode, which is described in detail in this section.

3.1. Adversary Characteristics

Consider three characteristics of an adversary. The first one is the degree of their involvement in the system, where the three following cases can be distinguished: when the adversary is fully external, external with extended capabilities, or internal with direct access to the system. As a second characteristic, the ability of the adversary to corrupt certain parties of the system is taken into account. Here, two cases can be considered: an adversary that either has physical access to the system or does not and thus can or cannot corrupt system parties, respectively. Finally, a third characteristic is related to the adversary's computational resources, represented in terms of the time it takes to complete an attack. All mentioned characteristics are described in Table 1. Combining the cases listed, 18 $(3 \times 3 \times 2)$ adversary types with different capabilities can be defined.

Table 1. Adversary characteristics.

Characteristic	Explanation
	Relation to the system ($\mathcal{RS}$)
External (*Ex*)	Adversary is located outside the system and has no accomplices who are immediate elements or participants in the system. They are therefore unable to observe processes inside the system.
External+ (Ex^+)	Adversary is located outside the system but has resources or accomplices that allow them, within a limited area, to observe processes inside the system.
Insider (*In*)	Adversary is a member of the system, so they may have access and knowledge of the protocols used and the processes taking place, as well as awareness of the communication between the objects.
	Corruption capabilities ($\mathcal{CC}$)
No (*N*)	Adversary has no physical access to the system and no opportunity to corrupt system parties.
Yes (*Y*)	Adversary has physical access to parts of the system and is able to corrupt desired parties.
	Time ($\mathcal{T}$)
Concrete (*C*)	Adversary runs in time t and is capable of launching a successful attack with probability at least ϵ against the system.
Asymptotic (*As*)	Adversary runs in polynomial-time $t(n)$ and is capable of launching a successful attack against the system with probability at least $c + \epsilon(n)$, where ϵ is negligible in the security parameter $n \in \mathbb{N}$ and c is some constant (typically, $c \in \{0, \frac{1}{2}\}$).
Information-theoretic (*It*)	Adversary has unlimited computation time and is capable of succeeding in an attack against the system with non-negligible probability $\epsilon(n)$ for security parameter $n \in \mathbb{N}$.

3.2. Adversary Goals

There are many possible goals of adversaries; however, in the context of security delegation, we focus on the three basic pillars of security known as the CIA-Triad (confidentiality, integrity, and availability). Assume that an adversary wants to violate these security properties defined as follows [24]:

- *Confidentiality:* Unauthorised disclosure and misuse of the resources or information should be prevented.
- *Integrity:* Unauthorised changes, destruction, or loss of resources or information should be prevented.
- *Availability:* Authorised users should have timely and uninterrupted access to requested resources or information.

3.3. Mathematical Model of an Adversary

Based on the characteristics of a potential adversary introduced in Section 3.1, the generalised mathematical adversary model is formulated.

Definition 1. *The adversary characteristics described in Table 1 are denoted as:*

$$\mathcal{RS} \in \{Ex, Ex^{+}, In\},$$
$$\mathcal{CC} \in \{N, Y\}, \text{ and}$$
$$\mathcal{T} \in \{C, As, It\},$$

Then, the general prototype of an individual adversary $\mathcal{A}$ is defined by a triple of features as

$$\mathcal{A} = (\mathcal{RS}, \mathcal{CC}, \mathcal{T}).$$

While attacking a system, the adversary can obtain some information depending on their characteristics and the target of the attack. To formally describe this process, the following oracles are introduced, each representing a specific source of information that may be available to the adversary:

Oracle `Del`: The delegation oracle allows the adversary to interact with the delegate $\mathcal{D}$:

$$\{\mathsf{t}, \perp\} \leftarrow \texttt{Del}(AD).$$

As input, `Del` receives the set of data AD that varies depending on the target of the adversary and application domain. It may include a party or resource id, etc. The oracle either returns an access token t or rejects the request by returning $\perp$.

Oracle `Cor`: The corruption oracle allows the adversary to corrupt parties and learn their secrets s:

$$\{\mathsf{s}, \perp\} \leftarrow \texttt{Cor}(\mathsf{id}).$$

As input, `Cor` receives an identifier of a party id that the adversary wants to corrupt. The oracle will then return the secrets s belonging to the party associated with this id or $\perp$, e.g., if no such party exists.

Oracle `Obs`: The observe oracle allows the adversary to observe the communication between system parties and the delegate $\mathcal{D}$:

$$\{\mathsf{ts}, \perp\} \leftarrow \texttt{Obs}(\mathsf{id}).$$

As input, `Obs` receives id, indicating which party is communicating with $\mathcal{D}$. The oracle will then return the transcript ts of the communication or $\perp$, e.g., if no party associated with id exists.

Oracle `ThP`: This oracle allows the adversary to interact with the third party $\mathcal{TP}$:

$$\{\mathsf{t}, \perp\} \leftarrow \texttt{ThP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i}, \mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i})).$$

As input, `ThP` receives id, indicating which party delegates its rights, $\mathsf{id}_{\mathcal{D}}$ of the party which requested the rights, an identifier of desired resource i and the proof of rights $\mathcal{RP}$ based on id, $\mathsf{id}_{\mathcal{D}}$ and i. The oracle will either return an access token t or reject the request by returning $\perp$.

The adversary can query one or more oracles to obtain information depending on its characteristics and needs. However, according to Table 1, the adversary with $\mathcal{CC} = N$ has no corruption capability; hence, they are not able to query `Cor`. Also, `Obs` cannot be invoked by the adversary with $\mathcal{RS} = Ex$ due to limited observation capabilities. As it was

mentioned in Section 3.1, the cartesian product of all characteristics allows us to generate 18 types of adversaries ($3 \times 3 \times 2 = 18$). Table 2 presents the available oracles that $\mathcal{A}$ can query, depending on their set of characteristics.

It can be observed that some adversary types can have access to the same oracles, raising the question of what differentiates them. For example, $\mathcal{A}_7$ and $\mathcal{A}_8$ can both query `Del`, `Obs`, and `ThP`, but neither can access `Cor`. Additionally, they have a similar set of characteristics, the only difference being the time parameter $\mathcal{T}$. This can affect which attacks can be executed by $\mathcal{A}$. For example, $\mathcal{A}_7$ is restricted to attacks that can be executed within a concrete time frame (C), whereas $\mathcal{A}_8$ can observe communications over an extended period, enabling the collection of information for more sophisticated future attacks. Thus, even when adversaries have access to the same oracles, differences in their characteristics can significantly influence their attack capabilities, which may also vary across targeted systems.

Table 2. Ability of different adversaries to query oracles.

$\mathcal{A}$	Characteristics			Del	Cor	Obs	ThP
	$\mathcal{RS}$	$\mathcal{CC}$	$\mathcal{T}$				
1	Ex	N	C	✓	✗	✗	✓
2	Ex	N	As	✓	✗	✗	✓
3	Ex	N	It	✓	✗	✗	✓
4	Ex	Y	C	✓	✓	✗	✓
5	Ex	Y	As	✓	✓	✗	✓
6	Ex	Y	It	✓	✓	✗	✓
7	Ex^+	N	C	✓	✗	✓	✓
8	Ex^+	N	As	✓	✗	✓	✓
9	Ex^+	N	It	✓	✗	✓	✓
10	Ex^+	Y	C	✓	✓	✓	✓
11	Ex^+	Y	As	✓	✓	✓	✓
12	Ex^+	Y	It	✓	✓	✓	✓
13	In	N	C	✓	✗	✓	✓
14	In	N	As	✓	✗	✓	✓
15	In	N	It	✓	✗	✓	✓
16	In	Y	C	✓	✓	✓	✓
17	In	Y	As	✓	✓	✓	✓
18	In	Y	It	✓	✓	✓	✓

✓—an adversary can query the oracle; ✗—an adversary cannot query the oracle.

Also, during an attack, the adversary $\mathcal{A}$ has a certain probability of success. If there are no specific data and conditions that can enhance this probability, then $\mathcal{A}$ can succeed with probability equal to some constant c. If some additional useful information is provided, this probability can increase by ϵ and become $c + \epsilon$. In other words, this ϵ is an advantage that is achieved by $\mathcal{A}$. For our study, the advantage is defined as follows:

Definition 2. *Let* Π *be an Access Control, Authentication, Rights or Computation delegation protocol, then the advantage of* $\mathcal{A}$ *is defined as*

$$Adv_{\Pi}^{\mathsf{G}}(\mathcal{A}) := \Pr[\mathsf{G}(\mathcal{A}) \to 1]$$
$$\textit{for } \mathsf{G} \in \{\mathsf{AC}, \mathsf{AD}, \mathsf{RD}, \mathsf{CD}\},$$

where Pr *is a probability to succeed,* AC *is an Access Control Delegation,* AD *is an Authentication Delegation,* RD *is a Rights Delegation, and* CD *is a Computation Delegation game (see Section 4).*

4. Formalisation of the Security Properties

In this section, mathematical formalisations of CIA security properties are introduced (see Section 3.2) for each application domain of delegation defined in Section 2 with respect to the adversary model from Section 3. All formalisations are represented as security games:

- AC is an Access Control/Authorisation delegation game.
- AD is an Authentication delegation game.
- RD is a Rights delegation game.
- CD is a Computation delegation game.

An adversary $\mathcal{A}$ is considered to win the security game if they successfully violate the targeted security property (confidentiality, integrity, or availability).

In order to be able to provide mathematical formalisations and clearly define the required elements, the following collections are introduced:

- $PL := \{\mathsf{id} = 0, 1, \ldots \mid \mathcal{P}_{\mathsf{id}}\}$ is a list of all system participants.
- $RL := \{\mathsf{i} = 0, 1, \ldots \mid \mathcal{R}_{\mathsf{i}}\}$ is a list of all system resources.
- $M \subseteq PL \times RL$ denotes the access matrix. More precisely, if $(\mathsf{id}, \mathsf{i}) \in M$ then party $\mathcal{P}_{\mathsf{id}}$ has access to resource $\mathcal{R}_{\mathsf{i}}$. It contains all system participants.
- $F \subseteq PL$ includes all $\mathcal{P}_{\mathsf{id}}$ which are accessible from outside of a system.
- $H := \{i = 0, 1, \ldots \mid \mathsf{h}_{\mathsf{i}}\}$ includes all elements of a system that are expected in case the system operates without deviations. It can be parties, passwords, messages, etc.
- $L := \{\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i} \in M \mid \mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i})\}$ specifies all valid proofs of rights $\mathcal{RP}$ related to an owner party $\mathcal{P}_{\mathsf{id}}$, a delegate $\mathcal{D}$ with $\mathsf{id}_{\mathcal{D}}$ and a resource $\mathcal{R}_{\mathsf{i}}$ for each party involved in a system.
- $S := \{\mathsf{id} \in M \mid \mathsf{s}_{\mathsf{id}}\}$ contains all secrets of each party in a system.

In all of the models described below, one of the initial steps for an adversary is to receive an access matrix M as input. However, just as in the case of oracles, some adversaries, depending on their characteristics, may not receive M, for example, an adversary with $\mathcal{RS} = Ex$ receives only F.

4.1. Access Control and/or Authorisation Delegation

Assume that $\exists\, \mathsf{id}, \mathsf{i} : (\mathsf{id}, \mathsf{i}) \in M$, then, in the considered application domain, a third party element $\mathcal{TP}_{\mathsf{id}}$ requests from a delegate $\mathcal{D}$ access to a resource $\mathcal{R}_{\mathsf{i}}$ provided by an RC system. $\mathcal{D}$ replies with a token t. Using t, $\mathcal{TP}_{\mathsf{id}}$ can access desired $\mathcal{R}_{\mathsf{i}}$.

The task of an adversary $\mathcal{A}$ is to disrupt the normal operation of the system and achieve their goal of violating one or more CIA properties. To model this process, a security game described in Definition 3 is introduced.

Definition 3. *Let* Π *be an access control or authorisation protocol, and* AC *be the following experiment:*

1. *Initializing M, F, H, S.*
2. $\mathcal{A}$ *receives as input the access matrix M or F.*
3. $\mathcal{A}$ *is assigned identifier* $\mathsf{id}_{\mathcal{A}}$.

4. $\mathcal{A}$ *can query the following oracles:*

$$\{\mathsf{t}, \perp\} \leftarrow \texttt{Del}(\mathsf{id}, \mathsf{i}),$$
$$\{\mathsf{s}, \perp\} \leftarrow \texttt{Cor}(\mathsf{id}), \textit{ and}$$
$$\{\mathsf{ts}, \perp\} \leftarrow \texttt{Obs}(\mathsf{id}),$$

where id *is an identifier of a protocol party* $\mathcal{TP}_{\mathsf{id}}$ *which wants to obtain access to an RC system resource* $\mathcal{R}_{\mathsf{i}}$.

5. $\mathcal{A}$ *wins if any of the following cases hold:*
   - *Confidentiality:* $\mathcal{A}$ *outputs a token* t *and a resource identifier* i*, such that*
     (1) $\mathcal{A}$ *is not allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M*, but*
     (2) $\mathcal{D}$ *grants* $\mathcal{A}$ *access to* $\mathcal{R}_{\mathsf{i}}$ *when provided with* t.
   - *Integrity:* $\mathcal{A}$ *outputs a party identifier* id*, a resource identifier* i*, and a modified item* $\mathsf{h}_{\mathcal{A}}$ *such that*
     (1) *there is a third party* $\mathcal{TP}_{\mathsf{id}}$ *that is allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M*, and*
     (2) $\mathcal{A}$ *is not allowed to access to* $\mathcal{R}_{\mathsf{i}}$ *according to* M*, but*
     (3) $\exists \mathsf{h}_{\mathcal{A}}$ *that does not match its corresponding item* $\mathsf{h} \in H$.
   - *Availability:* $\mathcal{A}$ *outputs an identifier* id *indicating party* $\mathcal{TP}_{\mathsf{id}}$ *and a resource identifier* i*, such that*
     (1) $\mathcal{TP}_{\mathsf{id}}$ *has access to* $\mathcal{R}_{\mathsf{i}}$ *according to* M*, but*
     (2) *access using a valid token* t *is not granted.*

4.2. Authentication Delegation

Assume that $\exists\, \mathsf{id}, \mathsf{i} : (\mathsf{id}, \mathsf{i}) \in M$, then, in this application domain, a party $\mathcal{P}_{\mathsf{id}}$ included in an RC system requests from a delegate $\mathcal{D}$ to authenticate against a third party $\mathcal{TP}$ on behalf of $\mathcal{P}_{\mathsf{id}}$, in order to $\mathcal{P}_{\mathsf{id}}$ grants access to $\mathcal{R}_{\mathsf{i}}$. In case of successful authentication, $\mathcal{TP}$ sends to $\mathcal{D}$ a token t such that $\mathcal{P}_{\mathsf{id}}$ is allowed to access desired $\mathcal{R}_{\mathsf{i}}$.

An adversary $\mathcal{A}$ targets the system elements in order to violate CIA properties. To model this process, a security game described in Definition 4 is introduced.

Definition 4. *Let* Π *be an authentication delegation protocol, and* AD *be the following experiment:*

1. *Initialising* M, F, H, S.
2. $\mathcal{A}$ *receives as input the access matrix* M *or* F.
3. $\mathcal{A}$ *is assigned identifier* $\mathsf{id}_{\mathcal{A}}$.
4. $\mathcal{A}$ *can query the following oracles:*

$$\{\mathsf{t}, \perp\} \leftarrow \texttt{Del}(\mathsf{id}, \mathsf{i}),$$
$$\{\mathsf{s}, \perp\} \leftarrow \texttt{Cor}(\mathsf{id}), \textit{ and}$$
$$\{\mathsf{ts}, \perp\} \leftarrow \texttt{Obs}(\mathsf{id}),$$

where id *identifies an RC system party* $\mathcal{P}_{\mathsf{id}}$ *which wants to be authenticated to interact with resource* $\mathcal{R}_{\mathsf{i}}$ *of the third party* $\mathcal{TP}$.

5. $\mathcal{A}$ *wins if any of the following cases hold:*
   - *Confidentiality:* $\mathcal{A}$ *outputs a resource identifier* i *and token* t*, such that*
     (1) $\mathcal{A}$ *is not allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M*, but*
     (2) $\mathcal{TP}$ *grants* $\mathcal{A}$ *access to* $\mathcal{R}_{\mathsf{i}}$ *when provided with* t.
   - *Integrity:* $\mathcal{A}$ *outputs a party identifier* id*, a resource identifier* i*, a token* t*, and a modified item* $\mathsf{h}_{\mathcal{A}}$ *such that*

(1) $\mathcal{P}_{\mathsf{id}}$ *is allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M *with provided token* t, *and*
(2) $\mathcal{A}$ *is not allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M, *but*
(3) $\exists \mathsf{h}_{\mathcal{A}}$ *which does not match corresponding item* $\mathsf{h} \in H$.

- *Availability:* $\mathcal{A}$ *outputs a party identifier* id *and a resource identifier* i, *such that*
  (1) $\mathcal{P}_{\mathsf{id}}$ *is allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M, *but*
  (2) $\mathcal{TP}$ *does not grants* $\mathcal{P}_{\mathsf{id}}$ *access to* $\mathcal{R}_{\mathsf{i}}$ *when provided with* t.

4.3. Rights Delegation

Assume that $\exists\, \mathsf{id}, \mathsf{i} : (\mathsf{id}, \mathsf{i}) \in M$ and $\exists\, \mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i}) \in L$, then, according to right delegation scenario, a party $\mathcal{P}_{\mathsf{id}}$ (RC system) possesses some kind of rights related to a resource $\mathcal{R}_{\mathsf{i}}$ owned by a third party $\mathcal{TP}$. A delegate $\mathcal{D}$ wants to access $\mathcal{R}_{\mathsf{i}}$ and in order to be able to do it, it requests the rights from $\mathcal{P}_{\mathsf{id}}$. In turn, $\mathcal{P}_{\mathsf{id}}$ sends a $\mathcal{RP} = \mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i})$ to $\mathcal{D}$, so it can request access to $\mathcal{R}_{\mathsf{i}}$ from $\mathcal{TP}$ and interact with it on its own.

The goal of an adversary $\mathcal{A}$ is to win the security game described in Definition 5, such that winning ensures that the confidentiality, integrity, and/or availability properties are violated.

Definition 5. *Let* Π *be a rights delegation protocol, and* RD *be the following experiment:*

1. *Initialising* M, F, H, L, S.
2. $\mathcal{A}$ *receives as input the access matrix* M *or* F.
3. $\mathcal{A}$ *is assigned identifier* $\mathsf{id}_{\mathcal{A}}$.
4. $\mathcal{A}$ *can query the following oracles:*

$$\{\mathsf{t}, \perp\} \leftarrow \mathtt{ThP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i}, \mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i})),$$
$$\{\mathsf{s}, \perp\} \leftarrow \mathtt{Cor}(\mathsf{id}), \text{ and}$$
$$\{\mathsf{ts}, \perp\} \leftarrow \mathtt{Obs}(\mathsf{id}),$$

   where id *identifies an RC system party* $\mathcal{P}_{\mathsf{id}}$ *which transfers its rights related to resource* $\mathcal{R}_{\mathsf{i}}$ *owned by* $\mathcal{TP}$, $\mathsf{id}_{\mathcal{D}}$ *identifies a delegate* $\mathcal{D}$ *which obtains rights by possessing proof of rights* $\mathcal{RP}$ *from* $\mathcal{P}_{\mathsf{id}}$.
5. $\mathcal{A}$ *wins if any of the following cases hold:*
   - *Confidentiality:* $\mathcal{A}$ *outputs a resource identifier* i *and a token* t, *such that*
     (1) $\mathcal{A}$ *is not allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M, *and*
     (2) $\mathcal{A}$ *with* $\mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{A}}, \mathsf{i})$ *is not allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* L, *but*
     (3) $\mathcal{TP}$ *grants* $\mathcal{A}$ *access to* $\mathcal{R}_{\mathsf{i}}$ *when provided with* t *and* $\mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{A}}, \mathsf{i})$.
   - *Integrity:* $\mathcal{A}$ *outputs a resource identifier* i, *token* t, *and a modified item* $\mathsf{h}_{\mathcal{A}}$ *such that*
     (1) $\mathcal{P}_{\mathsf{id}}$ *has access to* $\mathcal{R}_{\mathsf{i}}$, *and*
     (2) $\mathcal{A}$ *is not allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M, *and*
     (3) $\mathcal{A}$ *with* $\mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{A}}, \mathsf{i})$ *is not allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* L, *but*
     (4) $\exists \mathsf{h}_{\mathcal{A}}$ *does not match corresponding item* $\mathsf{h} \in H$.
   - *Availability:* $\mathcal{A}$ *outputs a resource identifier* i *and token* t, *such that*
     (1) $\mathcal{P}_{\mathsf{id}}$ *is allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* M, *and*
     (2) $\mathcal{D}$ *with* $\mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i})$ *is allowed to access* $\mathcal{R}_{\mathsf{i}}$ *according to* L, *but*
     (3) $\mathcal{TP}$ *does not grants* $\mathcal{D}$ *access to* $\mathcal{R}_{\mathsf{i}}$ *when provided with* t *and* $\mathcal{RP}(\mathsf{id}, \mathsf{id}_{\mathcal{D}}, \mathsf{i})$.

4.4. Computation Delegation

Assume that $\mathsf{id} \in M$, then in the discussed application domain of delegation, an RC system $\mathcal{P}_{\mathsf{id}}$ delegates costly computations m to a delegate $\mathcal{D}$. $\mathcal{D}$ processes the request and replies with m^*.

An adversary $\mathcal{A}$ tries to obtain secrets of $\mathcal{P}_{\mathsf{id}}$ or $\mathcal{D}$ in order to win the security game.

