Computers & Security 135 (2023) 103472

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Access control in Internet of Things: A survey

Rahma Trabelsi *, Ghofrane Fersi, Mohamed Jmaiel

ReDCAD laboratory, National Engineering School of Sfax (ENIS), University of Sfax, B.P. 1173, Soukra, 3038, Sfax, Tunisia

ARTICLE INFO

Keywords:
Access control
IoT
Fog computing
Blockchain
Survey

ABSTRACT

The speedy boom of Internet of Things (IoT) devices has revolutionized many fields including smart cities, healthcare, smart homes, etc. Most of these devices exchange sensitive and private data. Due to their exposure to the Internet, the IoT devices can be easily victims of hacking and tampering attacks. Also, attacks that seek to alter their settings, change their behavior and exhaust their resources are very common. Access control solutions help considerably IoT systems to efficiently cope with these attacks and ensure the required security level. In this paper, we survey the most relevant IoT access control solutions starting from the basic centralized ones to the more modern and distributed solutions that rely on emerging technologies such as blockchain and fog computing. Additionally, our work offers a spotlight on the IoT inter-organizational access control solutions. We demystify the challenges, problems and benefits of each surveyed approach. Furthermore, a novel taxonomy of the access control approaches according to their architecture, underlying layers and organizational aspect is proposed. Based on our deep study, we present the future directions of access control in the age of IoT.

1. Introduction

IoT is defined as a large-scale environment that connects various heterogeneous devices together (Rejeb et al., 2023; Hemmati and Rahmani, 2022). These devices interact with each other, exchange important data and proceed different sensitive actions via their actuators. Uncontrolled access to these data or resources may lead to harmful consequences. For example, in the healthcare sector (Saini et al., 2020; Sookhak et al., 2021), IoT devices collect sensitive data about the health status of patients and send them to a remote server where it will be stored and analyzed to take appropriate decisions. If an attacker manages to access these data and modifies them, the decision to be taken could be wrong and may be harmful to the patient. In a smart home scenario for example, a black hat hacker may access the cameras of a smart home and becomes able to spy on the inhabitants without their consent and knowledge. It is hence crucial to ensure a dedicated access control scheme to avoid these attacks particularly when the IoT devices acquire very sensitive data and any inappropriate access of one of them may lead to a breach of the users' privacy and/or disturbance of the whole IoT system.

Access control mechanisms overcome numerous security challenges in IoT environments (Stolojescu-Crisan et al., 2022) and prevent unauthorized access to data and resources (Ouaddah et al., 2016b). Many researchers (Alshehri and Sandhu, 2017) implemented different access control solutions that are disparate in techniques, policies, underlying technologies, each of which has advantages and drawbacks. In this paper, we provide an overview of these solutions, classify and evaluate them according to different criteria like scalability, dynamicity, distribution, complexity etc.

It is worth noting that access control solutions for IoT systems have been the subject of numerous surveys like (Akhuseyinoglu et al., 2020; Ouaddah et al., 2017; Abdulrahman et al., 2021) and (Singh and Singh, 2022). Some are no longer relevant Ouaddah et al. (2017), others have limited scope focusing on a specific technology (Malik et al., 2020; Ravidas et al., 2019; Abdulrahman et al., 2021; Singh and Singh, 2022), such as blockchain (Pal et al., 2022; Saha et al., 2022). The common drawback of these surveys is the level of granularity of the criteria they use to classify existing solutions and approaches. In fact, a fine-grained classification allows the readers to fully understand the specifications of each class. Furthermore, it helps researchers who are focusing on a specific access control domain to easily find and study the concerned solutions. Without such classifications, the reader spends more time to find the appropriate and required information from surveys. Here, we address these limitations by providing an up-to-date survey, targeting numerous existing IoT access control solutions, comparing and classifying them according to fine-grained criteria, such as simplicity, distribution and real-time response. In addition, we provide a list of open issues and propose new research directions in this area.

* Corresponding author.
E-mail address: rahma.trabelsi@redcad.org (R. Trabelsi).

https://doi.org/10.1016/j.cose.2023.103472
Received 22 March 2023; Received in revised form 13 August 2023; Accepted 5 September 2023
Available online 12 September 2023

In order to be exhaustive while addressing the most critical IoT systems, our study encompasses many IoT solution domains. It includes access control solutions for infrastructure-based IoT systems like smart grids and smart cities, residential IoT systems like wearables and Smart Offices/Home Offices (SOHO) and fog and cloud computing-based IoT systems as well as real-time IoT systems used in healthcare and telemedicine.