Definition 6. *Let* Π *be a Computation delegation protocol, and* CD *be the following experiment:*

1. *Initialising M, F, H, S.*
2. $\mathcal{A}$ *receives as input the access matrix M or F.*
3. $\mathcal{A}$ *is assigned identifier* $\mathsf{id}_{\mathcal{A}}$.
4. $\mathcal{A}$ *can query the following oracles:*

$$\{\mathsf{m}^*, \perp\} \leftarrow \texttt{Del}(\mathsf{id}, \mathsf{m}),$$
$$\{\mathsf{s}, \perp\} \leftarrow \texttt{Cor}(\mathsf{id}), \textit{ and}$$
$$\{\mathsf{ts}, \perp\} \leftarrow \texttt{Obs}(\mathsf{id}),$$

   where id *identifies an RC system party* $\mathcal{P}_{\mathsf{id}}$, m *is an unprocessed message and* m^* *is a processed message by a delegate* $\mathcal{D}$*, e.g., encrypted or decrypted.*
5. $\mathcal{A}$ *wins if any of the following cases hold:*
   - *Confidentiality:* $\mathcal{A}$ *outputs a party identifier* id *and a secret* s*, such that*
     (1) $\mathcal{A}$ *is not* $\mathcal{P}_{\mathsf{id}}$ *requested* $\mathcal{D}$ *(*$\mathsf{id}_{\mathcal{A}} \neq \mathsf{id}$*), but*
     (2) s *belongs to* $\mathcal{P}_{\mathsf{id}}$.
   - *Integrity:* $\mathcal{A}$ *outputs a party identifier* id*, a secret* s *and a modified item* $\mathsf{h}_{\mathcal{A}}$ *such that*
     (1) $\mathcal{P}_{\mathsf{id}}$ *legitimately belongs to the interaction process, and*
     (2) s *belongs to* $\mathcal{P}_{\mathsf{id}}$*, but*
     (3) $\exists \mathsf{h}_{\mathcal{A}}$ *does not match corresponding item* $\mathsf{h} \in H$.
   - *Availability:* $\mathcal{A}$ *outputs a party identifier* id *and a secret* s*, such that*
     (1) $\mathcal{P}_{\mathsf{id}}$ *legitimately belongs to the interaction process, and*
     (2) s *belongs to* $\mathcal{P}_{\mathsf{id}}$*, but*
     (3) $\mathcal{P}_{\mathsf{id}}$ *obtains either no result for its request or an incorrect one.*

5. Security Evaluation of Existing Protocols

In particular, we consider investigating whether the delegation approaches identified in the literature (Appendix A) can be shown to be secure under the formed definitions of Section 4. In this section, the robustness of these delegation solutions is qualitatively assessed against three types of adversaries aiming to violate confidentiality, integrity, and availability.

5.1. Adversary Types

As noted earlier, 18 types of adversaries (see Section 3.3) can be defined by combining the possible characteristics listed in Table 1. In order to provide a detailed illustrative example, we focus only on the three most representative and distinct types of adversaries:

$\mathcal{A}_{weak}$: An adversary belonging to this type is a "weak" one. They are external, have no corruption capability, and are able to perform attacks feasible within a concrete (typically short) time interval. $\mathcal{A}_{weak}$ can query the following oracles: `Del`, `ThP` (see Table 2 (1)).

$\mathcal{A}_{middle}$: Adversaries in this group can be described as "medium" ones. They have External+ access to the system; hence, they can observe the communication between

parties but have no corruption capability. However, $\mathcal{A}_{middle}$ may have accomplices within the system who may have a corruption capability. Their position allows more sophisticated attacks than $\mathcal{A}_{weak}$. $\mathcal{A}_{middle}$ can query the following oracles: `Del`, `Obs`, `ThP` (see Table 2 (8)).

$\mathcal{A}_{strong}$: When an adversary is categorised as "strong", it is assumed that they have direct access to the system, acting as insiders with full corruption capability. Combined with unlimited time, this enables them to carry out the most resource-intensive attacks. $\mathcal{A}_{strong}$ can query the following oracles: `Del`, `Cor`, `Obs`, `ThP` (see Table 2 (18)).

5.2. Process and Results of Security Evaluation

In this section, the approaches presented in the papers listed in Table A1 are evaluated to determine whether they are likely to be secure against the adversaries introduced above. Due to the large number of publications, we are not able to provide full formal proofs or attacks for each individual paper. Rather, we give our perspective on whether a construction could be proven secure with some effort or whether attacks exist. Thus, later in this section, a detailed analysis of one approach from each application domain is shown. A summary of the analysis for each paper included in this SoK is provided in Table A2.

5.2.1. Access Control and/or Authorisation Delegation

In this domain, the group-oriented access control security mechanism based on DTLS presented by Park and Park (see Section 2.1, Figure 3) is examined. According to the Definition 3, $\mathcal{A}_{weak}$ initially receives as an input list F identified parties which are remotely reachable by $\mathcal{A}_{weak}$. $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ receive as input the access matrix M; hence, they are aware of all participants of the system, and their legitimate access.

In this application domain, `ThP` is not available; therefore, it is assumed that $\mathcal{A}_{weak}$ can query only `Del` and interact directly with $\mathcal{D}$. In order to violate the confidentiality and integrity of any system participant $\mathcal{TP}$, $\mathcal{A}_{weak}$ has to obtain its secret `s` and perform authorisation pretending to be $\mathcal{TP}$. However, as $\mathcal{A}_{weak}$ does not have the corruption capability, they cannot defraud the target client acting as $\mathcal{TP}$ to obtain its `s` and alter the associated resources. Hence, the given system can be proven secure against $\mathcal{A}_{weak}$ in terms of confidentiality and integrity. Considering the availability of the system, $\mathcal{A}_{weak}$ is able to disrupt system functionality by exploiting the single point of failure (SPoF) vulnerability via performing a successful denial of service (DoS) attack against the SP acting as $\mathcal{D}$, sending multiple access requests.

In addition to `Del`, $\mathcal{A}_{middle}$ can query `Obs`. This allows $\mathcal{A}_{middle}$ to eavesdrop on the communication; however, due to using DTLS, confidentiality remains secure. However, having Ex^{+} position relating to the system, $\mathcal{A}_{middle}$ is potentially able to modify data from sensor devices using allies illegally. Also, by performing DoS attacks against SP, $\mathcal{A}_{middle}$ can violate system availability. Therefore, it can be concluded that this system is not secure against $\mathcal{A}_{middle}$ regarding confidentiality and availability properties, but secure concerning integrity.

$\mathcal{A}_{strong}$ is an insider with access to all available oracles and unlimited time. Thus, they potentially can retrieve secrets `s` of any system participant (e.g., security proxy, clients), alter any data from sensor devices, and disrupt the availability of these parties. Therefore, the given system is not considered secure against this type of adversary in terms of confidentiality, integrity, and availability.

5.2.2. Authentication Delegation

In this application domain, the D2TLS protocol introduced in [22] (see Section 2.2, Figure 4) is examined. According to Definition 4, $\mathcal{A}_{weak}$ initially receives as an input list

F identified parties which are remotely reachable by $\mathcal{A}_{weak}$. $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ receive as input the access matrix M; hence, they are aware of all participants of the system, and their legitimate access.

In this application domain, $\mathcal{A}_{weak}$ is able to query only `Del`. As $\mathcal{A}_{weak}$ does not have corruption capability, they cannot compromise any protocol participants in order to obtain their `s`. Hence, $\mathcal{A}_{weak}$ cannot be authenticated instead of legitimate clients and tamper with their resources $\mathcal{R}$. Based on this, the protocol can be proven secure against $\mathcal{A}_{weak}$ in terms of confidentiality and integrity. Considering the capability of $\mathcal{A}_{weak}$ to violate the availability property, $\mathcal{A}_{weak}$ is able to perform DoS attacks against the SA acting as $\mathcal{D}$ by sending numerous delegation requests. Additionally, DoS attacks against a client during protocol operation can cause its interruption. Therefore, this protocol is not secure against $\mathcal{A}_{weak}$ regarding availability.

$\mathcal{A}_{middle}$ can query not only `Del` but also `Obs`. In the given protocol, in order to be successfully authenticated, the adversary should not only have credentials but also be able to forge the client's signature during run time. We assume that this is likely not feasible even within the asymptotic time available for $\mathcal{A}_{middle}$, and the given protocol is secure against $\mathcal{A}_{middle}$ in terms of confidentiality. In this scenario, if confidentiality is not violated, integrity is not violated either. Attacks on communication channels, such as man-in-the-middle (MitM), also cannot be successful because the presented protocol employs the DTLS protocol, which is based on the TLS protocol that ensures the confidentiality and integrity of information during transmission. Therefore, this protocol is likely secure against $\mathcal{A}_{middle}$ in terms of integrity. Availability of the system can be disrupted by performing DoS attacks against SA and clients.

As the most powerful adversary, insider $\mathcal{A}_{strong}$ has access to all available oracles (`Del`, `Cor`, `Obs`) and also has unlimited time It. These resources allow $\mathcal{A}_{strong}$ to perform spoofing, information disclosure, tampering, repudiation, elevation of privilege, and DoS attacks against clients and the SA. Having enough time, $\mathcal{A}_{strong}$ can spoof a legitimate client and forge its signature in order to perform the authentication process. Also, $\mathcal{A}_{strong}$ can compromise the SA and manipulate its decisions, violating the confidentiality and integrity of the data and the availability of the system.

5.2.3. Rights Delegation

In this domain, the delegation of rights in IoT based on Blockchain technology [23] (see Section 2.3, Figure 5) is discussed. Following Definition 5, $\mathcal{A}_{weak}$ initially receives as an input list F identified parties which are remotely reachable by $\mathcal{A}_{weak}$. $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ receive as input the access matrix M; hence, they are aware of all participants of the system, and their legitimate access. Also, they all can query `ThP`. In this application domain, $\mathcal{A}_{weak}$ has access to two oracles (`Del`, `ThP`). The absence of corruption capability leads to the impossibility of $\mathcal{A}_{weak}$ to obtain any secrets. For example, an attempt to request $\mathcal{RP}$ for $\mathcal{R}$ cannot be successful for unauthenticated $\mathcal{A}_{weak}$, because of recurring validations within the blockchain. Therefore, if $\mathcal{A}_{weak}$ queries the resource manager acting as $\mathcal{TP}$ via `ThP` without a valid $\mathcal{RP}$, `ThP` will return $\perp$. Also, $\mathcal{A}_{weak}$ cannot compromise parties and manipulate available data; hence, the integrity of the data is ensured. In order to violate the availability of the system, $\mathcal{A}_{weak}$ can perform DoS attacks against the resource manager by requesting access to $\mathcal{R}$; however, first, recurring validation of a user prevents illegitimate items from making several requests; second, suspicious amount of requests leads to restrictions of suspicious items. DoS attacks against the buyer acting as $\mathcal{D}$ do not influence system functionality, since $\mathcal{A}_{weak}$ is only able to run attacks during C time, so the buyer can continue its operations after a DoS attack is finished. Summarising the above, it

can be concluded that this system is completely secure from $\mathcal{A}_{weak}$ with respect to all three security goals.

Since $\mathcal{A}_{middle}$ can query `Obs` and hence can observe communication. However, a blockchain-based network and smart contracts prevent the violation of data confidentiality and integrity. Considering the Ex^{+} relation to the system of $\mathcal{A}_{middle}$, they can have accomplices within the system, e.g., the resource manager. Hence, $\mathcal{A}_{middle}$ can compromise resource $\mathcal{R}$ and retrieve some information about the buyer or broker or tamper with their data. Also, corruption of the resource manager and its $\mathcal{R}$ leads to possible incorrect system behaviour, when the legitimate buyer with valid $\mathcal{RP}$ does not have access to the desired $\mathcal{R}$, for instance, if the list of approved users is modified. Therefore, this system is not secure against $\mathcal{A}_{middle}$ regarding all CIA-Triad.

Despite $\mathcal{A}_{strong}$ has more resources and capabilities than $\mathcal{A}_{weak}$ and $\mathcal{A}_{middle}$, it does not give $\mathcal{A}_{strong}$ a significant advantage in the results they can achieve by attacking this system in comparison with others. In order to obtain or manipulate information during the transfer of the right, $\mathcal{A}_{strong}$ should compromise the majority of nodes, which we assume is not possible even considering available It time. Therefore, $\mathcal{A}_{strong}$ can perform similar attacks to $\mathcal{A}_{middle}$, and the system is secure against $\mathcal{A}_{strong}$ with respect to all three security properties.

5.2.4. Computation Delegation

In this domain, the application of our mathematical model on the example of Lightweight Revocable Hierarchical Attribute-Based Encryption for the IoT [15] (see Section 2.4, Figure 6) is presented. Based on Definition 6, $\mathcal{A}_{weak}$ initially receives as an input list F identified parties which are remotely reachable by $\mathcal{A}_{weak}$. $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ receive as input the access matrix M; hence, they are aware of all participants of the system, and their legitimate access. As `ThP` is not available for this application domain, $\mathcal{A}_{weak}$ can query only `Del`. The absence of the capability of corruption does not allow this kind of adversary to acquire any secrets `s` of the system parties and to tamper with information within the system. However, $\mathcal{A}_{weak}$ can perform DoS attacks against the devices of data owners. Hence, the given system can be proven secure against $\mathcal{A}_{weak}$ in terms of confidentiality and integrity, but insecure in terms of availability.

The authors assume that all system elements are trusted and cannot be compromised except for data users, but even they are not able to disclose information and tamper with data. Additionally, all communication channels between system parties are considered secure against confidentiality and integrity violations, except three channels (between domain authorities and data owners, the cloud service provider and data owners, and the cloud service provider and data users) that can be susceptible to eavesdropping. Hence, the adversaries $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ can violate the confidentiality of the system by listening to these three channels, but they are not able to perform attacks against the integrity of the system data. Considering the possibilities of disrupting system availability, we see the potential for $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ to perform DoS attacks against the cloud service provider, causing SPoF. Concluding the above, the given system is not secure against attacks from $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ aimed at the availability property.

6. Discussion

During the analysis of the papers selected for our SoK, the approaches proposed by the authors were evaluated in terms of their resilience to attacks carried out by adversaries with varying capabilities, targeting the fundamental security properties of the system.

Given the extensive number of existing approaches, we provided a detailed security analysis for only four representative ones, one from each application domain (see Section 5).

The remaining evaluations were conducted using the same methodology. A summary of the results is presented in Table A2 and discussed below.

6.1. Access Control and/or Authorisation Delegation

In this domain, all approaches focus on delegating decision-making functions. Specifically, the RC system delegates access control and authorisation to a delegate, which then determines whether a third party is granted access. Most approaches either delegate these functions to a single device or utilise blockchain as a delegate. Additionally, some delegates incorporate monitoring mechanisms to track the activity of third parties and respond accordingly. For secure data transmission, the TLS protocol is predominantly employed.

The overall architecture of protocols related to this domain is illustrated in Figure 2a, and the summarised results of their security evaluation are presented in Figure 7a.

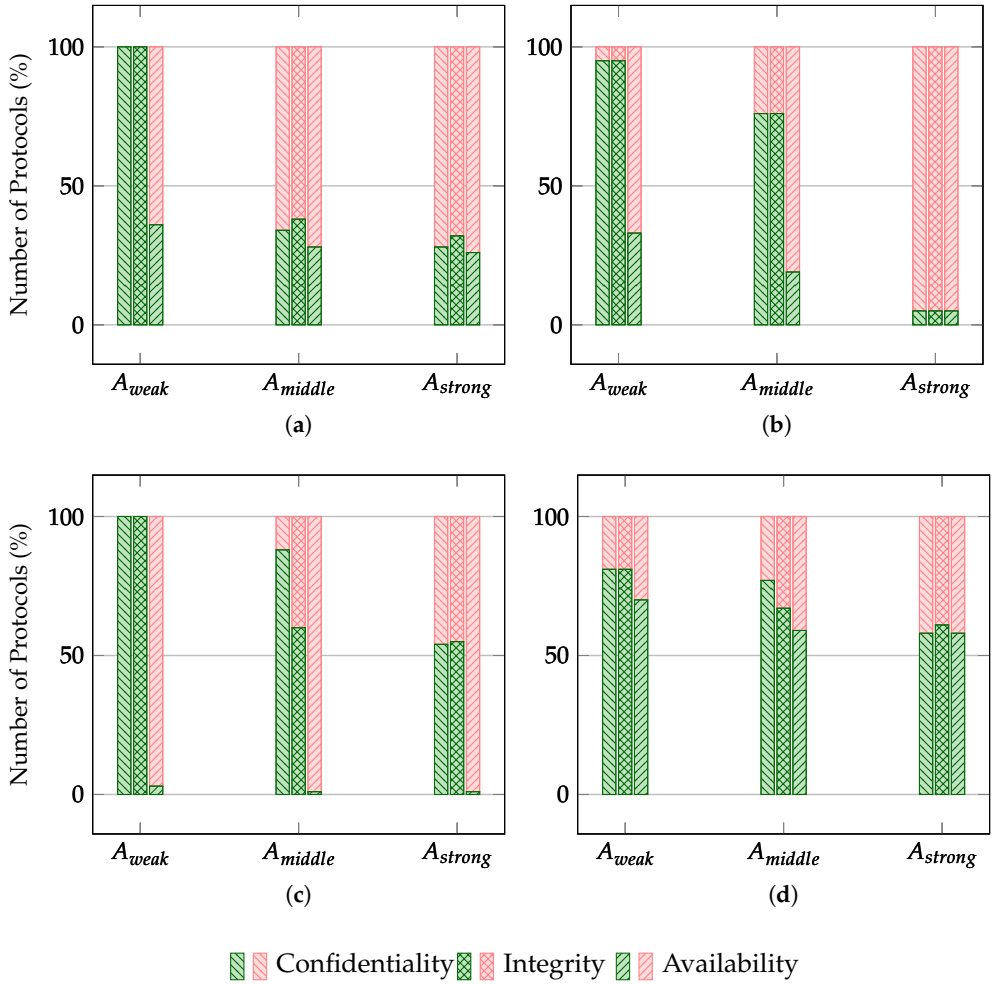


Figure 7. Number of secure (green) and insecure (red) delegation protocols against three types of adversaries in terms of violating confidentiality, integrity, and availability for (**a**) Access Control and/or Authorisation, (**b**) Authentication, (**c**) Rights, and (**d**) Computation delegation application domains.

6.1.1. Confidentiality

It can be observed that all systems in this domain are likely protected against $\mathcal{A}_{weak}$ in terms of confidentiality. $\mathcal{A}_{weak}$ can only observe communications, but cannot corrupt system parties and subsequently is unable to extract secrets. Moreover, many protocols include strong security measures such as encryption, key management, secure transport layers (e.g., DTLS [21,25]), and decentralised architectures (e.g., blockchain [17,26,27]) to protect sensitive data.

When $\mathcal{A}_{middle}$ is considered, a significantly smaller number of protocols are classified as secure. Although $\mathcal{A}_{middle}$, similar to $\mathcal{A}_{weak}$, lacks direct corruption capabilities, they may have accomplices within the system who assist them in obtaining sensitive data. These internal allies may potentially exploit vulnerabilities in access control mechanisms or gain direct access to cryptographic keys or secret information. For example, some protocols [25,28–30] are vulnerable to such internal threats, because $\mathcal{A}_{middle}$'s accomplices with legitimate access privileges may bypass protection layers or misuse their access to retrieve encrypted data. In contrast, blockchain-based protocols [26,31–33], which rely on immutable ledgers, provide stronger confidentiality guarantees in the presence of internal threats. They use cryptographic validation and distributed consensus, making it significantly more difficult for an insider to manipulate or access sensitive data undetected.

As $\mathcal{A}_{strong}$ is assumed to be a powerful adversary with extended access to the system and the ability to corrupt or manipulate critical system components, it is expected that more than half of the protocols under consideration are vulnerable. Similar to $\mathcal{A}_{middle}$, most of the affected protocols rely on traditional access control mechanisms, which are more susceptible to insider threats and compromise. In contrast, blockchain-based protocols demonstrate greater resistance due to their decentralised architecture, which makes it significantly more difficult to bypass or manipulate system components, even by insiders.

6.1.2. Integrity

Since $\mathcal{A}_{weak}$ does not have the ability to corrupt system components, the integrity of the data in all protocols remains unaffected.

For $\mathcal{A}_{middle}$, integrity is compromised in many protocols due to internal accomplices who can bypass access controls and potentially tamper with data. Although these protocols rely on encryption, digital signatures, and access control mechanisms, $\mathcal{A}_{middle}$'s accomplices may manipulate these mechanisms because they have privileged access to the system, making such protocols vulnerable to internal tampering. For example, while OAuth 2.0 and DTLS can guarantee integrity against external attacks from A_{weak}, $\mathcal{A}_{middle}$'s accomplices within the system may alter or corrupt data without detection. However, the use of blockchain in protocols prevents even internal accomplices from undetected data alteration, since each modification must be validated by the network, preventing tampering without consensus.

Similar conclusions can be drawn regarding the influence of $\mathcal{A}_{strong}$ on protocol integrity as with $\mathcal{A}_{middle}$. However, since $\mathcal{A}_{strong}$ is more powerful and has broader access to the system, even fewer protocols remain protected. Nevertheless, blockchain-based protocols continue to offer strong resistance. To compromise the integrity of such systems, $\mathcal{A}_{strong}$ would need to control more than 50% of the network, which is highly unlikely. Therefore, blockchain protocols maintain a high level of integrity assurance, even against strong adversaries.

It is logical to assume that, for any adversary, the number of systems protected against confidentiality and integrity violations should be equal, as in the case of $\mathcal{A}_{weak}$. However, for $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$, there are more systems that appear to maintain integrity than confidentiality. The reason for this is that some delegation solutions [32,34] include monitoring mechanisms capable of detecting suspicious activity or data manipulation and responding accordingly. For example, suppose an adversary may gain unauthorised access to data, thus violating confidentiality, without triggering any alarms, as long as the data remains unmodified. However, if the adversary attempts to alter the data, thereby violating integrity, the system's monitoring mechanisms are likely to detect and react to the intrusion.

6.1.3. Availability

When it comes to availability, it is reasonable to assert that the stronger the adversary, the fewer systems are capable of withstanding their attacks. $\mathcal{A}_{weak}$ can succeed primarily by targeting peripheral components of the system, such as users or delegates, through attacks (e.g., DoS) which can be executed from an external position. In many protocols, such attacks do not result in critical system failures and are therefore still considered secure in terms of availability. However, for example, in the healthcare domain [35,36], even minor disruptions of the operation of patient wearable devices, e.g., pulsimeters, can lead to significant damage. In such cases, the system's primary objective is to protect the individual user rather than just the system itself, and therefore, these protocols are considered vulnerable.

In contrast, $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$ are capable of disrupting the operation of critical system components, potentially leading to significant availability issues. However, despite their extensive resources and capabilities, the impact of such adversaries can be mitigated in protocols that incorporate decentralisation and redundancy into the system architecture [33,37]. These design choices enhance fault tolerance and ensure that the system can continue functioning even when individual components are compromised.

6.2. Authentication Delegation

In this domain, all approaches delegate the authentication function to a delegate, which performs the authentication process on behalf of the RC system with respect to the third party. These solutions primarily rely on existing technologies, such as OAuth, digital certificates, and DTLS handshakes, all of which are executed by the delegate.

The overall architecture of protocols related to this domain is illustrated in Figure 2b, and the summarised results of their security evaluation are presented in Figure 7b.

6.2.1. Confidentiality

Most of the protocols in this domain ensure confidentiality against $\mathcal{A}_{weak}$, as they use strong security techniques (e.g., DTLS [22,38], OAuth [39,40], certificates [41], zero-knowledge proofs [19]). Since $\mathcal{A}_{weak}$ can observe the communication but not corrupt it, using proper encryption and secure authentication mechanisms protects the transmitted data.

Considering security against $\mathcal{A}_{middle}$, confidentiality is compromised in several protocols due to $\mathcal{A}_{middle}$'s ability to exploit internal vulnerabilities or weak access controls [39,40,42–44]. Internal accomplices may potentially bypass encryption mechanisms or gain unauthorised access to sensitive data. However, most protocols that include, e.g., DTLS [22,38] or certificates [41] are generally secure against $\mathcal{A}_{middle}$ in terms of confidentiality. These protocols rely on strong authentication mechanisms, secure session management, and encryption to ensure that even if the adversary can observe the communication, they cannot easily access the sensitive data even in the presence of internal threats.

For $\mathcal{A}_{strong}$, confidentiality is compromised across almost all the protocols discussed, as this type of internal adversary has extended control over the system. They can manipulate access control, corrupt encryption keys, or modify communication channels. Because $\mathcal{A}_{strong}$ has access to internal resources, they can bypass most security mechanisms that are effective against external threats. Nevertheless, protocols that employ a decentralised system architecture [45,46] can maintain confidentiality even against such powerful adversaries.

6.2.2. Integrity

In this domain, the number of systems secure in terms of confidentiality is equal to those secure in terms of integrity across all types of adversaries. It can be associated with the absence of any monitoring mechanisms in the evaluated systems. As a result, a violation of confidentiality typically leads to a violation of integrity. For example, if $\mathcal{A}$ manages to capture the user's credentials and authenticate on their behalf to gain access to resources, $\mathcal{A}$ can often also manipulate those resources by impersonating the user. The same logic applies in reverse. If $\mathcal{A}$ cannot illegally authenticate and gain access to resources intended for the user (i.e., cannot violate confidentiality), then they cannot manipulate these resources to compromise integrity either.

Considering the influence of $\mathcal{A}_{weak}$ on system integrity, it can be concluded that $\mathcal{A}_{weak}$ is not able to violate it, as they can only observe the communication without the capability to alter or corrupt it.

Against $\mathcal{A}_{middle}$, integrity remains secure for most of the protocols because they use digital signatures, message authentication codes and hashes to ensure that any unauthorised modifications to data can be detected [41,47,48]. However, some protocols [39,40,42,43] may be vulnerable, because internal $\mathcal{A}_{middle}$'s accomplices could have access to sensitive tokens, session data, or authentication credentials, allowing them to tamper with the data or compromise their integrity.

For $\mathcal{A}_{strong}$, integrity is compromised in most protocols, as this adversary can exploit internal access to directly tamper with or modify data. The ability to manipulate keys, authentication data, or communication channels from within makes it difficult for these protocols to ensure data integrity. However, protocols employing a decentralised system architecture [45,46] demonstrate resistance even against $\mathcal{A}_{strong}$ due to their distributed nature.

6.2.3. Availability

Many protocols in this domain are vulnerable to $\mathcal{A}_{weak}$ in terms of availability. These protocols primarily focus on ensuring confidentiality and integrity, but often lack mechanisms to address availability threats such as DoS attacks. Hence, $\mathcal{A}_{weak}$ can exploit this by launching DoS attacks, overloading system resources, and preventing legitimate users from accessing services [16,41,47,49].

There are even fewer protocols that ensure availability against $\mathcal{A}_{middle}$, as this adversary not only possesses the capabilities of $\mathcal{A}_{weak}$ but can also exploit internal accomplices, who may potentially bypass built-in protection mechanisms against availability threats, such as rate limiting or traffic filtering. The same applies to $\mathcal{A}_{strong}$, which as the most powerful adversary, can exploit both external and internal access. However, the use of decentralised system architectures [46] can effectively mitigate availability attacks, even from the strongest adversaries.

6.3. Rights Delegation

In this domain, RC systems transfer to a delegate rights to use, own, or access specific resources (third party). This is typically achieved either through blockchain technology, which ensures that only authorised participants can acquire these rights, or through public key cryptography, where access is granted via cryptographic keys, possession of which is considered de facto proof of right. The existing approaches often incorporate mechanisms applied to third parties, such as limiting the number of granted access rights or introducing resource redundancy. However, articles in this category rarely address the methods and protocols employed for secure information transmission.

The overall architecture of protocols related to this domain is illustrated in Figure 2c, and the summarised results of their security evaluation are presented in Figure 7c.

6.3.1. Confidentiality

All protocols presented in this domain are secure against $\mathcal{A}_{weak}$, as they incorporate encryption mechanisms that prevent $\mathcal{A}_{weak}$ from extracting any sensitive information through passive observation of the communication.

Most protocols are also secure against $\mathcal{A}_{middle}$. Despite the presence of internal accomplices, several solutions provide strong confidentiality guarantees. For instance, some rely on blockchain-based designs [50–53], while others incorporate encryption-based mechanisms [54,55] that ensure sensitive data can only be decrypted by authorised parties, even if $\mathcal{A}_{middle}$ has internal access. However, a few protocols [56–58] are unable to fully resist internal threats, as in certain scenarios, even relatively weak accomplices may gain access to sensitive information.

Considering $\mathcal{A}_{strong}$, the majority of protocols can resist attacks, as they incorporate data obfuscation or decentralised control mechanisms, making it difficult even for $\mathcal{A}_{strong}$ to access sensitive information [50,53,59–61]. However, some protocols remain vulnerable [62–64], particularly when internal adversaries are able to access delegation tokens or manipulate session data.

6.3.2. Integrity

Evaluating integrity protection, it was found that all protocols are secure against $\mathcal{A}_{weak}$, as this adversary lacks corruption capabilities and is, therefore, unable to tamper with the data.

$\mathcal{A}_{middle}$ faces significant challenges in tampering with data integrity in most of the considered protocols, as these protocols are designed with strong encryption and authentication mechanisms. Many of them are based on blockchain technology, smart contracts, and secure encryption schemes to protect data from unauthorised modification [60,65–67]. However, some protocols may still be vulnerable to $\mathcal{A}_{middle}$'s attacks if internal accomplices are able to tamper with access tokens and thereby influence the delegation process [63,64,68]. The same holds true for $\mathcal{A}_{strong}$. Although this adversary has more advanced capabilities than $\mathcal{A}_{middle}$, they cannot compromise the integrity of systems based on blockchain, as any modification must pass a network-wide validation process. To manipulate the entire network, $\mathcal{A}_{strong}$ would need to control more than 50% of it, which is considered an unlikely scenario.

6.3.3. Availability

Examining the availability property, it is observed that the percentage of systems protected against $\mathcal{A}_{weak}$ in this domain is lower than in the previous two. Most protocols are vulnerable to $\mathcal{A}_{weak}$'s attacks, e.g., DoS, except for a few that employ techniques such as rate limiting, traffic filtering, load balancing, or redundancy mechanisms [23,56,61].

Furthermore, most protocols are also not protected against $\mathcal{A}_{middle}$ and $\mathcal{A}_{strong}$, as both adversaries have the capability to manipulate internal resources, bypass external protections, and disrupt services. Even if the entire system is not compromised, in certain application areas, e.g., healthcare, the availability disruption of even a single device can be critical [56,67,69,70].

6.4. Computation Delegation

In this domain, existing approaches focus on delegating computational tasks that are infeasible or resource-intensive for RC systems to perform independently. These solutions pay considerable attention to data protection during storage and transmission, often employing a combination of techniques such as digital signatures, encryption, and access control mechanisms to restrict data exposure, even among legitimate system participants.

However, some approaches prioritise the organisational aspects of delegation and provide limited details on the specific security technologies employed.

The overall architecture of protocols related to this domain is illustrated in Figure 2d, and the summarised results of their security evaluation are presented in Figure 7d.

6.4.1. Confidentiality

The majority of the protocols in this domain provide confidentiality through security techniques such as encryption, key management, and secure communication protocols, e.g., DTLS. These techniques ensure that even if $\mathcal{A}_{weak}$ tries to intercept the communication, the data remain inaccessible without the appropriate keys or permissions [15,71,72]. However, we have labelled some protocols as not protected against $\mathcal{A}_{weak}$, particularly those that do not mention the use of cryptographic mechanisms, as they are primarily focused on data processing and analytics [73–75]. These protocols might not focus on ensuring confidentiality in terms of encryption or secure data transmission and may be vulnerable to data exposure to $\mathcal{A}_{weak}$ because they do not incorporate sufficient protection mechanisms. The same holds true for $\mathcal{A}_{middle}$. Having accomplices within the system may provide an advantage for $\mathcal{A}_{middle}$ over $\mathcal{A}_{weak}$ only in the case of a few protocols [15,76].

Considering attacks against confidentiality from $\mathcal{A}_{strong}$, it is observed that more than half of the protocols remain resistant [20,71,77,78]. These protocols generally employ architectures that prevent internal adversaries from directly accessing or modifying data, even with full system access. However, several protocols are still vulnerable to $\mathcal{A}_{strong}$, particularly those that focus primarily on data-processing or -management frameworks [73,79] and do not incorporate sufficient security mechanisms to protect data against internal threats

6.4.2. Integrity

Most protocols are secure against $\mathcal{A}_{weak}$ in terms of integrity, as $\mathcal{A}_{weak}$ lacks the ability to tamper with data. However, some protocols do not mention any mechanisms for ensuring data integrity and are therefore classified as insecure [13,80–82].

Considering $\mathcal{A}_{midde}$, it is visible that the majority of discussed protocols are able to resist it in terms of integrity. Most of these protocols incorporate integrity verification measures, e.g., message authentication codes, digital signatures, end-to-end encryption, and hashing to detect and prevent unauthorised data tampering [71,78,83]. However, some protocols do not employ such measures and, hence, may be vulnerable to $\mathcal{A}_{midde}$'s attacks, which can be performed with the assistance of $\mathcal{A}_{midde}$'s accomplices [78,84]. Similar conclusions can be applied to $\mathcal{A}_{strong}$; however, as they have more resources than $\mathcal{A}_{midde}$, a higher number of protocols are vulnerable to their attacks [8,20,85,86].

6.4.3. Availability

When evaluating the availability of the systems, it is observed that the percentage of vulnerable systems is relatively low, less than half of the protocols are vulnerable regarding all three types of adversaries.

As an external adversary, $\mathcal{A}_{weak}$ can perform attacks only on parties that accept requests from outside the system and cause a single point of failure or overload the network and disrupt the system's availability [76,87,88].

$\mathcal{A}_{midde}$ and $\mathcal{A}_{strong}$ have also capabilities to disrupt the system functionality from inside; hence, more protocols are vulnerable to their attacks [89–91], as they can bypass traffic filtering mechanisms.

6.5. Common Vulnerabilities

Analysing the attacks to which systems are vulnerable, several key reasons for confidentiality breaches were identified. First, many systems rely on sensors and resource-constrained IoT nodes that store sensitive information but lack sufficient built-in security. As a result, adversaries with the capability to corrupt internal system components (such as $\mathcal{A}_{middle}$ or $\mathcal{A}_{strong}$) can access sensor data, disclose it, or leverage it for future attacks [28,34,39,47]. Second, user or client confidentiality is often compromised through fraudulent schemes in which users are tricked into voluntarily providing their credentials. This allows adversaries to impersonate legitimate users, effectively performing spoofing attacks. Third, insecure communication channels and transport protocols are another major vulnerability, as they are susceptible to eavesdropping, allowing adversaries to intercept sensitive data during transmission [15,40,62,92].

Integrity violation attacks often occur as a consequence of successful spoofing. Once an adversary has deceptively gained access to a user's resources, they can modify or manipulate those resources by leveraging the user's privileges [21,28,37]. Furthermore, many integrity breaches result from the use of insecure communication channels, enabling the adversary to launch MitM attacks. In addition, sensors are frequent targets of tampering due to their limited protection mechanisms. This allows the adversary to falsify sensor readings, which can have critical implications, particularly in healthcare systems, where accurate data are crucial for patients [42,43,56].

The majority of system availability violations are related to DoS attacks, which are often feasible even for the weakest adversary ($\mathcal{A}_{weak}$) [93,94]. For example, attacking sensors can disrupt the availability of their data. In some cases, this may not lead to critical issues, but in domains such as healthcare, data from devices like heart rate or oxygen monitors are crucial and must be available on demand [86]. More resourceful adversaries, with either indirect (through accomplices) or direct access to the system, are capable of targeting more critical components, e.g., databases or servers, via DoS attacks. Often, such attacks can lead to SPoF, causing a complete system outage. Additionally, powerful adversaries ($\mathcal{A}_{strong}$) that are insiders may be able to restrict legitimate user access depending on their position within the system, thereby compromising availability [85,87,95].

Summarising this section, it can be concluded that systems across all application domains are susceptible to similar types of attacks. The most common issues related to breaches of confidentiality and integrity are caused by the disclosure of credentials by users or clients, often as a result of social engineering or fraudulent schemes. Regarding system availability, the most frequent cause of disruption is a DoS attack targeting critical system components that lack redundancy, resulting in SPoF.

6.6. Proposed Countermeasures and Mitigations

This section is dedicated to the discussion of the countermeasures proposed by the authors of the reviewed papers, which aim to prevent various attacks and ensure the fundamental security properties (CIA).

In order to ensure the confidentiality and integrity of the information, several systems implement the TLS protocol directly [28,30,33,96–98] or use it as a basis for the DTLS handshake protocol [21,22,38,42,47,48,85,99–102]. DTLS not only secures transmitted data and provides strong authentication inherited from TLS, but also helps accelerate system processes. To counter long-term attacks, dynamic monitoring is proposed [103], where the system observes device activity during runtime. Based on this observation, it can detect suspicious behaviour and impose restrictions if necessary. Additionally, various combinations of lightweight cryptographic protocols have been suggested to ensure data protection, each offering specific advantages and trade-offs depending on the application

context [8,15,94,104]. Furthermore, many systems adopt security mechanisms such as cryptographic hashing and multi-factor authentication to enhance data protection. Decentralised architectures, including blockchain-based solutions, are also widely implemented to ensure tamper resistance, transparency, and trust [22,46,49,61,105,106].

According to the results of our analysis, DoS attacks that lead to SPoF pose the greatest risk to system availability. Delegation, by design, helps reduce the success rate of DoS attacks by shifting the adversary's target from a resource-constrained device to a more capable delegate. Since a delegate is assumed to have greater computational and communication resources, it is generally expected to withstand such attacks. However, in practice, a delegate may be more powerful than other devices in the system, but still not strong enough to resist a determined adversary. If an adversary succeeds in corrupting a delegate, this can result in a SPoF scenario that compromises the availability of the entire system. In order to mitigate risks associated with a SPoF, several countermeasures have been implemented in the evaluated systems. These include accepting requests only from already authenticated users [23,34,38,43,45,47,97,101,102], deploying multiple proxies instead of a single delegate to distribute the load and reduce reliance on a single point [20], and implementing decentralised or redundant architectures, often based on blockchain technology [8,32,33,37,45,46,61,107]. These strategies significantly reduce or even eliminate the impact of successful DoS attacks, thereby enhancing system availability. However, despite their undeniable advantages, for example, blockchain-based approaches are not always applicable for resource-constrained devices, which prevents them from being used for typical systems such as smart home, which mostly consists of "weak" devices.

Summarising the results of our research and discussion, the following conclusions are drawn:

- Most existing studies do not provide formalised models of their proposed solutions, with the notable exception of those within the cryptographic delegation application domain.
- The security analysis of the proposed delegation solutions is often either completely absent or limited to a narrow scope, typically considering only a single type of adversary. In most cases, the evaluated adversary is weak and external, while stronger internal threats or more complex attack scenarios are largely overlooked.
- Most of the proposed solutions meet confidentiality and integrity requirements when evaluated against specific types of adversaries. However, they often do not provide sufficient system availability, especially under DoS attacks or in the presence of a potential SPoF.
- Solutions that provide robust and comprehensive security guarantees are frequently tailored for environments with ample computational and network resources. Consequently, their applicability to typical IoT scenarios, e.g., smart home, may be limited, as these scenarios often lack the necessary infrastructure, device density, or processing capabilities required to support such solutions effectively.

7. Potential Future Research Directions

Based on the results of our research, the following potential future research directions in the domain of IoT security delegation may be considered particularly interesting:

Comprehensive and lightweight delegation solutions: Investigate the feasibility of designing delegation-based security frameworks that provide comprehensive protection of confidentiality, integrity, and availability, even in the presence of strong and internal adversaries, while remaining suitable for deployment in small-scale and highly resource-constrained IoT environments.

Formalisation of attacks: Explore whether common attack scenarios targeting delegation mechanisms in IoT systems can be generalised and expressed as formal mathematical models compatible with our security property definitions.
Ensuring security of a delegate: Research techniques to enhance the security of delegates, which are often assumed to be trustworthy and robust components. However, as they frequently serve as main components in delegation models, they become attractive targets for adversaries and may be vulnerable to various attacks.
Delegation in dynamic environments: Design adaptive delegation mechanisms that can respond to real-time contextual factors such as device failure, workload, trust levels, and network conditions, thereby improving both system robustness and efficiency in dynamic IoT environments.
Standardisation and interoperability: Investigate the feasibility of designing interoperable and standardised delegation solutions capable of operating across heterogeneous IoT environments, addressing the current limitations of many existing approaches that are highly domain- or vendor-specific.
Extended property evaluation: Explore the extension of the security evaluation model proposed in this paper to include additional security properties beyond those discussed, in order to support a more comprehensive assessment of system security.

We believe that these research directions provide a solid foundation for future advancements in delegation-based security for IoT systems. Addressing these challenges not only enhances the robustness of existing solutions but also promotes the development of scalable, interoperable, and adaptive frameworks suitable for diverse and resource-constrained IoT environments.

8. Conclusions

In this paper, we performed a comprehensive review of 256 existing solutions that propose delegation-based mechanisms for securing IoT systems. Through this analysis, four main application domains were identified: access control and/or authorisation delegation, authentication delegation, rights delegation, and computation delegation. For each domain, a generalised system architecture was derived based on common patterns observed across the solutions included in the category. Furthermore, a flexible mathematical model of a potential adversary was introduced, along with a formalisation of the confidentiality, integrity, and availability security properties relevant to each domain. These properties were expressed in the form of security games, in which an adversary attempts to win the game by violating the given property. Finally, all considered delegation solutions were evaluated in terms of their robustness against three distinct types of adversaries with respect to the introduced security games.

According to the obtained results, it can be concluded that despite the existence of many delegation approaches ensuring information confidentiality and integrity, the majority remain vulnerable to attacks, which target system availability, particularly those resulting in a single point of failure. Although delegation-based security mechanisms offer clear advantages over non-delegation approaches, especially in supporting resource-constrained IoT devices, there is still considerable room for improvement. Notably, delegation solutions face the dual challenge of securing both the constrained devices and the delegates themselves, which frequently become prime targets for adversaries.

Author Contributions: Conceptualisation, E.G. and S.K.; methodology, E.G. and P.S.; validation, E.G. and F.K.; formal analysis, E.G. and F.K.; investigation, E.G.; data curation, E.G.; writing—original draft preparation, E.G., F.K., P.S. and S.K.; writing—review and editing, E.G., F.K., P.S. and S.K.; visualisation, E.G.; supervision, S.K. All authors have read and agreed to the published version of the manuscript.

Funding: The work was funded by the Bavarian State Ministry of Science and Arts (BayStMWK), under the project "Secure Encapsulation" of the Bavarian Research Association "FORDaySec" (see https://fordaysec.de (accessed on 12 March 2025)) "Security in Everyday Use of Digital Technologies".

Data Availability Statement: No new data were created or analyzed in this study.

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

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
CIA	Confidentiality, Integrity and Availability
TLS	Transport Layer Security
SoK	Systematisation of Knowledge
ACM	Association for Computing Machinery
IEEE	Institute of Electrical and Electronics Engineers
RC	Resource-constrained
DTLS	Datagram Transport Layer Security
SP	Security Proxy
ID	Identification Number
SA	Security Agent
LW-RHABE	Lightweight Revocable Hierarchical Attribute-based Encryption
CA	Central Authority
DA	Domain Authority
CSP	Cloud Service Provider
DoS	Denial-of-Service
MitM	Man-in-the-Middle
SPoF	Single Point of Failure

Appendix A. Methodology for Selecting Papers Suitable for the Review

In this section, the approach used to collect existing publications on delegated IoT security for this survey is described.

Appendix A.1. Selection Procedure

In order to find suitable publications, the following scientific libraries were used: Google Scholar, Semantic Scholar, ACM Digital Library, and IEEE Xplore. Currently, these platforms provide access to more than 203 million papers across diverse research disciplines. Following Kitchenham et al., a keyword query was formulated to identify scientific works relevant to this study [108]:

$$(\text{“}\textit{Internet of Things}\text{”} \,||\, \text{“}\textit{IoT}\text{”}) \\ \wedge \\ (\text{“}\textit{Delegated}\text{”} \,||\, \text{“}\textit{Delegated Security}\text{”} \,||\, \text{“}\textit{Delegation}\text{”}).$$

Additionally, applying the snowballing strategy introduced by Wohlin and Prikladniki [109], the references of the previously identified papers were examined and searched for relevant publications containing additional security models and designs applicable to our study. After collecting the papers retrieved through this process, the next phase was initiated.