As a result, our survey provides the researchers with a study of the most relevant IoT access control solutions. It offers a deep inspection of them from different sides like architecture, access control model and applicability in inter-organizational networks. It also offers a structured and systematic analysis enabling the readers to understand the access control concept in general and to foster their consciousness about the specificity and variety of access control solutions. Moreover, it builds a clear idea about the role of emerging technologies like fog computing, blockchain and deep learning in the consolidation and the prosper of new access control solutions for IoT systems.

The remaining parts of our paper are organized as follows. The related work is given in section 2. In section 3, we present an overview of the IoT. We outline the access control models in section 4. Section 5 demystifies the various access control solutions while proposing a taxonomy of them. We discuss the different access control solutions and specify the various open issues in section 6. Finally, section 7 concludes the paper. Table 1 presents the list of abbreviations used in our paper.

2. Related work

In this section, we present other surveys that have studied IoT access control solutions and we highlight the difference and the novelty of our paper compared to them. Ouaddah et al. (2017) presented a detailed study of the access control models and studied the access control solutions that are based on them. The main limitation of this survey is that it only focused on access control solutions that are based on access control models. These solutions present only a small subset of the overall access control solutions that really exist in the literature. In contrast, our survey includes different types and structures of access control solutions, whether they rely on a specific access control model or not.

Ravidas et al. (2019), Ragothaman et al. (2023), and Bertin et al. (2019) presented different access control models and evaluated related work based on IoT objectives. Moreover, they presented a thorough analysis of the current state-of-the-art technologies of access control for IoT and gave discussions of technical challenges facing IoT access control techniques. The aforementioned surveys focused on access control policies, discussed them and presented their limitations. In spite of the importance of the conducted study in the cited surveys, they present various drawbacks. Effectively, they did not focus on the architectural concept of the access control solutions and they did not deal with inter-organizational access control solutions. However, these two concepts are of high importance for industries and organizations. In fact, numerous industries and organizations should comply with regulatory requirements. Studying access control architectures and understanding how access control among organizations can be established, helps them ensure compliance with relevant regulations, such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act HIPAA, etc. Compliance generally includes the implementation of specific access control measures, such as strong authentication mechanisms or data encryption. Without understanding the architecture of the access control solutions and their plan to manage the inter-organizational access, it is almost difficult to choose the suitable solution that is able to fulfill the regulatory requirements. To bridge this gap, we present a deep study of the access control solutions based on their architectures and we demystify the different layers that are constructing the access control solutions. We focus also in our survey on access control in the organizational context and provide the advantages and limitations of each solution. It is also worth noting that none of the previously cited surveys studied the impact of adding the fog computing layer between the IoT layer and the application layer to improve the performance of access control solutions. Particularly, our survey differs from existing ones by presenting an in-depth study of the fog-based access control solutions and by highlighting their advantages in overcoming the IoT devices resource shortage constraints and in improving their performance.

Qiu et al. (2020) focused on policy description and combination methods, conflicts detection and resolution and access control policy authorization. Although this work presents an in-depth study of access control solutions in IoT systems, it lacks attention to emerging technologies that play major roles in IoT access control such as blockchain and fog computing. We bridge this gap in our survey by giving an insight on the importance of these technologies to offer more reliable and efficient access control for IoT systems.

Many surveys focused on blockchain-based access control solutions for IoT. Rouhani and Deters (2019) overviewed the problems of current access control solutions and presented the added value of blockchain

Table 1
List of abbreviations.

Abbreviation	Definition
IoT	Internet of Things
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
VANET	Vehicular Ad hoc Network
SOHO	Smart Offices/Home Offices
DAC	Discretionary Access Control
MAC	Mandatory Access Control
RBAC	Role-Based Access Control
ABAC	Attribute-Based Access Control
PEP	Policy Enforcement Point
PDP	Policy Decision Point
PIP	Policy Information Point
OrBAC	Organization-Based Access Control
CapBAC	Capability-Based Access Control
UCON	Usage Control
XACML	eXtensible Access Control Markup Language
SMAC	Simple Messaging and Access Control
CNN	Convolutional Neural Network
FDL	Federated Deep Learning
P2P	Peer-to-Peer
IPFS	InterPlanetary File System
ACE	Authorization for Constrained Environments
AC	Access Contract
PC	Policy Contract
DC	Device Contract
PMC	Policy Management Contract
SAMC	Subject Attribute Management Contract
OAMC	Object Attribute Management Contract
ACC	Access Control Contract
SA	Subject Attributes
OA	Object Attributes
BLP	Bell-Lapadula
ss-policy	simple security policy
*-policy	star policy
TTP	Trusted Third Party
IIoT	Industrial Internet of Things
DCapBAC	Distributed Capability-Based Access Control model
SEA	Symmetric Encryption Algorithm
VPN	Virtual Private Network
ACL	Access Control Lists
PUF	Physically Unclonable Function
SPs	Service Providers
SMs	Smart Meters
CP-ABE	Ciphertext Policy and Attribute-Based Encryption
PHR	Personal Health Record
ECC	Elliptic Curve Cryptography
ABE	Attribute-Based Encryption
QKD	Quantum Key Distribution
QC	Quantum Cryptography
TRAC	Traceable and Revocable Access Control
mHealth	Mobile Health
VPNBDAC	Virtual Private Network Blockchain-based Dynamic Access Control
SD-IoT	Software-Defined Internet of Things