In order to establish a consistent standard among the selected papers, all collected papers were filtered based on the following criteria:

Inclusion criteria:

$(IC1)$ A paper provides a unique approach toward the definition, description, or classification of security delegating in IoT systems.

$(IC2)$ A paper presents metrics or security models that allow for explaining or measuring security delegation.

$(IC3)$ A paper introduces a specific approach to security delegation that can be applied in at least one sub-area of IoT.

Exclusion criteria:

$(EC1)$ A paper is not peer-reviewed.

$(EC2)$ A paper does not present a novel security model or design.

A paper is considered relevant if at least one inclusion criterion is met and none of the exclusion criteria apply:

$$(IC1 \vee IC2 \vee IC3) \wedge \overline{(EC1 \vee EC2)} = 1.$$

Appendix A.2. Results of the Selection Procedure

After completing the search phase of the selection procedure, a list of 940 publications was obtained. The filtering process then began with an initial scan to assess whether each publication might be relevant. At this stage, only papers clearly unrelated to our topic were excluded, for example, those whose subject matter did not fall within the IoT domain. As a result, 404 papers remained.

In the second round, all remaining papers were examined to determine whether they met the inclusion or exclusion criteria (see Appendix A.1). Subsequently, each paper was categorised as either relevant or not relevant. Finally, 254 papers were selected for the review.

Table A1 contains all papers retrieved during the selection procedure which are grouped according to the categories identified in Section 2. The *Rights Delegation* category in this table is split into two parts since papers #153-192 focus on Delegated Proof of Stake, Delegated Proof of Authority, etc. While these papers fall under the rights delegation category, they are primarily concerned with consensus protocols. Therefore, although they do involve the delegation of rights, we have chosen to partially highlight them. Special designations used in the table: **Y**—a year of publication, **T**—a type of the paper (**C**onference, **J**ournal), **Cn**—number of citations, **h** is an *h*-index.

Table A1. List of the papers retrieved during the selection procedure.

№	Title	Y	T	Cn	h
	Access Control and/or Authorisation Delegation				
1	Authorisation framework for the Internet-of-Things [110]	2013	C	70	/
2	A DTLS-based security architecture for the Internet of Things [25]	2015	C	24	/
3	A delegated authorisation solution for smart-city mobile applications [97]	2016	C	4	/
4	Access control framework for API-enabled devices in smart buildings [111]	2016	C	18	/
5	An overview on delegated authorisation for CoAP: Authentication and authorisation for … (ACE) [99]	2016	C	8	/
6	Building secure healthcare services using OAuth 2.0 and JSON web token in IOT cloud scenario [30]	2016	C	23	/
7	IoT Delegate: Smart Home Framework for Heterogeneous IoT Service Collaboration [112]	2016	J	15	34
8	IoT-cloud authorisation and delegation mechanisms for ubiquitous sensing and actuation [34]	2016	C	8	/
9	TACIoT: multidimensional trust-aware access control system for the Internet of Things [113]	2016	J	109	102
10	A Community-Driven Access Control Approach in Distributed IoT Environments [114]	2017	J	55	272
11	A model to enable application-scoped access control as a service for IoT using OAuth 2.0 [29]	2017	C	24	/
12	Achievable Multi-Security Levels for Lightweight IoT-Enabled Devices in …Communications [115]	2017	J	24	204
13	ControlChain: Blockchain as a Central Enabler for Access Control Authorisations in the IoT [31]	2017	C	95	/
14	OAuth-IoT: An access control framework for the Internet of Things based on open standards [28]	2017	C	45	/
15	User-centric access control for efficient security in smart cities [116]	2017	C	11	/
16	A Group-Oriented DTLS Handshake for Secure IoT Applications [21]	2018	J	21	102
17	Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT [26]	2018	J	905	149
18	Decentralised IoT Data Management Using BlockChain and Trusted Execution Environment [32]	2018	C	98	/
19	Group-Oriented Range-Bound Key Agreement for Internet of Things Scenarios [117]	2018	J	18	149
20	Heracles: Scalable, Fine-Grained Access Control for Internet-of-Things in Enterprise Environments [118]	2018	C	14	/
21	Validation of an Adaptive Risk-based Access Control Model for the Internet of Things [103]	2018	J	59	/
22	5G-SSAAC: Slice-specific Authentication and Access Control in 5G [119]	2019	C	5	/
23	Blockchain and Structural Relationship-Based Access Control for IoT: A Smart City Use Case [27]	2019	C	6	/
24	Dynamic Multiparty Authentication using Cryptographic Hardware for the Internet of Things [120]	2019	C	3	/
25	Enabling Decentralised Identifiers and Verifiable Credentials for Constrained …Devices … [121]	2019	J	33	4
26	Fine-grained multi-authority access control in IoT-enabled mHealth [36]	2019	J	24	43
27	Policy-based access control for constrained healthcare resources in the context of the Internet of Things [35]	2019	J	47	129
28	Trusted D2D-Based IoT Resource Access Using Smart Contracts [33]	2019	C	7	/
29	A new scalable authentication and access control mechanism for 5G-based IoT [122]	2020	J	29	151
30	Access control for Internet of Things—enabled assistive technologies: … [37]	2020	J	11	/

Table A1. *Cont.*

№	Title	Y	T	Cn	h
31	BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control [123]	2020	J	41	204
32	Droplet: Decentralized Authorisation and Access Control for Encrypted Data Streams [17]	2020	J	30	4
33	Reliable Task Management Based on a Smart Contract for Runtime Verification … [124]	2020	J	34	219
34	User-Managed Access Delegation for Blockchain-driven IoT Services [125]	2020	C	4	/
35	Delegated Device Attestation for IoT [96]	2021	C	1	/
36	A Proxy Signature-Based Swarm Drone Authentication With Leader Selection in 5G Networks [126]	2022	J	10	204
37	Perils and Mitigation of Security Risks of Cooperation in Mobile-as-a-Gateway IoT [18]	2022	C	1	/
38	Securing Smart Home IoT Systems with Attribute-Based Access Control [127]	2022	C	5	/
39	A Blockchain-Based Framework for Scalable and Trustless Delegation of Cyber Threat Intelligence [106]	2023	C	1	/
40	An access control scheme for distributed IoT based on adaptive trust evaluation and blockchain [128]	2023	J	2	5
41	An extended Attribute-based access control with controlled delegation in IoT [129]	2023	J	1	54
42	Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation … [130]	2023	J	5	149
43	Multi-tenant, Decentralized Access Control for the Internet of Things [131]	2023	C	0	/
44	Multilevel Subgranting by Power of Attorney and OAuth Authorisation Server … [132]	2023	J	0	149
45	Smart Blockchain-based Authorisation for Social Internet of Things [12]	2023	C	0	/
46	Flexible and Fine-grained Access Control for EHR in Blockchain-assisted E-healthcare Systems [133]	2024	J	0	149
47	Privacy-Preserving Fine-Grained Data Sharing With Dynamic Service for the Cloud-Edge IoT [134]	2025	C	2	/
	Authentication Delegation				
48	A Simple Delegation Scheme for RFID Systems (SiDeS) [49]	2007	C	14	/
49	End-to-end transport-layer security for Internet-integrated sensing applications with … [47]	2013	J	11	9
50	Towards viable certificate-based authentication for the Internet of Things [41]	2013	C	91	/
51	Delegation-based authentication and authorisation for the IP-based Internet of Things [100]	2014	C	102	/
52	Lightweight secure communication for CoAP-enabled Internet of Things using delegated DTLS … [38]	2014	C	21	/
53	An OAuth based authentication mechanism for IoT networks [39]	2015	C	39	/
54	ESSE: Efficient Secure Session Establishment for Internet-Integrated Wireless Sensor Networks [101]	2015	J	20	65
55	IoT-OAS: An OAuth-Based Authorisation Service Architecture for Secure Services in IoT Scenarios [40]	2015	J	174	145
56	SEA: A Secure and Efficient Authentication and Authorisation Architecture for IoT-Based Healthcare … [42]	2015	J	222	/
57	Toward a Lightweight Authentication and Authorisation Framework for Smart Objects [135]	2015	J	111	251
58	An Authentication and Key Management Mechanism for Resource Constrained Devices … [45]	2017	J	22	219
59	IoT–Cloud collaboration to establish a secure connection for lightweight devices [48]	2017	J	25	98

Table A1. *Cont.*

№	Title	Y	T	Cn	h
60	Secure Service Proxy: A CoAP(s) Intermediary for a Securer and Smarter Web of Things [102]	2017	J	9	219
61	BF-IoT: Securing the IoT Networks via Fingerprinting-Based Device Authentication [43]	2018	C	32	/
62	A DPN (Delegated Proof of Node) Mechanism for Secure Data Transmission in IoT Services [136]	2019	J	20	51
63	D2TLS: delegation-based DTLS for cloud-based IoT services [22]	2019	C	6	/
64	Privacy-preserving delegable authentication in the Internet of Things [16]	2019	C	11	/
65	Master-slave chain based trusted cross-domain authentication mechanism in IoT [46]	2020	J	31	129
66	Cost-Efficient Anonymous Authentication Scheme Based on Set-Membership Zero-Knowledge Proof [14]	2023	C	0	/
67	Leakage of Authorisation-Data in IoT Device Sharing: New Attacks and Countermeasure [44]	2023	J	0	92
68	Zero-Knowledge Proofs based delegation authentication for Industrial Internet of Things … [19]	2023	C	0	/
	Rights Delegation				
69	Capability-based access control delegation model on the federated IoT network [93]	2012	J	9	9
70	A Hot-topic based Distribution and Notification of Events in Pub/Sub Mobile Brokers [137]	2013	J	8	/
71	A capability-based security approach to manage access control in the Internet of Things [57]	2013	J	299	116
72	Distributed Capability-based Access Control for the Internet of Things [138]	2013	J	178	9
73	DCapBAC: embedding authorisation logic into smart things through ECC optimisations [68]	2016	J	125	54
74	FairAccess: a new Blockchain?based access control framework for the Internet of Things [50]	2016	J	650	58
75	Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things [139]	2017	J	173	35
76	Offline Trusted Device and Proxy Architecture Based on a new TLS Switching Technique [92]	2017	C	1	/
77	RSPP: A reliable, searchable and privacy-preserving e-healthcare system … [140]	2017	C	31	/
78	ViotSOC: Controlling Access to Dynamically Virtualized IoT Services using Service Object Capability [141]	2017	C	4	/
79	BlendCAC: A BLockchain-Enabled Decentralized Capability-Based Access Control for IoTs [52]	2018	C	103	/
80	BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control … [51]	2018	J	121	32
81	Blockchain-Based IoT-Cloud Authorisation and Delegation [142]	2018	C	41	/
82	CapChain: A Privacy Preserving Access Control Framework Based on Blockchain … [53]	2018	C	29	/
83	IoTChain: A blockchain security architecture for the Internet of Things [65]	2018	C	146	/
84	Pragmatic approach using OAuth mechanism for IoT device authorisation in cloud [62]	2018	C	2	/
85	A Novel Entitlement-based Blockchain-enabled Security Architecture for IoT [143]	2019	C	17	/
86	A Secure Key Delegation Mechanism for Fog Networking [144]	2019	C	4	/
87	Access Control Model Based on Dynamic Delegations and Privacy in a Health System … [63]	2019	C	0	/
88	Blockchain Based Fine-Grained and Scalable Access Control for IoT Security and Privacy [145]	2019	C	8	/

Table A1. *Cont.*

№	Title	Y	T	Cn	h
89	Blockchain based permission delegation and access control in Internet of Things (BACI) [146]	2019	J	70	112
90	CA-ADP: Context-Aware Authorisation and Delegation Protocol for IoT-based healthcare smart systems [56]	2019	C	2	/
91	Context-aware pseudonymisation and authorisation model for IoT-based smart hospitals [147]	2019	J	11	64
92	DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA … [148]	2019	C	18	/
93	Design and implementation of a secure and flexible access-right delegation for … [58]	2019	J	21	151
94	Tc-PEDCKS: Towards time controlled public key encryption with … keyword search … [149]	2019	J	22	129
95	WAVE: A Decentralized Authorisation Framework with Transitive Delegation [61]	2019	J	68	4
96	A Flexible Privacy-Preserving Data Sharing Scheme in Cloud-Assisted IoT [150]	2020	J	38	149
97	Ciphertext-Policy Hierarchical Attribute-Based Encryption Against Key-Delegation Abuse … [64]	2020	J	9	204
98	Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things [151]	2020	J	67	219
99	On the Design of a Flexible Delegation Model for the Internet of Things Using Blockchain [23]	2020	J	33	170
100	On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation [152]	2020	J	42	149
101	Proxy re-encryption with equality test for secure data sharing in IoT-based healthcare systems [69]	2020	J	11	/
102	Towards Decentralized IoT Updates Delivery Leveraging Blockchain and Zero-Knowledge Proofs [153]	2020	C	6	/
103	xDBAuth: Blockchain Based Cross Domain Authentication and Authorisation Framework for IoT [154]	2020	J	56	204
104	A Secure and Privacy-Preserving Machine Learning Model Sharing Scheme for Edge-Enabled IoT [155]	2021	J	13	204
105	An Efficient Access Control Scheme With Outsourcing and Attribute Revocation … [156]	2021	J	17	204
106	Blockchain-Based DNS Root Zone Management Decentralisation for Internet of Things [157]	2021	J	5	73
107	Cost-Effective Proxy Signcryption Scheme for Internet of Things [158]	2021	J	3	42
108	Entitlement-Based Access Control for Smart Cities Using Blockchain [159]	2021	J	10	219
109	FogFrame: a framework for IoT application execution in the fog [160]	2021	J	15	37
110	On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things [66]	2021	J	24	149
111	A Bidirectional Trust Model for Service Delegation in Social Internet of Things [161]	2022	J	6	4
112	A Novel MQTT 5.0-Based Over-the-Air Updating Architecture Facilitating Stronger Security [162]	2022	J	10	62
113	A Proxy Re-Encryption Approach to Secure Data Sharing in the IoT Based on Blockchain [60]	2022	J	58	98
114	A Study on Vehicle Monitoring Service Using Attribute-Based Security Scheme … [163]	2022	J	1	101
115	A Traceable Capability-based Access Control for IoT [164]	2022	J	3	51
116	An Efficient Blockchain-Based Hierarchical Data Sharing for Healthcare Internet of Things [67]	2022	J	39	170

Table A1. *Cont.*

№	Title	Y	T	Cn	h
117	An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach … [165]	2022	J	95	219
118	Attribute-Based Data Sharing in Smart Healthcare Environment [70]	2022	C	0	/
119	BlueSky: Combining Task Planning and Activity-Centric Access Control for Assistive Humanoid Robots [166]	2022	C	2	/
120	Burn After Reading: Adaptively Secure Puncturable Identity-Based Proxy Re-Encryption Scheme … [167]	2022	J	9	149
121	ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things [168]	2022	J	10	204
122	DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System [169]	2022	J	4	204
123	Delegated Anonymous Credentials With Revocation Capability for IoT …(*DANCIS*) [170]	2022	J	2	149
124	Dynamic Delegation-based Privacy Preserving in IoT Architectures [171]	2022	C	4	/
125	EDTP: Energy and Delay Optimized Trajectory Planning for UAV-IoT Environment [172]	2022	J	18	150
126	Efficient multi-tier, multiple entry PBFT consensus algorithm for IoT [173]	2022	C	3	/
127	How to divide a permission token in the delegation process of blockchain-based access control for IoT [174]	2022	C	0	/
128	Joint Content and Radio Access for the IoT: A Smart-Contract-Based Trusted Framework [59]	2022	J	2	149
129	Monitoring Provenance of Delegated Personal Data with Blockchain [175]	2022	C	2	/
130	Mutual-contained access delegation scheme for the Internet of Things user services [176]	2022	J	29	45
131	Omnes pro uno: Practical Multi-Writer Encrypted Database [177]	2022	J	21	4
132	Redefining the Trust Model for the Internet of Everything in the 6G era [178]	2022	C	1	/
133	Reliable Application Layer Routing Using Decentralized Identifiers [9]	2022	J	1	49
134	SEDIMENT: An IoT-device-centric Methodology for Scalable 5G Network Security [179]	2022	C	0	/
135	Scalable IoT Sensing Systems With Dynamic Sinks [180]	2022	J	3	149
136	Secure Trust-Based Delegated Consensus for Blockchain Frameworks … [181]	2022	J	7	204
137	Secure and Efficient Certificate-Based Proxy Signature Schemes for Industrial Internet of Things [182]	2022	J	11	98
138	Security and Privacy Service Level Agreement composition for Internet of Things systems … [183]	2022	J	2	84
139	Verifiable online/offline multi-keyword search for cloud-assisted Industrial Internet of Things [10]	2022	J	18	54
140	A Fault-Tolerant Distributed Air-to-Ground Communication Architecture for Urban Air Mobility [184]	2023	C	0	/
141	A Linear Homomorphic Proxy Signature Scheme Based on Blockchain for Internet of Things [185]	2023	J	0	64
142	Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security … [186]	2023	J	4	219
143	Attribute based access control (ABAC) scheme with a fully flexible delegation mechanism … [54]	2023	J	3	42
144	Blend CAC: Integration for the Blockchain for Distributed Potential Network Access for the IoT [187]	2023	C	1	/
145	Edge-Assisted Intelligent Device Authentication in Cyber–Physical Systems [188]	2023	J	17	149

Table A1. *Cont.*

№	Title	Y	T	Cn	h
146	Key-aggregate searchable encryption with multi-user authorisation and keyword untraceability … [189]	2023	J	0	/
147	SAMP-RPL: secure and adaptive multipath RPL for enhanced security and reliability … [190]	2023	J	7	64
148	SEEMQTT: Secure End-to-End MQTT-Based Communication for Mobile IoT Systems … [191]	2023	J	6	149
149	Blockchain-Enabled Key Aggregate Searchable Encryption Scheme … [105]	2024	J	0	149
150	Identity-Based Multiproxy Signature With Proxy Signing Key for Internet of Drones [77]	2024	J	0	149
151	Multi-objective cost-aware bag-of-tasks scheduling optimisation model for IoT applications … [192]	2024	J	0	150
152	Pairing-Free Certificate-Based Proxy Re-Encryption Plus Scheme for Secure Cloud Data Sharing [55]	2024	J	60	62
153	Roll-DPoS: A Randomized Delegated Proof of Stake Scheme … [193]	2018	C	40	/
154	HyBloSE: hybrid blockchain for secure-by-design smart environments [194]	2020	C	3	/
155	Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks [195]	2021	J	2	/
156	A Blockchain-Based Privacy Information Security Sharing Scheme in Industrial Internet of Things [196]	2022	J	9	219
157	A Solution for Bilayer Energy-Trading Management in Microgrids Using Multiblockchain [197]	2022	J	10	149
158	A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city [198]	2022	J	68	101
159	Blockchain-Enhanced Federated Learning Market With Social Internet of Things [199]	2022	J	7	251
160	Blockchain-Governed Federated Transfer Learning for Secure Internet of Drones Networks [200]	2022	J	0	/
161	Cooperative Communication Method Based on Block Chain … [201]	2022	J	3	204
162	Delegated Proof of Accessibility (DPoAC): A Novel Consensus Protocol for Blockchain Systems [202]	2022	J	12	55
163	Delegated Proof of Secret Sharing: A Privacy-Preserving Consensus Protocol … [203]	2022	J	5	/
164	Delegated Proof of Stake Consensus with Mobile Voters and Multiple Entry PBFT Voting [204]	2022	C	1	/
165	Design of a Blockchain-based Security Algorithm for IoT in Healthcare [11]	2022	C	1	/
166	EdgeShare: A blockchain-based edge data-sharing framework for Industrial Internet of Things [205]	2022	J	15	177
167	Investigating Distance Bounding for Delegated Proof-of-Proximity Consensus within IIoT [206]	2022	C	0	/
168	Leveraging Blockchain for Multi-Operator Access Sharing Management in Internet of Vehicles [207]	2022	J	9	204
169	Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers … [208]	2022	J	14	76
170	Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain [209]	2022	J	61	182
171	Sustainable Smart Industry: A Secure and Energy Efficient Consensus Mechanism … [210]	2022	J	18	70
172	A Secure and Intelligent Data Sharing Scheme for UAV-Assisted Disaster Rescue [211]	2023	J	15	179

Table A1. *Cont.*

№	Title	Y	T	Cn	h
173	Achieving a Decentralized and Secure Cab Sharing System Using Blockchain Technology [212]	2023	J	19	182
174	Authentication Technology in IoT and Privacy Security Issues in Typical Application Scenarios [213]	2023	J	4	62
175	Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT [214]	2023	J	1	149
176	Efficient Internet-of-Things Cyberattack Depletion … [215]	2023	J	33	219
177	Enabling a Secure IoT Environment Using a Blockchain-Based Local-Global Consensus Manager [216]	2023	J	2	62
178	Improving Quality of Service for Users of Leaderless DAG-Based Distributed Ledgers [217]	2023	J	1	/
179	LightPoW: A trust based time-constrained PoW for blockchain in Internet of Things [218]	2023	J	5	150
180	Optimisation of a Consensus Protocol in Blockchain-IoT Convergence [219]	2023	C	0	/
181	pDPoSt+sPBFT: A High Performance Blockchain-Assisted Parallel Reinforcement Learning … [220]	2023	J	1	65
182	Safe and Efficient Delegated Proof of Stake Consensus Mechanism … [221]	2023	J	1	25
183	Secure Spectrum Sharing for Satellite Internet-of-Things Based on Blockchain [222]	2023	J	0	75
184	A novel blockchain-based digital forensics framework for preserving evidence … [223]	2024	J	0	81
185	Blockchain-enabled trust management for secure content caching in mobile edge computing … [107]	2024	J	0	39
186	Computing Power Networking Meets Blockchain: A Reputation-Enhanced Trading Framework … [224]	2024	J	0	149
187	Enhancing IoT Data Security with Lightweight Blockchain and … [225]	2024	J	0	64
188	On-Chain and Off-Chain Data Management for Blockchain-Internet of Things: A Multi-Agent … [226]	2024	J	0	58
1890	Optimized blockchain-based healthcare framework … [227]	2024	J	2	129
190	Resource Efficient Federated Learning and DAG Blockchain With Sharding … [228]	2024	J	0	149
191	LT-DBFT: A Hierarchical Blockchain Consensus Using Location and Trust in IoT [229]	2025	C	0	/
	Computations Delegation				
192	HIP Tiny Exchange (TEX): A distributed key exchange scheme for HIP-based Internet of Things [91]	2012	C	9	/
193	A federated architecture approach for Internet of Things security [230]	2014	C	83	/
194	C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things [71]	2014	C	46	/
195	Lightweight DTLS Implementation in CoAP-based IoT [72]	2014	J	26	9
196	Lightweight collaborative key establishment scheme for the Internet of Things [8]	2014	J	79	150
197	Mitigating loT Security Threats with a Trusted Network Element [98]	2014	C	19	/
198	Efficient Key Establishment for Constrained IoT Devices with Collaborative HIP-Based Approach [231]	2015	C	5	/
199	Proxy-based end-to-end key establishment protocol for the Internet of Things [20]	2015	C	18	/
200	S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things [85]	2016	J	80	102
201	ScriptIoT: A Script Framework for and Internet-of-Things Applications [73]	2016	J	13	149
202	An Ontology-Based Approach for IoT Data Processing Using Semantic Rules [81]	2017	C	6	/
203	CHIP: Collaborative Host Identity Protocol with Efficient Key Establishment … [90]	2017	J	10	75
204	Fast and Parallel Keyword Search Over Public-Key Ciphertexts for Cloud-Assisted IoT [232]	2017	J	11	204

Table A1. *Cont.*

№	Title	Y	T	Cn	h
205	DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices [233]	2018	J	31	54
206	Efficient Outsourced Data Access Control with User Revocation for Cloud-Based IoT [234]	2018	C	3	/
207	Secure and trusted telemedicine in Internet of Things IoT [86]	2018	C	9	/
208	Securely outsourcing the ciphertext-policy attribute-based encryption [235]	2018	J	21	54
209	Event driven and semantic based approach for data processing on IoT gateway devices [74]	2019	J	17	64
210	IoT meets distributed AI—Deployment scenarios of Bonseyes AI applications on FIWARE [236]	2019	C	6	/
211	JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT [87]	2019	J	90	4
212	On-Demand Computation Offloading Architecture in Fog Networks [89]	2019	J	10	62
213	Powering Smart Homes with Information-Centric Networking [80]	2019	J	17	272
214	A Layer-Partitioning Approach for Faster Execution of Neural Network-Based . . . Applications . . . [79]	2020	J	5	204
215	A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment [104]	2020	J	36	204
216	Identity-based encryption with authorized equivalence test for cloud-assisted IoT [237]	2020	J	17	63
217	Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things [15]	2020	J	33	204
218	Lightweighted Secure Searching Over Public-Key Ciphertexts for . . . Industrial IoT Devices [238]	2020	J	27	170
219	Match in My Way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing [239]	2020	J	43	92
220	Privacy-Preserving Computation Offloading for Time-Series Activities Classification in eHealthcare [240]	2020	C	9	/
221	Reliable and secure data transfer in IoT networks [241]	2020	J	20	98
222	Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage [242]	2020	J	33	204
223	A Hybrid Artificial Neural Network for Task Offloading in Mobile Edge Computing [75]	2022	C	5	/
224	A Queueing Game Based Management Framework for Fog Computing . . . [243]	2022	J	22	151
225	Achieving reliable and anti-collusive outsourcing computation and verification . . . [244]	2022	J	5	40
223	An IoT Digital Twin for Cyber-Security Defence Based on Runtime Verification [245]	2022	C	1	/
227	Architecture Blueprints to Enable Scalable Vertical Integration of Assets with Digital Twins [84]	2022	C	3	/
228	Attribute-based searchable encryption with delegated equality test in cloud-assisted Internet of Things [78]	2022	C	0	/
229	Certificateless Group to Many Broadcast Proxy Reencryptions for Data Sharing . . . [246]	2022	J	1	73
230	Edge-assisted Puncturable Fine-grained Task Distribution for the IoT-oriented Crowdsensing [247]	2022	C	0	/
231	Efficient Privacy-Preserving Outsourced Discrete Wavelet Transform in the Encrypted Domain [248]	2022	J	1	61
232	Enabling secure mutual authentication and storage checking in cloud-assisted IoT [249]	2022	J	4	53

Table A1. *Cont.*

№	Title	Y	T	Cn	h
233	Privacy-Preserving and Verifiable Outsourcing Message Transmission and Authentication Protocol … [95]	2022	C	1	/
234	Privacy-preserving CNN feature extraction and retrieval over medical images [250]	2022	J	0	/
235	SecDT: Privacy-Preserving Outsourced Decision Tree Classification … [251]	2022	J	0	36
236	Secure Infectious Diseases Detection System With IoT-Based e-Health Platforms [82]	2022	J	5	149
237	Secure and Temporary Access Delegation With Equality Test for Cloud-Assisted IoV [252]	2022	J	3	182
238	Supporting AI Engineering on the IoT Edge through Model-Driven TinyML [13]	2022	C	4	/
239	A Fog-Based Architecture for Latency-Sensitive Monitoring Applications … [253]	2023	J	2	149
240	A Novel Multi-Party Authentication Scheme for FCN-based MIoT Systems … [254]	2023	J	1	20
241	A key-insulated secure multi-server authenticated key agreement protocol … [255]	2023	J	4	39
242	Computation Offloading for Industrial Internet of Things: A Cooperative Approach [256]	2023	C	0	/
243	Everything Under Control: Secure Data Sharing Mechanism for Cloud-Edge Computing [257]	2023	J	2	154
244	Improving efficiency and security of IIoT communications … [258]	2023	J	4	117
245	LNGate^2: Secure Bidirectional IoT Micro-Payments … [259]	2023	J	0	151
246	Novel proxy signature from lattice for the post-quantum Internet of Things [260]	2023	J	13	64
247	Outsourcing the Computation of Plaintext Encryption for Homomorphic Encryption [88]	2023	C	0	/
248	Management of IoT Devices Data Security Using Blockchain and Proxy Re-encryption Algorithm [83]	2023	C	1	/
249	Proxy-Based Re-Encryption Design for the IoT Ecosystem [261]	2023	C	0	/
250	Towards Fine-Grained Task Allocation With Bilateral Access Control … [262]	2023	J	0	149
251	A lightweight attribute-based signcryption scheme based on cloud-fog assisted in smart healthcare [263]	2024	J	0	404
252	Fog-Assisted Dynamic IoT Device Access Management Using Attribute-Based Encryption [264]	2024	C	0	/
253	QB-IMD: A Secure Medical Data Processing System With Privacy Protection … [265]	2024	J	7	149
254	REEDS: An Efficient Revocable End-to-End Encrypted Message Distribution System for IoT [76]	2024	J	0	92

Appendix B. Results of the Security Evaluation

Table A2 presents a summary of the security evaluation of existing delegation solutions, focusing on confidentiality, integrity, and availability against three types of adversaries. The evaluation was conducted using the security models introduced in Sections 3 and 4. If we believe that a system can be proven secure against a given adversary type, the attack is unlikely or has no critical impact on system functionality, we mark it as (✓). If an attack against the system is feasible and causes significant damage, we mark it as (✗).

Table A2. Results of the Security Evaluation of Existing Delegation Protocols against Three Adversary Types within the Framework of the CIA-Triad (**C**onfidentiality, **I**netegrity and **A**vailability).

№	Paper Title	C			I			A		
		$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$
Access Control and/or Authorisation Delegation										
1	Seitz et al. [110] (2013)	✓	✗	✗	✓	✗	✗	✗	✗	✗
2	Lessa dos Santos et al. [25] (2015)	✓	✗	✗	✓	✗	✗	✗	✗	✗
3	Sciarretta et al. [97] (2016)	✓	✓	✗	✓	✓	✗	✓	✗	✗
4	Bandara et al. [111] (2016)	✓	✗	✗	✓	✗	✗	✗	✗	✗
5	Beltran and Skarmeta [99] (2016)	✓	✗	✗	✓	✗	✗	✗	✗	✗
6	Solapurkar [30] (2016)	✓	✗	✗	✓	✗	✗	✗	✗	✗
7	Kum et al. [112] (2016)	✓	✗	✗	✓	✗	✗	✗	✗	✗
8	Bruneo et al. [34] (2016)	✓	✗	✗	✓	✓	✗	✓	✗	✗
9	Bernal Bernabe et al. [113] (2016)	✓	✗	✗	✓	✗	✗	✗	✗	✗
10	Hussein et al. [114] (2017)	✓	✗	✗	✓	✗	✗	✗	✗	✗
11	Fernández et al. [29] (2017)	✓	✗	✗	✓	✗	✗	✗	✗	✗
12	Dao et al. [115] (2017)	✓	✗	✗	✓	✗	✗	✗	✗	✗
13	Pinno et al. [31] (2017)	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Sciancalepore et al. [28] (2017)	✓	✗	✗	✓	✗	✗	✗	✗	✗
15	Beltran et al. [116] (2017)	✓	✗	✗	✓	✗	✗	✗	✗	✗
16	Park and Park [21] (2018)	✓	✓	✗	✓	✗	✗	✗	✗	✗
17	Novo [26] (2018)	✓	✓	✓	✓	✓	✓	✓	✓	✓
18	Ayoade et al. [32] (2018)	✓	✓	✓	✓	✓	✓	✓	✓	✓
19	Chien [117] (2018)	✓	✗	✗	✓	✗	✗	✗	✗	✗
20	Zhou et al. [118] (2018)	✓	✗	✗	✓	✗	✗	✗	✗	✗
21	Atlam et al. [103] (2018)	✓	✗	✗	✓	✓	✓	✓	✗	✗
22	Behrad et al. [119] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗
23	Sabrina [27] (2019)	✓	✓	✓	✓	✓	✓	✓	✓	✓
24	Al-Aqrabi et al. [120] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗
25	Lagutin et al. [121] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗
26	Li et al. [36] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗
27	Pal et al. [35] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗
28	Siris et al. [33] (2019)	✓	✓	✓	✓	✓	✓	✓	✓	✓
29	Behrad et al. [122] (2020)	✓	✗	✗	✓	✗	✗	✗	✗	✗
30	Pal et al. [37] (2020)	✓	✓	✗	✓	✗	✗	✗	✗	✗
31	Xu et al. [123] (2020)	✓	✗	✓	✓	✓	✓	✓	✓	✓
32	Shafagh et al. [17] (2020)	✓	✓	✗	✓	✓	✓	✗	✗	✗
33	Hang and Kim [124] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
34	Lin and Liao [125] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
35	Julku et al. [96] (2021)	✓	✗	✗	✓	✗	✗	✗	✗	✗
36	Abdel-Malek et al. [126] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✗
37	Zhou et al. [18] (2022)	✓	✗	✗	✓	✗	✗	✗	✗	✗
38	Goyal et al. [127] (2022)	✓	✗	✗	✓	✗	✗	✗	✗	✗
39	Dunnett et al. [106] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
40	Jiang et al. [128] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
41	Tegane et al. [129] (2023)	✓	✗	✗	✓	✓	✗	✗	✗	✗
42	Alshehri et al. [130] (2023)	✓	✗	✗	✓	✗	✗	✗	✗	✗
43	Pittaras and Polyzos [131] (2023)	✓	✗	✗	✓	✗	✗	✗	✗	✗
44	Vattaparambil Sudarsan et al. [132] (2023)	✓	✗	✗	✓	✗	✗	✗	✗	✗
45	Dallel et al. [12] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
46	Chen et al. [133] (2024)	✓	✓	✓	✓	✓	✓	✓	✓	✓
47	Sun et al. [134] (2025)	✓	✗	✗	✓	✗	✗	✓	✗	✗

Table A2. *Cont.*

№	Paper Title	C			I			A		
		$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$
Authentication Delegation										
48	Fouladgar and Afifi [49] (2007)	✓	✓	✗	✓	✓	✗	✗	✗	✗
49	Granjal et al. [47] (2013)	✓	✓	✗	✓	✓	✗	✗	✗	✗
50	Hummen et al. [41] (2013)	✓	✓	✗	✓	✓	✗	✗	✗	✗
51	Hummen et al. [100] (2014)	✓	✓	✗	✓	✓	✗	✗	✗	✗
52	Park and Kang [38] (2014)	✓	✓	✗	✓	✓	✗	✓	✓	✗
53	Emerson et al. [39] (2015)	✓	✗	✗	✓	✗	✗	✗	✗	✗
54	Kang et al. [101] (2015)	✓	✓	✗	✓	✓	✗	✓	✓	✗
55	Cirani et al. [40] (2015)	✓	✗	✗	✓	✗	✗	✗	✗	✗
56	Moosavi et al. [42] (2015)	✓	✗	✗	✓	✗	✗	✗	✗	✗
57	Hernandez-Ramos et al. [135] (2015)	✓	✓	✗	✓	✓	✗	✗	✗	✗
58	Kim et al. [45] (2017)	✓	✓	✓	✓	✓	✓	✓	✓	✗
59	Park et al. [48] (2017)	✓	✓	✗	✓	✓	✗	✓	✗	✗
60	Van den Abeele et al. [102] (2017)	✓	✓	✗	✓	✓	✗	✓	✗	✗
61	Gu and Mohapatra [43] (2018)	✓	✗	✗	✓	✗	✗	✓	✗	✗
62	Kim et al. [136] (2019)	✓	✓	✗	✓	✓	✗	✗	✗	✗
63	Cho et al. [22] (2019)	✓	✓	✗	✓	✓	✗	✗	✗	✗
64	Gritti et al. [16] (2019)	✓	✓	✗	✓	✓	✗	✗	✗	✗
65	Guo et al. [46] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
66	Wiraatmaja and Kasahara [14] (2023)	✓	✓	✗	✓	✓	✗	✗	✗	✗
67	Yuan et al. [44] (2023)	✓	✓	✗	✓	✓	✗	✓	✓	✗
68	Rafiqullah et al. [19] (2023)	✓	✓	✗	✓	✓	✗	✗	✗	✗
Rights Delegation										
69	Anggorojati et al. [93] (2012)	✓	✗	✗	✓	✗	✗	✗	✗	✗
70	Morales et al. [137] (2013)	✓	✓	✗	✓	✓	✗	✗	✗	✗
71	Gusmeroli et al. [57] (2013)	✓	✗	✗	✓	✗	✗	✗	✗	✗
72	Hernández-Ramos et al. [138] (2013)	✓	✗	✗	✓	✗	✗	✗	✗	✗
73	Hernández-Ramos et al. [68] (2016)	✓	✗	✗	✓	✗	✗	✗	✗	✗
74	Ouaddah et al. [50] (2016)	✓	✓	✓	✓	✓	✓	✗	✗	✗
75	Outchakoucht et al. [139] (2017)	✓	✓	✓	✓	✓	✓	✗	✗	✗
76	Denis et al. [92] (2017)	✓	✓	✗	✓	✓	✗	✗	✗	✗
77	Yang et al. [140] (2017)	✓	✓	✓	✓	✓	✓	✗	✗	✗
78	Ko et al. [141] (2017)	✓	✓	✗	✓	✓	✗	✗	✗	✗
79	Xu et al. [52] (2018)	✓	✓	✓	✓	✓	✓	✗	✗	✗
80	Xu et al. [51] (2018)	✓	✓	✓	✓	✓	✓	✗	✗	✗
81	Tapas et al. [142] (2018)	✓	✓	✓	✓	✓	✓	✗	✗	✗
82	Le and Mutka [53] (2018)	✓	✓	✓	✓	✓	✓	✗	✗	✗
83	Alphand et al. [65] (2018)	✓	✓	✓	✓	✓	✓	✗	✗	✗
84	Chung et al. [62] (2018)	✓	✗	✗	✓	✗	✗	✗	✗	✗
85	Sabrina [143] (2019)	✓	✓	✓	✓	✓	✓	✗	✗	✗
86	Porwal and Mittal [144] (2019)	✓	✓	✓	✓	✓	✓	✗	✗	✗
87	Mendy et al. [63] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗
88	Sun et al. [145] (2019)	✓	✓	✓	✓	✓	✓	✗	✗	✗
89	Ali et al. [146] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗
90	Zemmoudj et al. [56] (2019)	✓	✗	✗	✓	✓	✗	✓	✗	✗
91	Zemmoudj et al. [147] (2019)	✓	✓	✓	✓	✓	✓	✗	✗	✗
92	Pinjala and Sivalingam [148] (2019)	✓	✓	✓	✓	✓	✓	✗	✗	✗
93	Rabehaja et al. [58] (2019)	✓	✗	✗	✓	✗	✗	✗	✗	✗

Table A2. *Cont.*

№	Paper Title	C			I			A		
		$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$
94	Xu et al. [149] (2019)	✓	✓	✓	✓	✓	✓	✗	✗	✗
95	Andersen et al. [61] (2019)	✓	✓	✓	✓	✓	✓	✓	✗	✗
96	Deng et al. [150] (2020)	✓	✓	✓	✓	✓	✓	✗	✗	✗
97	Chen et al. [64] (2020)	✓	✗	✗	✓	✗	✗	✗	✗	✗
98	Nakamura et al. [151] (2020)	✓	✓	✓	✓	✓	✓	✗	✗	✗
99	Pal et al. [23] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
100	Pal et al. [152] (2020)	✓	✓	✓	✓	✓	✓	✗	✗	✗
101	Li et al. [69] (2020)	✓	✓	✓	✓	✓	✓	✗	✗	✗
102	Puggioni et al. [153] (2020)	✓	✓	✓	✓	✓	✓	✗	✗	✗
103	Ali et al. [154] (2020)	✓	✓	✓	✓	✓	✓	✗	✗	✗
104	Zhou et al. [155] (2021)	✓	✓	✓	✓	✓	✓	✗	✗	✗
105	Zhao et al. [156] (2021)	✓	✓	✓	✓	✓	✓	✗	✗	✗
106	Zhang et al. [157] (2021)	✓	✓	✓	✓	✓	✓	✗	✗	✗
107	Ullah et al. [158] (2021)	✓	✓	✓	✓	✓	✓	✗	✗	✗
108	Sabrina and Jang-Jaccard [159] (2021)	✓	✓	✓	✓	✓	✓	✗	✗	✗
109	Skarlat and Schulte [160] (2021)	✓	✓	✗	✓	✗	✗	✗	✗	✗
110	Wei et al. [66] (2021)	✓	✗	✗	✓	✓	✗	✗	✗	✗
111	Lastname et al. [161] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
112	Chien and Wang [162] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
113	Agyekum et al. [60] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
114	Cha et al. [163] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
115	Li et al. [164] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
116	Zhang et al. [67] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
117	Ali et al. [165] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
118	Kumar and Kumar [70] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
119	Bayreuther et al. [166] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
120	Xiong et al. [167] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
121	Latif [168] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
122	Xue [169] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
123	Pinjala et al. [170] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
124	Silva and Barraca [171] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
125	Banerjee et al. [172] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
126	Qushtom et al. [173] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
127	Heo et al. [174] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
128	Hu et al. [59] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
129	Ju et al. [175] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
130	Panneerselvam and Krithiga [176] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
131	Wang and Chow [177] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
132	Sama et al. [178] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
133	Alsubhi et al. [9] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
134	Shur et al. [179] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
135	Tanyingyong et al. [180] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
136	Goh et al. [181] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
137	Qiao et al. [182] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
138	Rios et al. [183] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
139	Ali et al. [10] (2022)	✓	✓	✓	✓	✓	✓	✗	✗	✗
140	Wanniarachchi and Turau [184] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
141	Wang and Wu [185] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
142	Alharbi [186] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗

Table A2. *Cont.*

№	Paper Title	C			I			A		
		$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$
143	Choksy et al. [54] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
144	Malhotra [187] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
145	Lu et al. [188] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
146	Trivedi and Patel [189] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
147	Sahraoui and Henni [190] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
148	Hamad et al. [191] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
149	Lee et al. [105] (2024)	✓	✓	✓	✓	✓	✓	✗	✗	✗
150	Shin et al. [77] (2024)	✓	✓	✓	✓	✓	✓	✗	✗	✗
151	Seifhosseini et al. [192] (2024)	✓	✓	✓	✓	✓	✓	✗	✗	✗
152	Yan et al. [55] (2024)	✓	✗	✗	✓	✓	✗	✗	✗	✗
153	Fan and Chai [193] (2018)	✓	✗	✗	✓	✗	✗	✗	✗	✗
154	Maselli et al. [194] (2020)	✓	✓	✗	✓	✗	✗	✗	✗	✗
155	Vairagade and Brahmananda [195] (2021)	✓	✓	✗	✓	✗	✗	✗	✗	✗
156	Wang et al. [196] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
157	Huang et al. [197] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
158	Ahmed et al. [198] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
159	Wang et al. [199] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
160	Wang et al. [200] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
161	Zhi et al. [201] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
162	Kaur et al. [202] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
163	Geng et al. [203] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
164	Misic et al. [204] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
165	Rastogi et al. [11] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
166	Yang et al. [205] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
167	Ledwaba et al. [206] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
168	Hu et al. [207] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
169	Bachani and Bhattacharjya [208] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
170	Cui et al. [209] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
171	Sasikumar et al. [210] (2022)	✓	✓	✗	✓	✗	✗	✗	✗	✗
172	Wang et al. [211] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
173	Namasudra and Sharma [212] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
174	Zhao et al. [213] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
175	Wang et al. [214] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
176	Razaque et al. [215] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
177	Alghamdi et al. [216] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
178	Cullen et al. [217] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
179	Qi et al. [218] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
180	Kaur and Gupta [219] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
181	Yang et al. [220] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
182	Mingjie Zhao et al. [221] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
183	Wang et al. [222] (2023)	✓	✓	✗	✓	✗	✗	✗	✗	✗
184	Xiao et al. [223] (2024)	✓	✓	✗	✓	✗	✗	✗	✗	✗
185	Bounaira et al. [107] (2024)	✓	✓	✗	✓	✗	✗	✗	✗	✗
186	Lin et al. [224] (2024)	✓	✓	✗	✓	✗	✗	✗	✗	✗
187	Mohammed and Wahab [225] (2024)	✓	✓	✗	✓	✗	✗	✗	✗	✗
188	Tsang et al. [226] (2024)	✓	✓	✗	✓	✗	✗	✗	✗	✗
189	Al-Marridi et al. [227] (2024)	✓	✓	✗	✓	✗	✗	✗	✗	✗
190	Jiang et al. [228] (2024)	✓	✓	✗	✓	✗	✗	✗	✗	✗
191	Wang et al. [229] (2025)	✓	✗	✗	✓	✗	✗	✓	✗	✗