Table 2
Comparison of our survey to related work.

	Ouaddah et al. (2017) Bertin et al. (2019)	Ravidas et al. (2019)	Rouhani and Deters (2019)	Riabi et al. (2019)	Abdi et al. (2020)	Qiu et al. (2020)	Patil et al. (2021)	Abdulrahman et al. (2021)	Singh and Singh (2022) Hussain et al. (2021) Namane and Ben Dhaou (2022) Bagga et al. (2022)	Our Survey
Access control models	Full coverage	Partial coverage	Partial coverage	No coverage	Full coverage	Full coverage	Partial coverage	Partial coverage	No coverage	✓ **Full coverage**
Centralized solutions	Partial coverage	No coverage	No coverage	No coverage	Partial coverage	No coverage	No coverage	No coverage	No coverage	✓ **Full coverage**
Distributed solutions	No coverage	No coverage	No coverage	No coverage	Partial coverage	No coverage	No coverage	No coverage	No coverage	✓ **Full coverage**
Blockchain-based Solution	No coverage	No coverage	Partial coverage	Partial coverage	Partial coverage	No coverage	Partial coverage	Partial coverage	Partial coverage	✓ **Full coverage**
Access control solution evaluation	According to scalability, usability, flexibility, interoperability, context awareness, distribution, real-time response, heterogeneity, lightweight, user-driven and granularity.	Evaluation of solutions between (2010-2018) according to context-awareness, policy generation, policy configuration, multi-domain administration.	No evaluation	Advantages and disadvantages of transaction-based solutions and smart contract-based solutions	According to scalability, distribution, user-centric, data-privacy, user-privacy, self-enforcing-policies and security	No evaluation	According to scalability, decentralization, privacy, extensibility and reduced computational overhead	No evaluation	In Singh and Singh (2022), Hussain et al. (2021) and Namane and Ben Dhaou (2022) according to authentication, computational cost, scalability, memory overhead and communication cost. In Bagga et al. (2022), evaluation according to computation and communication costs.	**According to scalability, decentralization, dynamicity, complexity and real-time response. We also evaluate access control models.**

and challenges of its integration in IoT environment. They admitted that blockchain may not be the optimal choice for storing a significant amount of information. Therefore, it is recommended to utilize secure off-chain storage solutions for data storage purposes. Likewise, Riabi et al. (2019) presented the benefits of the integration of blockchain in access control solutions including distribution, heterogeneity, scalability, security and privacy. They classified solutions into two main types: transaction-based solutions and smart contract-based solutions, and presented the advantages and disadvantages of each class. Abdi et al. (2020) presented an overview of blockchain technology and its platform. They have compared different blockchain platforms. Based on this comparison, they affirmed that private and consortium blockchains are more suitable for IoT, due to low latency and high transaction rate. Patil et al. (2021) showed the effectiveness of utilizing blockchain technology in several domains, such as healthcare, IoT access control, supply chain and Vehicular Ad Hoc Networks (VANETs). They analyzed the existing security techniques in these domains, according to these criteria: storage and computation overhead, scalability, privacy, extensibility and accuracy. In addition, they classified the existing related works according to several categories such as the distributed access control category, distributed key management category and token-based access control category. Based on their analysis, they concluded that employing a consortium blockchain coupled with a robust consensus algorithm, offers a better solution for various applications. Bagga et al. (2022) presented a review about IoT including its architecture, its security requirements, its domain of application and its security attacks. Then, they discussed the use of blockchain for IoT security. They classified the access control solutions as certificate-based, certificate-less and blockchain-based. Also, they elaborated a comparative analysis of the existing access control solutions and compared them in terms of computation and communication costs. Abdulrahman et al. (2021) surveyed blockchain types and classified solutions according to these types. In their study, they summarized the requirements for designing blockchain-based solutions in IoT environments that satisfy properties like scalability, lightweight, dynamicity, latency, delegation and revocation. Singh and Singh (2022) have introduced merits and challenges of different blockchain-based access control systems. They concluded that smart contract technology can solve security issues for IoT networks to a certain extent. Hussain et al. (2021) used two groups to classify the blockchain-based access control solutions. The first group is made up of solutions based on transactions. The second group consists of solutions that used the smart contract technology. However, they only used two comparison criteria: implementation and security levels. Namane and Ben Dhaou (2022) proposed a blockchain-based access control taxonomy according to the access control nature: partially decentralized and fully decentralized. Then, they classified solutions according to IoT domains so that they address access control requirements for each application domain. Finally, they provided a deep analysis of recent authorization frameworks.