Table A2. *Cont.*

№	Paper Title	C			I			A		
		$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$
Computations Delegation										
192	Ben Saied and Olivereau [91] (2012)	✓	✓	✗	✓	✗	✗	✓	✗	✗
193	Leo et al. [230] (2014)	✓	✓	✗	✓	✗	✗	✓	✗	✗
194	Touati et al. [71] (2014)	✓	✓	✓	✓	✓	✓	✓	✓	✓
195	Lakkundi and Singh [72] (2014)	✓	✓	✗	✓	✗	✗	✓	✗	✗
196	Saied et al. [8] (2014)	✓	✓	✗	✓	✓	✗	✓	✓	✓
197	Kuusijarvi [98] (2014)	✓	✓	✗	✓	✗	✗	✓	✗	✗
198	Porambage et al. [231] (2015)	✓	✓	✗	✓	✗	✗	✓	✗	✗
199	Porambage et al. [20] (2015)	✓	✓	✗	✓	✓	✗	✓	✓	✗
200	Raza et al. [85] (2016)	✓	✓	✗	✓	✓	✗	✗	✗	✗
201	Hsieh et al. [73] (2016)	✗	✗	✗	✗	✗	✗	✗	✗	✗
202	Bali et al. [81] (2017)	✗	✗	✗	✗	✗	✗	✗	✗	✗
203	Porambage et al. [90] (2017)	✓	✓	✗	✓	✗	✗	✓	✗	✗
204	Xu et al. [232] (2017)	✓	✓	✓	✓	✓	✓	✓	✓	✓
205	Huang et al. [233] (2018)	✓	✓	✓	✓	✓	✓	✓	✓	✓
206	Hao et al. [234] (2018)	✓	✓	✓	✓	✓	✓	✓	✓	✓
207	Albalawi and Joshi [86] (2018)	✓	✓	✗	✓	✓	✗	✗	✗	✗
208	Nguyen et al. [235] (2018)	✓	✓	✓	✓	✓	✓	✓	✓	✓
209	Al-Osta et al. [74] (2019)	✗	✗	✗	✗	✗	✗	✗	✗	✗
210	Moor et al. [236] (2019)	✗	✗	✗	✗	✗	✗	✗	✗	✗
211	Kumar et al. [87] (2019)	✓	✓	✗	✓	✓	✓	✗	✗	✗
212	Jin and Lee [89] (2019)	✓	✓	✗	✓	✗	✗	✓	✗	✗
213	Xu et al. [80] (2019)	✗	✗	✗	✗	✗	✗	✗	✗	✗
214	Saguil and Azim [79] (2020)	✗	✗	✗	✗	✗	✗	✗	✗	✗
215	Luo et al. [104] (2020)	✓	✗	✗	✓	✗	✗	✗	✗	✗
216	Elhabob et al. [237] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
217	Ali et al. [15] (2020)	✓	✗	✗	✓	✓	✓	✗	✗	✗
218	Wang et al. [238] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
219	Xu et al. [239] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
220	Zheng et al. [240] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
221	Gochhayat et al. [241] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
222	Tao et al. [242] (2020)	✓	✓	✓	✓	✓	✓	✓	✓	✓
223	Hamadi et al. [75] (2022)	✗	✗	✗	✗	✗	✗	✗	✗	✗
224	Yi et al. [243] (2022)	✗	✗	✗	✗	✗	✗	✗	✗	✗
225	Wang et al. [244] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
226	De Hoz Diego et al. [245] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
227	Schnicke et al. [84] (2022)	✗	✗	✗	✗	✗	✗	✗	✗	✗
228	Hu et al. [78] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
229	Kim et al. [246] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
230	Jiang and Qin [247] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
231	Zhou et al. [248] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
232	Liu et al. [249] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
233	Li et al. [95] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
234	Cai et al. [250] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
235	Chen et al. [251] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
236	Zhao et al. [82] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
237	Li et al. [252] (2022)	✓	✓	✓	✓	✓	✓	✓	✓	✓
238	Moin et al. [13] (2022)	✗	✗	✗	✗	✗	✗	✗	✗	✗

Table A2. *Cont.*

№	Paper Title	C			I			A		
		$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$	$\mathcal{A}_{weak}$	$\mathcal{A}_{middle}$	$\mathcal{A}_{strong}$
239	Benomar et al. [253] (2023)	✗	✗	✗	✗	✗	✗	✗	✗	✗
240	Meng et al. [254] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
241	Yao et al. [255] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
242	Chouikhi et al. [256] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
243	Song et al. [257] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
244	Atutxa et al. [258] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
245	Kurt et al. [259] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
246	Wang et al. [260] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
247	Li et al. [88] (2023)	✓	✓	✓	✓	✓	✓	✗	✗	✗
248	Mahamuni et al. [83] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
249	Srikanth et al. [261] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
250	Wu et al. [262] (2023)	✓	✓	✓	✓	✓	✓	✓	✓	✓
251	Sun et al. [263] (2024)	✓	✓	✓	✓	✓	✓	✓	✓	✓
252	Routray and Bera [264] (2024)	✓	✓	✓	✓	✓	✓	✓	✓	✓
253	Qu et al. [265] (2024)	✓	✓	✓	✓	✓	✓	✓	✓	✓
254	Li et al. [76] (2024)	✓	✗	✗	✓	✗	✗	✗	✗	✗

References

1. Statista. *Internet of Things—Market Outlook Report*; Statista. Juni 2024. Available online: https://de.statista.com/statistik/studie/id/109209/dokument/internet-der-dinge-market-outlook-report/ (accessed on 28 April 2025).
2. Statista Market Insights. *Annual Number of Cyberattacks Worldwide from 2016 to 2023 (In Millions)*; Graph: 2024. Available online: https://www.statista.com/forecasts/1485031/cyberattacks-annual-worldwide (accessed on 28 April 2025).
3. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of Things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [CrossRef]
4. Chacko, A.; Hayajneh, T. Security and Privacy Issues with IoT in Healthcare. *EAI Endorsed Trans. Pervasive Health Technol.* **2018**, *4*, e2. [CrossRef]
5. Canavese, D.; Mannella, L.; Regano, L.; Basile, C. Security at the Edge for Resource-Limited IoT Devices. *Sensors* **2024**, *24*, 590. [CrossRef]
6. Wang, Q.; Li, N.; Chen, H. On the Security of Delegation in Access Control Systems. In Proceedings of the Computer Security—ESORICS 2008, Málaga, Spain, 6–8 October 2008; Jajodia, S., Lopez, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 317–332.
7. Chuat, L.; Abdou, A.; Sasse, R.; Sprenger, C.; Basin, D.; Perrig, A. SoK: Delegation and Revocation, the Missing Links in the Web's Chain of Trust. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Genoa, Italy, 7–11 September 2020; pp. 624–638. [CrossRef]
8. Saied, Y.B.; Olivereau, A.; Zeghlache, D.; Laurent, M. Lightweight collaborative key establishment scheme for the Internet of Things. *Comput. Netw.* **2014**, *64*, 273–295. [CrossRef]
9. Alsubhi, K.; Alzahrani, B.; Fotiou, N.; Albeshri, A.; Alreshoodi, M. Reliable Application Layer Routing Using Decentralized Identifiers. *Future Internet* **2022**, *14*, 322. [CrossRef]
10. Ali, M.; Sadeghi, M.R.; Liu, X.; Miao, Y.; Vasilakos, A.V. Verifiable online/offline multi-keyword search for cloud-assisted Industrial Internet of Things. *J. Inf. Secur. Appl.* **2022**, *65*, 103101. [CrossRef]
11. Rastogi, P.; Singh, D.; Singh Bedi, S. Design of a Blockcdhain based Security Algorithm for IoT in Healthcare. In Proceedings of the 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 28–29 April 2022. [CrossRef]
12. Dallel, O.; Ayed, S.B.; Tahar, J.B.H. Smart Blockchain-based Authorization for Social Internet of Things. In Proceedings of the 2023 International Conference on Cyberworlds (CW), Sousse, Tunisia, 3–5 October 2023; pp. 440–447. [CrossRef]
13. Moin, A.; Challenger, M.; Badii, A.; Gunnemann, S. Supporting AI Engineering on the IoT Edge through Model-Driven TinyML. In Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 27 June–1 July 2022; pp. 884–893. [CrossRef]

14. Wiraatmaja, C.; Kasahara, S. Cost-Efficient Anonymous Authentication Scheme Based on Set-Membership Zero-Knowledge Proof. In Proceedings of the 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 11–13 October 2023; pp. 1–8. [CrossRef]
15. Ali, M.; Sadeghi, M.R.; Liu, X. Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things. *IEEE Access* **2020**, *8*, 23951–23964. [CrossRef]
16. Gritti, C.; Önen, M.; Molva, R. Privacy-preserving delegable authentication in the internet of things. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, Limassol, Cyprus, 8–12 April 2019; pp. 861–869. [CrossRef]
17. Shafagh, H.; Burkhalter, L.; Ratnasamy, S.; Hithnawi, A. Droplet: Decentralized Authorization and Access Control for Encrypted Data Streams. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), Boston, MA, USA, 12–14 August 2020; pp. 2469–2486.
18. Zhou, X.; Guan, J.; Xing, L.; Qian, Z. Perils and Mitigation of Security Risks of Cooperation in Mobile-as-a-Gateway IoT. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, 7–11 November 2022; pp. 3285–3299. [CrossRef]
19. Rafiqullah; Mehmood, A.; Khan, M.A.; Maple, C.; Lloret, J. Zero-Knowledge Proofs based delegation authentication for Industrial Internet of Things in certificateless proxy signatures. In Proceedings of the 2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), San Antonio, TX, USA, 23–25 October 2023; pp. 8–14. [CrossRef]
20. Porambage, P.; Braeken, A.; Kumar, P.; Gurtov, A.; Ylianttila, M. Proxy-based end-to-end key establishment protocol for the Internet of Things. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2677–2682. [CrossRef]
21. Park, C.S.; Park, W.S. A Group-Oriented DTLS Handshake for Secure IoT Applications. *IEEE Trans. Autom. Sci. Eng.* **2018**, *15*, 1920–1929. [CrossRef]
22. Cho, E.; Park, M.; Lee, H.; Choi, J.; Kwon, T.T. D2TLS: Delegation-based DTLS for cloud-based IoT services. In Proceedings of the International Conference on Internet of Things Design and Implementation, Montreal, QC, Canada, 15–18 April 2019; pp. 190–201. [CrossRef]
23. Pal, S.; Rabehaja, T.; Hitchens, M.; Varadharajan, V.; Hill, A. On the Design of a Flexible Delegation Model for the Internet of Things Using Blockchain. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3521–3530. [CrossRef]
24. Samonas, S.; Coss, D. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *J. Inf. Syst. Secur.* **2014**, *10*, 21–45.
25. Lessa dos Santos, G.; Guimarães, V.T.; da Cunha Rodrigues, G.; Granville, L.Z.; Tarouco, L.M.R. A DTLS-based security architecture for the Internet of Things. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 809–815. [CrossRef]
26. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
27. Sabrina, F. Blockchain and Structural Relationship Based Access Control for IoT: A Smart City Use Case. In Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrück, Germany, 14–17 October 2019; pp. 137–140. [CrossRef]
28. 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.
29. Fernández, F.; Alonso, A.; 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. [CrossRef]
30. Solapurkar, P. Building secure healthcare services using OAuth 2.0 and JSON web token in IOT cloud scenario. In Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Greater Noida, India, 14–17 December 2016; pp. 99–104. [CrossRef]
31. Pinno, O.J.A.; Gregio, A.R.A.; De Bona, L.C.E. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6. [CrossRef]
32. 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. [CrossRef]
33. Siris, V.; Dimopoulos, D.; Fotiou, N.; Voulgaris, S.; Polyzos, G. Trusted D2D-Based IoT Resource Access Using Smart Contracts. In Proceedings of the 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–9. [CrossRef]

34. Bruneo, D.; Distefano, S.; Longo, F.; Merlino, G.; Puliafito, A. IoT-cloud authorization and delegation mechanisms for ubiquitous sensing and actuation. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 222–227. [CrossRef]
35. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. Policy-based access control for constrained healthcare resources in the context of the Internet of Things. *J. Netw. Comput. Appl.* **2019**, *139*, 57–74. [CrossRef]
36. Li, Q.; Zhu, H.; Xiong, J.; Mo, R.; Ying, Z.; Wang, H. Fine-grained multi-authority access control in IoT-enabled mHealth. *Ann. Telecommun.* **2019**, *74*, 389–400. [CrossRef]
37. Pal, S.; Hitchens, M.; Varadharajan, V. Access control for Internet of Things—Enabled assistive technologies: An architecture, challenges and requirements. In *Assistive Technology for the Elderly*; Elsevier: Cambridge, MA, USA, 2020; pp. 1–43. [CrossRef]
38. Park, J.; Kang, N. Lightweight secure communication for CoAP-enabled Internet of Things using delegated DTLS handshake. In Proceedings of the 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, Republic of Korea, 22–24 October 2014; pp. 28–33. [CrossRef]
39. Emerson, S.; Choi, Y.K.; Hwang, D.Y.; Kim, K.S.; Kim, K.H. An OAuth based authentication mechanism for IoT networks. In Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 28–30 October 2015; pp. 1072–1074. [CrossRef]
40. Cirani, S.; Picone, M.; Gonizzi, P.; Veltri, L.; Ferrari, G. IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. *IEEE Sens. J.* **2015**, *15*, 1224–1234. [CrossRef]
41. Hummen, R.; Ziegeldorf, J.H.; Shafagh, H.; Raza, S.; Wehrle, K. Towards viable certificate-based authentication for the internet of things. In Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy, Budapest, Hungary, 19 April 2013; HotWiSec '13, pp. 37–42. [CrossRef]
42. Moosavi, S.R.; Gia, T.N.; Rahmani, A.M.; Nigussie, E.; Virtanen, S.; Isoaho, J.; Tenhunen, H. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **2015**, *52*, 452–459. [CrossRef]
43. Gu, T.; Mohapatra, P. BF-IoT: Securing the IoT Networks via Fingerprinting-Based Device Authentication. In Proceedings of the 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Chengdu, China, 9–12 October 2018; pp. 254–262. [CrossRef]
44. Yuan, B.; Yang, M.; Xu, Z.; Chen, Q.; Song, Z.; Li, Z.; Zou, D.; Jin, H. Leakage of Authorization-Data in IoT Device Sharing: New Attacks and Countermeasure. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 3196–3210. [CrossRef]
45. Kim, K.; Han, Y.H.; Min, S.G. An Authentication and Key Management Mechanism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks. *Sensors* **2017**, *17*, 2170. [CrossRef]
46. Guo, S.; Wang, F.; Zhang, N.; Qi, F.; Qiu, X. Master-slave chain based trusted cross-domain authentication mechanism in IoT. *J. Netw. Comput. Appl.* **2020**, *172*, 102812. [CrossRef]
47. Granjal, J.; Monteiro, E.; Silva, J.S. End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. In Proceedings of the 2013 IFIP Networking Conference, Brooklyn, NY, USA, 22–24 May 2013; pp. 1–9.
48. Park, J.; Kwon, H.; Kang, N. IoT—Cloud Collaboration to Establish a Secure Connection for Lightweight Devices. *Wirel. Netw.* **2017**, *23*, 681–692. [CrossRef]
49. Fouladgar, S.; Afifi, H. A Simple Delegation Scheme for RFID Systems (SiDeS). In Proceedings of the 2007 IEEE International Conference on RFID, Grapevine, TX, USA, 26–28 March 2007; pp. 1–6. [CrossRef]
50. Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
51. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT. *Computers* **2018**, *7*, 39. [CrossRef]
52. 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]
53. Le, T.; Mutka, M.W. CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 57–64. [CrossRef]
54. Choksy, P.; Chaurasia, A.; Rao, U.P.; Kumar, S. Attribute based access control (ABAC) scheme with a fully flexible delegation mechanism for IoT healthcare. *Peer-to-Peer Netw. Appl.* **2023**, *16*, 1445–1467. [CrossRef]
55. Yan, L.; Qin, H.; Yang, K.; Xie, H.; Wang, X.A.; Liu, S. Pairing-Free Certificate-Based Proxy Re-Encryption Plus Scheme for Secure Cloud Data Sharing. *Electronics* **2024**, *13*, 534. [CrossRef]

56. Zemmoudj, S.; Bermad, N.; Omar, M. CA-ADP: Context-Aware Authorization and Delegation Protocol for IoT-based healthcare smart systems. In Proceedings of the 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Tunis, Tunisia, 20–22 December 2019; pp. 203–208. [CrossRef]
57. Gusmeroli, S.; Piccione, S.; Rotondi, D. A capability-based security approach to manage access control in the Internet of Things. *Math. Comput. Model.* **2013**, *58*, 1189–1205. [CrossRef]
58. Rabehaja, T.; Pal, S.; Hitchens, M. Design and implementation of a secure and flexible access-right delegation for resource constrained environments. *Future Gener. Comput. Syst.* **2019**, *99*, 593–608. [CrossRef]
59. Hu, Q.; Zheng, G.; Jiang, T. Joint Content and Radio Access for the Internet of Things: A Smart-Contract-Based Trusted Framework. *IEEE Internet Things J.* **2022**, *9*, 18142–18152. [CrossRef]
60. Agyekum, K.O.B.O.; Xia, Q.; Sifah, E.B.; Cobblah, C.N.A.; Xia, H.; Gao, J. A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. *IEEE Syst. J.* **2022**, *16*, 1685–1696. [CrossRef]
61. Andersen, M.P.; Kumar, S.; AbdelBaky, M.; Fierro, G.; Kolb, J.; Kim, H.S.; Culler, D.E.; Popa, R.A. WAVE: A Decentralized Authorization Framework with Transitive Delegation. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 1375–1392.
62. Chung, S.H.; Kim, J.H.; Kim, Y. Pragmatic approach using OAuth mechanism for IoT device authorization in cloud. In Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 12–13 October 2018; pp. 1–4. [CrossRef]
63. Mendy, G.; Ouya, S.; Dioum, I.; Thiaré, O. (Eds.) *e-Infrastructure and e-Services for Developing Countries: 10th EAI International Conference, AFRICOMM 2018, Dakar, Senegal, 29–30 November 2019, Proceedings*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer International Publishing: Cham, Switzerland, 2019; Volume 275. [CrossRef]
64. Chen, X.; Liu, Y.; Chao, H.C.; Li, Y. Ciphertext-Policy Hierarchical Attribute-Based Encryption Against Key-Delegation Abuse for IoT-Connected Healthcare System. *IEEE Access* **2020**, *8*, 86630–86650. [CrossRef]
65. Alphand, O.; Amoretti, M.; Claeys, T.; Dall'Asta, S.; Duda, A.; Ferrari, G.; Rousseau, F.; Tourancheau, B.; Veltri, L.; Zanichelli, F. IoTChain: A blockchain security architecture for the Internet of Things. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6. [CrossRef]
66. Wei, L.; Wu, J.; Long, C.; Li, B. On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 4775–4787. [CrossRef]
67. Zhang, J.; Yang, Y.; Liu, X.; Ma, J. An Efficient Blockchain-Based Hierarchical Data Sharing for Healthcare Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7139–7150. [CrossRef]
68. Hernández-Ramos, J.L.; Jara, A.J.; Marín, L.; Skarmeta Gómez, A.F. DCapBAC: Embedding authorization logic into smart things through ECC optimizations. *Int. J. Comput. Math.* **2016**, *93*, 345–366. [CrossRef]
69. Li, W.; Jin, C.; Kumari, S.; Xiong, H.; Kumar, S. Proxy re-encryption with equality test for secure data sharing in Internet of Things-based healthcare systems. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, e3986. [CrossRef]
70. Kumar, D.; Kumar, M. Attribute-Based Data Sharing in Smart Healthcare Environment. In Proceedings of the 2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), Jamshedpur, India, 11–12 February 2022; pp. 150–157. [CrossRef]
71. Touati, L.; Challal, Y.; Bouabdallah, A. C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things. In Proceedings of the 2014 International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, Algeria, 17–19 June 2014; pp. 64–69. [CrossRef]
72. Lakkundi, V.; Singh, K. Lightweight DTLS implementation in CoAP-based Internet of Things. In Proceedings of the 20th Annual International Conference on Advanced Computing and Communications (ADCOM), Bangalore, India, 19–22 September 2014; pp. 7–11. [CrossRef]
73. Hsieh, H.C.; Chang, K.D.; Wang, L.F.; Chen, J.L.; Chao, H.C. ScriptIoT: A Script Framework for and Internet-of-Things Applications. *IEEE Internet Things J.* **2016**, *3*, 628–636. [CrossRef]
74. Al-Osta, M.; Bali, A.; Gherbi, A. Event driven and semantic based approach for data processing on IoT gateway devices. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 4663–4678. [CrossRef]
75. Hamadi, R.; Khanfor, A.; Ghazzai, H.; Massoud, Y. A Hybrid Artificial Neural Network for Task Offloading in Mobile Edge Computing. In Proceedings of the 2022 IEEE 65th International Midwest Symposium on Circuits and Systems (MWSCAS), Fukuoka, Japan, 7–10 August 2022; pp. 1–4. [CrossRef]
76. Li, C.; Chen, R.; Wang, Y.; Xing, Q.; Wang, B. REEDS: An Efficient Revocable End-to-End Encrypted Message Distribution System for IoT. *IEEE Trans. Dependable Secur. Comput.* **2024**, *21*, 4526–4542. [CrossRef]
77. Shin, Y.A.; Jeong, I.R.; Byun, J.W. Identity-Based Multiproxy Signature with Proxy Signing Key for Internet of Drones. *IEEE Internet Things J.* **2024**, *11*, 4191–4205. [CrossRef]

78. Hu, Y.; Niu, S.; Shao, H. Attribute-based searchable encryption with delegated equality test in cloud-assisted Internet of Things. In Proceedings of the 2022 3rd International Conference on Electronics, Communications and Information Technology (CECIT), Sanya, China, 23–25 December 2022; pp. 328–333. [CrossRef]
79. Saguil, D.; Azim, A. A Layer-Partitioning Approach for Faster Execution of Neural Network-Based Embedded Applications in Edge Networks. *IEEE Access* **2020**, *8*, 59456–59469. [CrossRef]
80. Xu, K.; Wan, Y.; Xue, G. Powering Smart Homes with Information-Centric Networking. *IEEE Commun. Mag.* **2019**, *57*, 40–46. [CrossRef]
81. Bali, A.; Al-Osta, M.; Abdelouahed, G. An Ontology-Based Approach for IoT Data Processing Using Semantic Rules. In *SDL 2017: Model-Driven Engineering for Future Internet*; Lecture Notes in Computer Science; Csöndes, T., Kovács, G., Réthy, G., Eds.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10567, pp. 61–79. [CrossRef]
82. Zhao, Z.; Guo, F.; Wu, G.; Susilo, W.; Wang, B. Secure Infectious Diseases Detection System with IoT-Based e-Health Platforms. *IEEE Internet Things J.* **2022**, *9*, 22595–22607. [CrossRef]
83. Mahamuni, N.; Nikam, H.; Pattewar, G.; Loka, O.; Patil, R. Management of IoT Devices Data Security Using Blockchain and Proxy Re-encryption Algorithm. In *2nd International Conference on Emerging Technologies and Intelligent Systems*; Al-Sharafi, M.A., Al-Emran, M., Al-Kabi, M.N., Shaalan, K., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 551–558.
84. Schnicke, F.; Haque, A.; Kuhn, T.; Espen, D.; Antonino, P.O. Architecture Blueprints to Enable Scalable Vertical Integration of Assets with Digital Twins. In Proceedings of the 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), Stuttgart, Germany, 6–9 September 2022; pp. 1–8. [CrossRef]
85. Raza, S.; Seitz, L.; Sitenkov, D.; Selander, G. S3K: Scalable Security with Symmetric Keys—DTLS Key Establishment for the Internet of Things. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 1270–1280. [CrossRef]
86. Albalawi, U.; Joshi, S. Secure and trusted telemedicine in Internet of Things IoT. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 30–34. [CrossRef]
87. Kumar, S.; Hu, Y.; Andersen, M.P.; Popa, R.A.; Culler, D.E. JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 1519–1536.
88. Li, X.; Li, R.; Bai, B.; Zhao, Y.; Liu, G.; Li, R. Outsourcing the Computation of Plaintext Encryption for Homomorphic Encryption. In Proceedings of the 2023 8th International Conference on Computer and Communication Systems (ICCCS), Guangzhou, China, 21–24 April 2023; pp. 408–413. [CrossRef]
89. Jin, Y.; Lee, H. On-Demand Computation Offloading Architecture in Fog Networks. *Electronics* **2019**, *8*, 1076. [CrossRef]
90. Porambage, P.; Braeken, A.; Kumar, P.; Gurtov, A.; Ylianttila, M. CHIP: Collaborative Host Identity Protocol with Efficient Key Establishment for Constrained Devices in Internet of Things. *Wirel. Pers. Commun.* **2017**, *96*, 421–440. [CrossRef]
91. Ben Saied, Y.; Olivereau, A. HIP Tiny Exchange (TEX): A distributed key exchange scheme for HIP-based Internet of Things. In Proceedings of the Third International Conference on Communications and Networking, Hammamet, Tunisia, 29 March–1 April 2012; pp. 1–8. [CrossRef]
92. Denis, M.; Johansen, C.; Jøsang, A. Offline Trusted Device and Proxy Architecture Based on a new TLS Switching Technique. In Proceedings of the 2017 International Workshop on Secure Internet of Things (SIoT), Oslo, Norway, 15 September 2017; pp. 10–19. [CrossRef]
93. Anggorojati, B.; Mahalle, P.N.; Prasad, N.R.; Prasad, R. Capability-based access control delegation model on the federated IoT network. In Proceedings of the The 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, 24–27 September 2012; pp. 604–608.
94. Venkatesan, S.; Rajeshwari, K.R.; Ramakrishnan, M. A Lightweight Searchable Encryption and Delegation Mechanism with Forward Privacy for Improving the Security of Industrial Internet of Things-Cloud Systems. *Res. Sq.* 2022, *preprint*. [CrossRef]
95. Li, H.; Kong, F.; Yu, J.; Zhang, H.; Diao, L.; Tao, Y. Privacy-Preserving and Verifiable Outsourcing Message Transmission and Authentication Protocol in IoT. In Proceedings of the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 9–11 December 2022; pp. 556–564. [CrossRef]
96. Julku, J.; Suomalainen, J.; Kylanpaa, M. Delegated Device Attestation for IoT. In Proceedings of the 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Gandia, Spain, 6–9 December 2021; pp. 1–8. [CrossRef]
97. Sciarretta, G.; Carbone, R.; Ranise, S. A delegated authorization solution for smart-city mobile applications. In Proceedings of the 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), Bologna, Italy, 7–9 September 2016; pp. 1–6. [CrossRef]
98. Kuusijarvi, J. Mitigating loT Security Threats with a Trusted Network Element. In Proceedings of the The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), London, UK, 8–10 December 2014.

99. Beltran, V.; Skarmeta, A.F. An overview on delegated authorization for CoAP: Authentication and authorization for Constrained Environments (ACE). In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 706–710. [CrossRef]
100. Hummen, R.; Shafagh, H.; Raza, S.; Voig, T.; Wehrle, K. Delegation-based authentication and authorization for the IP-based Internet of Things. In Proceedings of the 2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Singapore, 30 June–3 July 2014; pp. 284–292. [CrossRef]
101. Kang, N.; Park, J.; Kwon, H.; Jung, S. ESSE: Efficient Secure Session Establishment for Internet-Integrated Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 393754. [CrossRef]
102. Van den Abeele, F.; Moerman, I.; Demeester, P.; Hoebeke, J. Secure Service Proxy: A CoAP(s) Intermediary for a Securer and Smarter Web of Things. *Sensors* **2017**, *17*, 1609. [CrossRef]
103. Atlam, H.F.; Alenezi, A.; Hussein, R.K.; Wills, G.B. Validation of an Adaptive Risk-based Access Control Model for the Internet of Things. *Int. J. Comput. Netw. Inf. Secur. (IJCNIS)* **2018**, *10*, 26–35. [CrossRef]
104. Luo, X.; Yin, L.; Li, C.; Wang, C.; Fang, F.; Zhu, C.; Tian, Z. A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment. *IEEE Access* **2020**, *8*, 67192–67204. [CrossRef]
105. Lee, J.; Oh, J.; Kwon, D.; Kim, M.; Kim, K.; Park, Y. Blockchain-Enabled Key Aggregate Searchable Encryption Scheme for Personal Health Record Sharing with Multi-Delegation. *IEEE Internet Things J.* **2024**, 11, 17482–17494. [CrossRef]
106. Dunnett, K.; Pal, S.; Jadidi, Z.; Jurdak, R. A Blockchain-Based Framework for Scalable and Trustless Delegation of Cyber Threat Intelligence. In Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, 1–5 May 2023; pp. 1–9. [CrossRef]
107. Bounaira, S.; Alioua, A.; Souici, I. Blockchain-enabled trust management for secure content caching in mobile edge computing using deep reinforcement learning. *Internet Things* **2024**, *25*, 101081. [CrossRef]
108. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic literature reviews in software engineering—A systematic literature review. *Inf. Softw. Technol.* **2009**, *51*, 7–15. [CrossRef]
109. Wohlin, C.; Prikladniki, R. Systematic literature reviews in software engineering. *Inf. Softw. Technol.* **2013**, *55*, 919–920. [CrossRef]
110. 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; pp. 1–6. [CrossRef]
111. Bandara, S.; Yashiro, T.; Koshizuka, N.; Sakamura, K. Access control framework for API-enabled devices in smart buildings. In Proceedings of the 2016 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, Indonesia, 25–27 August 2016; pp. 210–217. [CrossRef]
112. Kum, S.W.; Kang, M.; Park, J.I. IoT Delegate: Smart Home Framework for Heterogeneous IoT Service Collaboration. *KSII Trans. Internet Inf. Syst.* **2016**, *10*, 3958–3971.
113. Bernal Bernabe, J.; Hernandez Ramos, J.L.; Skarmeta Gomez, A.F. TACIoT: Multidimensional trust-aware access control system for the Internet of Things. *Soft Comput.* **2016**, *20*, 1763–1779. [CrossRef]
114. Hussein, D.; Bertin, E.; Frey, V. A Community-Driven Access Control Approach in Distributed IoT Environments. *IEEE Commun. Mag.* **2017**, *55*, 146–153. [CrossRef]
115. Dao, N.N.; Kim, Y.; Jeong, S.; Park, M.; Cho, S. Achievable Multi-Security Levels for Lightweight IoT-Enabled Devices in Infrastructureless Peer-Aware Communications. *IEEE Access* **2017**, *5*, 26743–26753. [CrossRef]
116. Beltran, V.; Martinez, J.A.; Skarmeta, A.F. User-centric access control for efficient security in smart cities. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6. [CrossRef]
117. Chien, H.Y. Group-Oriented Range-Bound Key Agreement for Internet of Things Scenarios. *IEEE Internet Things J.* **2018**, *5*, 1890–1903. [CrossRef]
118. Zhou, Q.; Elbadry, M.; Ye, F.; Yang, Y. Heracles: Scalable, Fine-Grained Access Control for Internet-of-Things in Enterprise Environments. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications, Honolulu, HI, USA, 15–19 April 2018; pp. 1772–1780. [CrossRef]
119. Behrad, S.; Bertin, E.; Tuffin, S.; Crespi, N. 5G-SSAAC: Slice-specific Authentication and Access Control in 5G. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019; pp. 281–285. [CrossRef]
120. Al-Aqrabi, H.; Johnson, A.P.; Hill, R. Dynamic Multiparty Authentication using Cryptographic Hardware for the Internet of Things. In Proceedings of the 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 19–23 August 2019; pp. 21–28. [CrossRef]
121. Lagutin, D.; Kortesniemi, Y.; Fotiou, N.; Siris, V. 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, London, UK, 15 November 2019. [CrossRef]

122. Behrad, S.; Bertin, E.; Tuffin, S.; Crespi, N. A new scalable authentication and access control mechanism for 5G-based IoT. *Future Gener. Comput. Syst.* **2020**, *108*, 46–61. [CrossRef]
123. Xu, H.; He, Q.; Li, X.; Jiang, B.; Qin, K. BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control. *IEEE Access* **2020**, *8*, 87552–87561. [CrossRef]
124. Hang, L.; Kim, D.H. Reliable Task Management Based on a Smart Contract for Runtime Verification of Sensing and Actuating Tasks in IoT Environments. *Sensors* **2020**, *20*, 1207. [CrossRef]
125. Lin, C.A.; Liao, C.F. User-Managed Access Delegation for Blockchain-driven IoT Services. In Proceedings of the 2020 International Computer Symposium (ICS), Tainan, Taiwan, 17–19 December 2020; pp. 462–467. [CrossRef]
126. Abdel-Malek, M.A.; Akkaya, K.; Bhuyan, A.; Ibrahim, A.S. A Proxy Signature-Based Swarm Drone Authentication with Leader Selection in 5G Networks. *IEEE Access* **2022**, *10*, 57485–57498. [CrossRef]
127. Goyal, G.; Liu, P.; Sural, S. Securing Smart Home IoT Systems with Attribute-Based Access Control. In Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Baltimore, MD, USA, 25–27 April 2022; pp. 37–46. [CrossRef]
128. Jiang, W.; Lin, Z.; Tao, J. An access control scheme for distributed Internet of Things based on adaptive trust evaluation and blockchain. *High-Confid. Comput.* **2023**, *3*, 100104. [CrossRef]
129. Tegane, S.; Semchedine, F.; Boudries, A. An extended Attribute-based access control with controlled delegation in IoT. *J. Inf. Secur. Appl.* **2023**, *76*, 103473. [CrossRef]
130. Alshehri, S.; Bamasaq, O.; Alghazzawi, D.; Jamjoom, A. Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment. *IEEE Internet Things J.* **2023**, *10*, 4239–4256. [CrossRef]
131. Pittaras, I.; Polyzos, G.C. Multi-tenant, Decentralized Access Control for the Internet of Things. In Proceedings of the 2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bali, Indonesia, 28–30 November 2023; pp. 28–34. [CrossRef]
132. Vattaparambil Sudarsan, S.; Schelén, O.; Bodin, U. Multilevel Subgranting by Power of Attorney and OAuth Authorization Server in Cyber–Physical Systems. *IEEE Internet Things J.* **2023**, *10*, 15266–15282. [CrossRef]
133. Chen, D.; Zhang, L.; Liao, Z.; Dai, H.N.; Zhang, N.; Shen, X.; Pang, M. Flexible and Fine-Grained Access Control for EHR in Blockchain-Assisted E-Healthcare Systems. *IEEE Internet Things J.* **2024**, *11*, 10992–11007. [CrossRef]
134. Sun, J.; Bao, Y.; Qiu, W.; Lu, R.; Zhang, S.; Guan, Y.; Cheng, X. Privacy-Preserving Fine-Grained Data Sharing with Dynamic Service for the Cloud-Edge IoT. *IEEE Trans. Dependable Secur. Comput.* **2025**, *22*, 1329–1346. [CrossRef]
135. Hernandez-Ramos, J.L.; Pawlowski, M.P.; Jara, A.J.; Skarmeta, A.F.; Ladid, L. Toward a Lightweight Authentication and Authorization Framework for Smart Objects. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 690–702. [CrossRef]
136. Kim, D.Y.; Min, S.D.; Kim, S. A DPN (Delegated Proof of Node) Mechanism for Secure Data Transmission in IoT Services. *Comput. Mater. Contin.* **2019**, *58*, 1–14. [CrossRef]
137. Morales, A.; Robles, T.; Alcarria, R.; Cedeño, E. A Hot-topic based Distribution and Notification of Events in Pub/Sub Mobile Brokers. *Netw. Protoc. Algorithms* **2013**, *5*, 90–110. [CrossRef]
138. Hernández-Ramos, J.; Jara, A.J.; Marin, L.; Skarmeta, A. Distributed Capability-based Access Control for the Internet of Things. *J. Internet Serv. Inf. Secur. (JISIS)* **2013**, *3*, 1–16.
139. Outchakoucht, A.; Es-Samaali, H.; Philippe, J. Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 417–424. [CrossRef]
140. Yang, L.; Zheng, Q.; Fan, X. RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks. In Proceedings of the IEEE INFOCOM 2017—IEEE Conference on Computer Communications, Atlanta, GA, USA, 1–4 May 2017; pp. 1–9. [CrossRef]
141. Ko, H.; Jin, J.; Keoh, S.L. ViotSOC: Controlling Access to Dynamically Virtualized IoT Services using Service Object Capability. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, Abu Dhabi, United Arab Emirates, 2 April 2017; pp. 69–80. [CrossRef]
142. Tapas, N.; Merlino, G.; Longo, F. Blockchain-Based IoT-Cloud Authorization and Delegation. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Sicily, Italy, 18–20 June 2018; pp. 411–416. [CrossRef]
143. Sabrina, F. A Novel Entitlement-based Blockchain-enabled Security Architecture for IoT. In Proceedings of the 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand, 27–29 November 2019; pp. 1–7. [CrossRef]
144. Porwal, S.; Mittal, S. A Secure Key Delegation Mechanism for Fog Networking. In Proceedings of the 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 8–10 August 2019; pp. 1–7. [CrossRef]
145. Sun, S.; Chen, S.; Du, R.; Li, W.; Qi, D. Blockchain Based Fine-Grained and Scalable Access Control for IoT Security and Privacy. In Proceedings of the 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), Hangzhou, China, 23–25 June 2019; pp. 598–603. [CrossRef]

146. Ali, G.; Ahmad, N.; Cao, Y.; Asif, M.; Cruickshank, H.; Ali, Q.E. Blockchain based permission delegation and access control in Internet of Things (BACI). *Comput. Secur.* **2019**, *86*, 318–334. [CrossRef]
147. Zemmoudj, S.; Bermad, N.; Omar, M. Context-aware pseudonymization and authorization model for IoT-based smart hospitals. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 4473–4490. [CrossRef]
148. Pinjala, S.K.; Sivalingam, K.M. DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 13–18. [CrossRef]
149. Xu, L.; Li, J.; Chen, X.; Li, W.; Tang, S.; Wu, H.T. Tc-PEDCKS: Towards time controlled public key encryption with delegatable conjunctive keyword search for Internet of Things. *J. Netw. Comput. Appl.* **2019**, *128*, 11–20. [CrossRef]
150. Deng, H.; Qin, Z.; Sha, L.; Yin, H. A Flexible Privacy-Preserving Data Sharing Scheme in Cloud-Assisted IoT. *IEEE Internet Things J.* **2020**, *7*, 11601–11611. [CrossRef]
151. Nakamura, Y.; Zhang, Y.; Sasabe, M.; Kasahara, S. Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things. *Sensors* **2020**, *20*, 1793. [CrossRef]
152. Pal, S.; Rabehaja, T.; Hill, A.; Hitchens, M.; Varadharajan, V. On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation. *IEEE Internet Things J.* **2020**, *7*, 2630–2639. [CrossRef]
153. Puggioni, E.; Shaghaghi, A.; Doss, R.; Kanhere, S.S. Towards Decentralized IoT Updates Delivery Leveraging Blockchain and Zero-Knowledge Proofs. In Proceedings of the 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 24–27 November 2020; pp. 1–10. [CrossRef]
154. Ali, G.; Ahmad, N.; Cao, Y.; Khan, S.; Cruickshank, H.; Qazi, E.A.; Ali, A. xDBAuth: Blockchain Based Cross Domain Authentication and Authorization Framework for Internet of Things. *IEEE Access* **2020**, *8*, 58800–58816. [CrossRef]
155. Zhou, X.; Xu, K.; Wang, N.; Jiao, J.; Dong, N.; Han, M.; Xu, H. A Secure and Privacy-Preserving Machine Learning Model Sharing Scheme for Edge-Enabled IoT. *IEEE Access* **2021**, *9*, 17256–17265. [CrossRef]
156. Zhao, J.; Zeng, P.; Choo, K.K.R. An Efficient Access Control Scheme with Outsourcing and Attribute Revocation for Fog-Enabled E-Health. *IEEE Access* **2021**, *9*, 13789–13799. [CrossRef]
157. Zhang, Y.; Liu, W.; Xia, Z.; Wang, Z.; Liu, L.; Zhang, W.; Zhang, H.; Fang, B. Blockchain-Based DNS Root Zone Management Decentralization for Internet of Things. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6620236. [CrossRef]
158. Ullah, I.; Alkhalifah, A.; Khan, M.A.; Mostafa, S.M. Cost-Effective Proxy Signcryption Scheme for Internet of Things. *Mob. Inf. Syst.* **2021**, *2021*, 2427434. [CrossRef]
159. Sabrina, F.; Jang-Jaccard, J. Entitlement-Based Access Control for Smart Cities Using Blockchain. *Sensors* **2021**, *21*, 5264. [CrossRef]
160. Skarlat, O.; Schulte, S. FogFrame: A framework for IoT application execution in the fog. *PeerJ Comput. Sci.* **2021**, *7*, e588. [CrossRef]
161. Lastname, F.; Lastname, F.; Lastname, F. A Bidirectional Trust Model for Service Delegation in Social Internet of Things. *Future Internet* **2022**, *14*, 135. [CrossRef]
162. Chien, H.Y.; Wang, N.Z. A Novel MQTT 5.0-Based Over-the-Air Updating Architecture Facilitating Stronger Security. *Electronics* **2022**, *11*, 3899. [CrossRef]
163. Cha, H.J.; Yang, H.K.; Song, Y.J. A Study on Vehicle Monitoring Service Using Attribute-Based Security Scheme in Cyber–Physical Systems. *Appl. Sci.* **2022**, *12*, 4300. [CrossRef]
164. Li, C.; Li, F.; Huang, C.; Yin, L.; Luo, T.; Wang, B. A Traceable Capability-based Access Control for IoT. *Comput. Mater. Contin.* **2022**, *72*, 4967–4982. [CrossRef]
165. Ali, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors* **2022**, *22*, 572. [CrossRef]
166. Bayreuther, S.; Jacob, F.; Grotz, M.; Kartmann, R.; Peller-Konrad, F.; Paus, F.; Hartenstein, H.; Asfour, T. BlueSky: Combining Task Planning and Activity-Centric Access Control for Assistive Humanoid Robots. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, New York, NY, USA, 8–10 June 2022; pp. 185–194. [CrossRef]
167. Xiong, H.; Wang, L.; Zhou, Z.; Zhao, Z.; Huang, X.; Kumari, S. Burn After Reading: Adaptively Secure Puncturable Identity-Based Proxy Re-Encryption Scheme for Securing Group Message. *IEEE Internet Things J.* **2022**, *9*, 11248–11260. [CrossRef]
168. Latif, R. ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things. *IEEE Access* **2022**, *10*, 46526–46537. [CrossRef]
169. Xue, L. DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System. *IEEE Access* **2022**, *10*, 30779–30791. [CrossRef]
170. Pinjala, S.K.; Vivek, S.S.; Sivalingam, K.M. Delegated Anonymous Credentials with Revocation Capability for IoT Service Chains (*DANCIS*). *IEEE Internet Things J.* **2022**, *9*, 3729–3742. [CrossRef]
171. Silva, C.; Barraca, J.P. Dynamic Delegation-based Privacy Preserving in IoT Architectures. In Proceedings of the 2022 9th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 22–24 August 2022; pp. 46–54. [CrossRef]

172. Banerjee, A.; Sufian, A.; Paul, K.K.; Gupta, S.K. EDTP: Energy and Delay Optimized Trajectory Planning for UAV-IoT Environment. *Comput. Netw.* **2022**, *202*, 108623. [CrossRef]
173. Qushtom, H.; Misic, J.; Misic, V.B. Efficient multi-tier, multiple entry PBFT consensus algorithm for IoT. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 44–49. [CrossRef]
174. Heo, J.; Jang, H.; Lee, H. How to divide a permission token in the delegation process of blockchain-based access control for IoT. In Proceedings of the 2022 IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 25–28 April 2022; pp. 1–8. [CrossRef]
175. Ju, C.; Tang, W.; Chenli, C.; Lee, G.; Seo, J.H.; Jung, T. Monitoring Provenance of Delegated Personal Data with Blockchain. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 22–25 August 2022; pp. 11–20. [CrossRef]
176. Panneerselvam, N.; Krithiga, S. Mutual-contained access delegation scheme for the Internet of Things user services. *Distrib. Parallel Databases* **2022**, *40*, 835–860. [CrossRef]
177. Wang, J.; Chow, S.S.M. Omnes pro uno: Practical Multi-Writer Encrypted Database. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 2371–2388.
178. Sama, M.R.; Kiess, W.; Guerzoni, R.; Thakolsri, S.; Jurjens, J. Redefining the Trust Model for the Internet of Everything in the 6G era. In Proceedings of the 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan, 12–15 September 2022; pp. 1400–1406. [CrossRef]
179. Shur, D.; Di Crescenzo, G.; Zhang, Q.; Chen, T.; Krishnan, R.; Lin, Y.J.; Patni, Z.; Alexander, S.; Tsudik, G. SEDIMENT: An IoT-device-centric Methodology for Scalable 5G Network Security. In Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022; pp. 49–54. [CrossRef]
180. Tanyingyong, V.; Olsson, R.; Hidell, M.; Sjodin, P. Scalable IoT Sensing Systems with Dynamic Sinks. *IEEE Internet Things J.* **2022**, *9*, 7211–7227. [CrossRef]
181. Goh, Y.; Yun, J.; Jung, D.; Chung, J.M. Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning. *IEEE Access* **2022**, *10*, 118498–118511. [CrossRef]
182. Qiao, Z.; Zhou, Y.; Yang, B.; Zhang, M.; Wang, T.; Xia, Z. Secure and Efficient Certificate-Based Proxy Signature Schemes for Industrial Internet of Things. *IEEE Syst. J.* **2022**, *16*, 4719–4730. [CrossRef]
183. Rios, E.; Higuero, M.; Larrucea, X.; Rak, M.; Casola, V.; Iturbe, E. Security and Privacy Service Level Agreement composition for Internet of Things systems on top of standard controls. *Comput. Electr. Eng.* **2022**, *98*, 107690. [CrossRef]
184. Wanniarachchi, S.T.; Turau, V. A Fault-Tolerant Distributed Air-to-Ground Communication Architecture for Urban Air Mobility. In Proceedings of the 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Pafos, Cyprus, 19–21 June 2023; pp. 639–646. [CrossRef]
185. Wang, C.; Wu, B. A Linear Homomorphic Proxy Signature Scheme Based on Blockchain for Internet of Things. *Comput. Model. Eng. Sci.* **2023**, *136*, 1857–1878. [CrossRef]
186. Alharbi, A. Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System. *Sensors* **2023**, *23*, 3020. [CrossRef]
187. Malhotra, A. Blend CAC: Integration for the Blockchain for Distributed Potential Network Access for the Internet of Things. In Proceedings of the 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 27–29 January 2023; pp. 1145–1149. [CrossRef]
188. Lu, Y.; Wang, D.; Obaidat, M.S.; Vijayakumar, P. Edge-Assisted Intelligent Device Authentication in Cyber–Physical Systems. *IEEE Internet Things J.* **2023**, *10*, 3057–3070. [CrossRef]
189. Trivedi, H.S.; Patel, S.J. Key-aggregate searchable encryption with multi-user authorization and keyword untraceability for distributed IoT healthcare systems. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4734. [CrossRef]
190. Sahraoui, S.; Henni, N. SAMP-RPL: Secure and adaptive multipath RPL for enhanced security and reliability in heterogeneous IoT-connected low power and lossy networks. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 409–429. [CrossRef]
191. Hamad, M.; Finkenzeller, A.; Liu, H.; Lauinger, J.; Prevelakis, V.; Steinhorst, S. SEEMQTT: Secure End-to-End MQTT-Based Communication for Mobile IoT Systems Using Secret Sharing and Trust Delegation. *IEEE Internet Things J.* **2023**, *10*, 3384–3406. [CrossRef]
192. Seifhosseini, S.; Hosseini Shirvani, M.; Ramzanpoor, Y. Multi-objective cost-aware bag-of-tasks scheduling optimization model for IoT applications running on heterogeneous fog environment. *Comput. Netw.* **2024**, *240*, 110161. [CrossRef]
193. Fan, X.; Chai, Q. Roll-DPoS: A Randomized Delegated Proof of Stake Scheme for Scalable Blockchain-Based Internet of Things Systems. In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, NY, USA, 5–7 November 2018; pp. 482–484. [CrossRef]
194. Maselli, G.; Piva, M.; Restuccia, F. HyBloSE: Hybrid blockchain for secure-by-design smart environments. In Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, London UK, 25 September 2020; pp. 23–28. [CrossRef]

195. Vairagade, R.S.; Brahmananda, S.H. Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks. *Trans. Emerg. Telecommun. Technol.* **2021**, *33*, e4433. [CrossRef]
196. Wang, Y.; Che, T.; Zhao, X.; Zhou, T.; Zhang, K.; Hu, X. A Blockchain-Based Privacy Information Security Sharing Scheme in Industrial Internet of Things. *Sensors* **2022**, *22*, 3426. [CrossRef]
197. Huang, X.; Zhang, Y.; Li, D.; Han, L. A Solution for Bilayer Energy-Trading Management in Microgrids Using Multiblockchain. *IEEE Internet Things J.* **2022**, *9*, 13886–13900. [CrossRef]
198. Ahmed, I.; Zhang, Y.; Jeon, G.; Lin, W.; Khosravi, M.R.; Qi, L. A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. *Int. J. Intell. Syst.* **2022**, *37*, 6493–6507. [CrossRef]
199. Wang, P.; Zhao, Y.; Obaidat, M.S.; Wei, Z.; Qi, H.; Lin, C.; Xiao, Y.; Zhang, Q. Blockchain-Enhanced Federated Learning Market with Social Internet of Things. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3405–3421. [CrossRef]
200. Wang, H.; Jiang, H.; Wu, J.; Zhou, P.; Huang, H. Blockchain-Governed Federated Transfer Learning for Secure Internet of Drones Networks. *IEEE Internet Things Mag.* **2022**, *5*, 134–139. [CrossRef]
201. Zhi, H.; Ge, H.; Wang, Y. Cooperative Communication Method Based on Block Chain for a Large Number of Distributed Terminals. *IEEE Access* **2022**, *10*, 11679–11695. [CrossRef]
202. Kaur, M.; Gupta, S.; Kumar, D.; Verma, C.; Neagu, B.C.; Raboaca, M.S. Delegated Proof of Accessibility (DPoAC): A Novel Consensus Protocol for Blockchain Systems. *Mathematics* **2022**, *10*, 2336. [CrossRef]
203. Geng, T.; Njilla, L.; Huang, C.T. Delegated Proof of Secret Sharing: A Privacy-Preserving Consensus Protocol Based on Secure Multiparty Computation for IoT Environment. *Network* **2022**, *2*, 66–80. [CrossRef]
204. Misic, J.; Misic, V.B.; Chang, X. Delegated Proof of Stake Consensus with Mobile Voters and Multiple Entry PBFT Voting. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 6253–6258. [CrossRef]
205. Yang, L.; Zou, W.; Wang, J.; Tang, Z. EdgeShare: A blockchain-based edge data-sharing framework for Industrial Internet of Things. *Neurocomputing* **2022**, *485*, 219–232. [CrossRef]
206. Ledwaba, L.P.; Hancke, G.P.; Isaac, S.J. Investigating Distance Bounding for Delegated Proof-of-Proximity Consensus within IIoT. In Proceedings of the 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE), Anchorage, AK, USA, 1–3 June 2022; pp. 627–630. [CrossRef]
207. Hu, D.; Chen, J.; Zhou, H.; Yu, K.; Qian, B.; Xu, W. Leveraging Blockchain for Multi-Operator Access Sharing Management in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2774–2787. [CrossRef]
208. Bachani, V.; Bhattacharjya, A. Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS. *Symmetry* **2022**, *15*, 4. [CrossRef]
209. Cui, J.; Ouyang, F.; Ying, Z.; Wei, L.; Zhong, H. Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 8857–8867. [CrossRef]
210. Sasikumar, A.; Ravi, L.; Kotecha, K.; Saini, J.R.; Varadarajan, V.; Subramaniyaswamy, V. Sustainable Smart Industry: A Secure and Energy Efficient Consensus Mechanism for Artificial Intelligence Enabled Industrial Internet of Things. *Comput. Intell. Neurosci.* **2022**, *2022*, 1419360. [CrossRef]
211. Wang, Y.; Su, Z.; Xu, Q.; Li, R.; Luan, T.H.; Wang, P. A Secure and Intelligent Data Sharing Scheme for UAV-Assisted Disaster Rescue. *IEEE/ACM Trans. Netw.* **2023**, *31*, 2422–2438. [CrossRef]
212. Namasudra, S.; Sharma, P. Achieving a Decentralized and Secure Cab Sharing System Using Blockchain Technology. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 15568–15577. [CrossRef]
213. Zhao, J.; Hu, H.; Huang, F.; Guo, Y.; Liao, L. Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios. *Electronics* **2023**, *12*, 1812. [CrossRef]
214. Wang, J.; Lin, X.; Wu, Y.; Wu, J. Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT. *IEEE Internet Things J.* **2023**, *10*, 21566–21579. [CrossRef]
215. Razaque, A.; Yoo, J.; Bektemyssova, G.; Alshammari, M.; Chinibayeva, T.T.; Amanzholova, S.; Alotaibi, A.; Umutkulov, D. Efficient Internet-of-Things Cyberattack Depletion Using Blockchain-Enabled Software-Defined Networking and 6G Network Technology. *Sensors* **2023**, *23*, 9690. [CrossRef]
216. Alghamdi, S.; Albeshri, A.; Alhusayni, A. Enabling a Secure IoT Environment Using a Blockchain-Based Local-Global Consensus Manager. *Electronics* **2023**, *12*, 3721. [CrossRef]
217. Cullen, A.; Zhao, L.; Vigneri, L.; Shorten, R. Improving Quality of Service for Users of Leaderless DAG-Based Distributed Ledgers. *Distrib. Ledger Technol. Res. Pract.* **2023**, *2*, 1–18. [CrossRef]
218. Qi, L.; Tian, J.; Chai, M.; Cai, H. LightPoW: A trust based time-constrained PoW for blockchain in Internet of Things. *Comput. Netw.* **2023**, *220*, 109480. [CrossRef]
219. Kaur, M.; Gupta, S. Optimization of a Consensus Protocol in Blockchain-IoT Convergence. In Proceedings of the 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 1–3 March 2023; pp. 1–5.

220. Yang, F.; Xu, F.; Feng, T.; Qiu, C.; Zhao, C. pDPoSt+sPBFT: A High Performance Blockchain-Assisted Parallel Reinforcement Learning in Industrial Edge-Cloud Collaborative Network. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 2744–2759. [CrossRef]
221. Mingjie Zhao, M.Z.; Mingjie Zhao, C.D.; Cheng Dai, B.G. Safe and Efficient Delegated Proof of Stake Consensus Mechanism Based on Dynamic Credit in Electronic Transaction. *J. Internet Technol.* **2023**, *24*, 123–133. [CrossRef]
222. Wang, L.; Zheng, Y.; Zhang, Y.; Li, F. Secure Spectrum Sharing for Satellite Internet-of-Things Based on Blockchain. *Wirel. Pers. Commun.* **2023**, *131*, 357–369. [CrossRef]
223. Xiao, N.; Wang, Z.; Sun, X.; Miao, J. A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alex. Eng. J.* **2024**, *86*, 631–643. [CrossRef]
224. Lin, L.; Wu, J.; Zhou, Z.; Zhao, J.; Li, P.; Xiong, J. Computing Power Networking Meets Blockchain: A Reputation-Enhanced Trading Framework for Decentralized IoT Cloud Services. *IEEE Internet Things J.* **2024**, *11*, 17082–17096. [CrossRef]
225. Mohammed, M.A.; Wahab, H.B.A. Enhancing IoT Data Security with Lightweight Blockchain and Okamoto Uchiyama Homomorphic Encryption. *Comput. Model. Eng. Sci.* **2024**, *138*, 1731–1748. [CrossRef]
226. Tsang, Y.P.; Lee, C.K.M.; Zhang, K.; Wu, C.H.; Ip, W.H. On-Chain and Off-Chain Data Management for Blockchain-Internet of Things: A Multi-Agent Deep Reinforcement Learning Approach. *J. Grid Comput.* **2024**, *22*, 16. [CrossRef]
227. Al-Marridi, A.Z.; Mohamed, A.; Erbad, A. Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning. *J. Netw. Comput. Appl.* **2024**, *224*, 103834. [CrossRef]
228. Jiang, L.; Liu, Y.; Tian, H.; Tang, L.; Xie, S. Resource Efficient Federated Learning and DAG Blockchain with Sharding in Digital Twin Driven Industrial IoT. *IEEE Internet Things J.* **2024**, *11*, 17113–17127. [CrossRef]
229. Wang, Y.; Xing, X.; Li, P.; Wang, G. LT-DBFT: A Hierarchical Blockchain Consensus Using Location and Trust in IoT. *IEEE Internet Things J.* 2025, *early access*. [CrossRef]
230. Leo, M.; Battisti, F.; Carli, M.; Neri, A. A federated architecture approach for Internet of Things security. In Proceedings of the 2014 Euro Med Telco Conference (EMTC), Naples, Italy, 12–15 November 2014; pp. 1–5. [CrossRef]
231. Porambage, P.; Braeken, A.; Kumar, P.; Gurtov, A.; Ylianttila, M. Efficient Key Establishment for Constrained IoT Devices with Collaborative HIP-Based Approach. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]
232. Xu, P.; Tang, X.; Wang, W.; Jin, H.; Yang, L.T. Fast and Parallel Keyword Search Over Public-Key Ciphertexts for Cloud-Assisted IoT. *IEEE Access* **2017**, *5*, 24775–24784. [CrossRef]
233. Huang, Q.; Wang, L.; Yang, Y. DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices. *World Wide Web* **2018**, *21*, 151–167. [CrossRef]
234. Hao, J.; Huang, C.; Liu, J.; Xian, M.; Shen, X. Efficient Outsourced Data Access Control with User Revocation for Cloud-Based IoT. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6. [CrossRef]
235. Nguyen, K.T.; Oualha, N.; Laurent, M. Securely outsourcing the ciphertext-policy attribute-based encryption. *World Wide Web* **2018**, *21*, 169–183. [CrossRef]
236. Moor, L.; Bitter, L.; Prado, M.D.; Pazos, N.; Ouerhani, N. IoT meets distributed AI—Deployment scenarios of Bonseyes AI applications on FIWARE. In Proceedings of the 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), London, UK, 29–31 October 2019; pp. 1–2. [CrossRef]
237. Elhabob, R.; Zhao, Y.; Eltayieb, N.; Abdelgader, A.M.S.; Xiong, H. Identity-based encryption with authorized equivalence test for cloud-assisted IoT. *Clust. Comput.* **2020**, *23*, 1085–1101. [CrossRef]
238. Wang, W.; Xu, P.; Liu, D.; Yang, L.T.; Yan, Z. Lightweighted Secure Searching Over Public-Key Ciphertexts for Edge-Cloud-Assisted Industrial IoT Devices. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4221–4230. [CrossRef]
239. Xu, S.; Ning, J.; Li, Y.; Zhang, Y.; Xu, G.; Huang, X.; Deng, R. Match in My Way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 1064–1077. [CrossRef]
240. Zheng, Y.; Lu, R.; Mamun, M. Privacy-Preserving Computation Offloading for Time-Series Activities Classification in eHealthcare. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
241. Gochhayat, S.P.; Lal, C.; Sharma, L.; Sharma, D.P.; Gupta, D.; Saucedo, J.A.M.; Kose, U. Reliable and secure data transfer in IoT networks. *Wirel. Netw.* **2020**, *26*, 5689–5702. [CrossRef]
242. Tao, Y.; Xu, P.; Jin, H. Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage. *IEEE Access* **2020**, *8*, 15963–15972. [CrossRef]
243. Yi, C.; Cai, J.; Zhu, K.; Wang, R. A Queueing Game Based Management Framework for Fog Computing with Strategic Computing Speed Control. *IEEE Trans. Mob. Comput.* **2022**, *21*, 1537–1551. [CrossRef]
244. Wang, L.; Tian, Y.; Xiong, J. Achieving reliable and anti-collusive outsourcing computation and verification based on blockchain in 5G-enabled IoT. *Digit. Commun. Netw.* **2022**, *8*, 644–653. [CrossRef]

245. De Hoz Diego, J.D.; Temperekidis, A.; Katsaros, P.; Konstantinou, C. An IoT Digital Twin for Cyber-Security Defence Based on Runtime Verification. In *Leveraging Applications of Formal Methods, Verification and Validation. Verification Principles*; Lecture Notes in Computer Science; Margaria, T., Steffen, B., Eds.; Springer International Publishing: Cham, Switzerland, 2022; Volume 13701, pp. 556–574. [CrossRef]
246. Kim, W.B.; Kim, S.H.; Seo, D.; Lee, I.Y. Certificateless Group to Many Broadcast Proxy Reencryptions for Data Sharing towards Multiple Parties in IoTs. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1903197. [CrossRef]
247. Jiang, L.; Qin, Z. Edge-assisted Puncturable Fine-grained Task Distribution for the IoT-oriented Crowdsensing. In Proceedings of the 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Espoo, Finland, 22–25 August 2022; pp. 131–138. [CrossRef]
248. Zhou, J.; Cao, Z.; Dong, X.; Choo, K.K.R. Efficient Privacy-Preserving Outsourced Discrete Wavelet Transform in the Encrypted Domain. *IEEE Trans. Cloud Comput.* **2022**, *10*, 366–382. [CrossRef]
249. Liu, D.; Li, Z.; Wang, C.; Ren, Y. Enabling secure mutual authentication and storage checking in cloud-assisted IoT. *Math. Biosci. Eng.* **2022**, *19*, 11034–11046. [CrossRef]
250. Cai, G.; Wei, X.; Yao, L. Privacy-preserving CNN feature extraction and retrieval over medical images. *Int. J. Intell. Syst.* **2022**, *37*, 9267–9289. [CrossRef]
251. Chen, Y.C.; Chang, C.C.; Hung, C.C.; Lin, J.F.; Hsu, S.Y. SecDT: Privacy-Preserving Outsourced Decision Tree Classification without Polynomial Forms in Edge-Cloud Computing. *IEEE Trans. Signal Inf. Process. Netw.* **2022**, *8*, 1037–1048. [CrossRef]
252. Li, W.; Xia, C.; Wang, C.; Wang, T. Secure and Temporary Access Delegation with Equality Test for Cloud-Assisted IoV. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 20187–20201. [CrossRef]
253. Benomar, Z.; Campobello, G.; Segreto, A.; Battaglia, F.; Longo, F.; Merlino, G.; Puliafito, A. A Fog-Based Architecture for Latency-Sensitive Monitoring Applications in Industrial Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 1908–1918. [CrossRef]
254. Meng, X.; Yang, C.; Qi, Y.; Liang, W.; Xu, Z.; Li, K.; Deng, H. A Novel Multi-Party Authentication Scheme for FCN-based MIoT Systems in Natural Language Processing Environment. In *ACM Transactions on Asian and Low-Resource Language Information Processing*; Association for Computing Machinery: New York, NY, USA, 2023; p. 3590149. [CrossRef]
255. Yao, M.; Gan, Q.; Wang, X.; Yang, Y. A key-insulated secure multi-server authenticated key agreement protocol for edge computing-based VANETs. *Internet Things* **2023**, *21*, 100679. [CrossRef]
256. Chouikhi, S.; Esseghir, M.; Merghem-Boulahia, L. Computation Offloading for Industrial Internet of Things: A Cooperative Approach. In Proceedings of the 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 19–23 June 2023; pp. 626–631. [CrossRef]
257. Song, Z.; Ma, H.; Zhang, R.; Xu, W.; Li, J. Everything Under Control: Secure Data Sharing Mechanism for Cloud-Edge Computing. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 2234–2249. [CrossRef]
258. Atutxa, A.; Astorga, J.; Barcelo, M.; Urbieta, A.; Jacob, E. Improving efficiency and security of IIoT communications using in-network validation of server certificate. *Comput. Ind.* **2023**, *144*, 103802. [CrossRef]
259. Kurt, A.; Akkaya, K.; Yilmaz, S.; Mercan, S. LNGate^2: Secure Bidirectional IoT Micro-Payments Using Bitcoin's Lightning Network and Threshold Cryptography. *IEEE Trans. Mob. Comput.* **2023**, *23*, 6027–6044. [CrossRef]
260. Wang, L.; Huang, C.; Cheng, H. Novel proxy signature from lattice for the post-quantum internet of things. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 9939–9946. [CrossRef]
261. Srikanth, K.; Rajesh, P.G.; Prasad, N.D.; Asmathulla, M.; Reddy, T.P.K. Proxy-Based Re-Encryption Design for the IoT Ecosystem. In Proceedings of the 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 25–26 May 2023; pp. 1–6. [CrossRef]
262. Wu, T.; Ma, X.; Zhang, C.; Liu, X.; Yang, G.; Zhu, L. Towards Fine-Grained Task Allocation with Bilateral Access Control for Intelligent Transportation Systems. *IEEE Internet Things J.* **2023**, *11*, 14814–14828. [CrossRef]
263. Sun, Y.; Du, X.; Niu, S.; Zhou, S. A lightweight attribute-based signcryption scheme based on cloud-fog assisted in smart healthcare. *PLoS ONE* **2024**, *19*, e0297002. [CrossRef] [PubMed]
264. Routray, K.; Bera, P. Fog-Assisted Dynamic IoT Device Access Management Using Attribute-Based Encryption. In Proceedings of the 25th International Conference on Distributed Computing and Networking, Chennai, India, 4–7 January 2024; pp. 346–352. [CrossRef]
265. Qu, Z.; Meng, Y.; Liu, B.; Muhammad, G.; Tiwari, P. QB-IMD: A Secure Medical Data Processing System with Privacy Protection Based on Quantum Blockchain for IoMT. *IEEE Internet Things J.* **2024**, *11*, 40–49. [CrossRef]