The above discussed papers (Rouhani and Deters, 2019; Riabi et al., 2019; Abdi et al., 2020; Patil et al., 2021; Bagga et al., 2022; Abdulrahman et al., 2021; Singh and Singh, 2022; Hussain et al., 2021) and (Namane and Ben Dhaou, 2022) focused only on blockchain-based access control solutions and did not study the blockchain-free approaches. Unlike these studies, our survey presents a more extensive investigation of the IoT access control solutions that encompass technologies such as cryptography, fog computing, deep learning, etc. Furthermore, most of the priorly mentioned surveys evaluated access control solutions according to handful criteria like scalability, privacy and complexity.

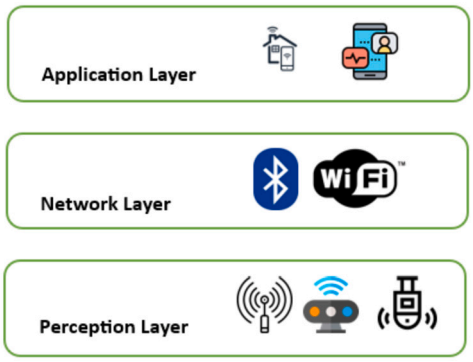

Fig. 1. Three-layer IoT architecture.

In spite of the importance of these evaluation criteria, they are not sufficient to offer an objective and in-depth evaluation. In contrast, our survey presents a more rigorous evaluation by the specification of stringent, thorough and insightful criteria like scalability, distribution, complexity, real-time responsiveness, dynamicity, user-driven and granularity.

To summarize, our survey presents a wider and more recent systematic analysis of existing access control solutions. It clarifies the requirements and presents the access control models. Also, it studies the different access control approaches in the IoT field and evaluates them. The added value of our work in comparison to the existing ones, is the deep study of blockchain-based solutions in addition to the traditional ones in the IoT access control field. Additionally, in our survey, we introduce solutions that integrated fog computing in the access control. Moreover, to the best of our knowledge, our paper is the first survey that proposes a fine-grained classification of access control solutions. Indeed, we classify access control according to their access model, their architecture, their intervening layers and their organizational concept. Furthermore, our survey presents a deeper discussion that has led us to more robust findings and broader open issues with greater relevance. Table 2 provides a comparison of our survey to the other existing ones. Accordingly, we can notice that our survey is of the very few ones that covered access control models, centralized, distributed and blockchain solutions.

3. Internet of Things (IoT)

Thanks to the IoT, users are no more just using the Internet, but actually the Internet is living with them. With the use of smart objects that acquire information about our surroundings, locations, daily routines, etc, the user's life is enhanced and eased in many ways. We present, in this section an overview of the different IoT architectures and we give an insight on some IoT application domains.

3.1. Architecture

IoT has numerous architectural layouts (Al-Qaseemi et al., 2016). The first architecture basically consists of three layers as depicted in Fig. 1: perception or physical layer, network layer and application layer. In the perception layer IoT devices collect data and send them to the network layer. The network layer is responsible for transferring collected data to the application layer. The application layer allows users to access different services using an interface.

IoT can have four-layer architecture (Soumyalatha, 2016) as shown in Fig. 2. This architecture is composed of sensors or physical layer, gateway or network layer, management service layer and application layer. The management service layer acts as an interface between the gateway network layer and the application layer. It assumes responsibility for overseeing device and information management, as well as the task of collecting substantial volumes of raw data and subsequently extracting pertinent information from both stored and real-time data.

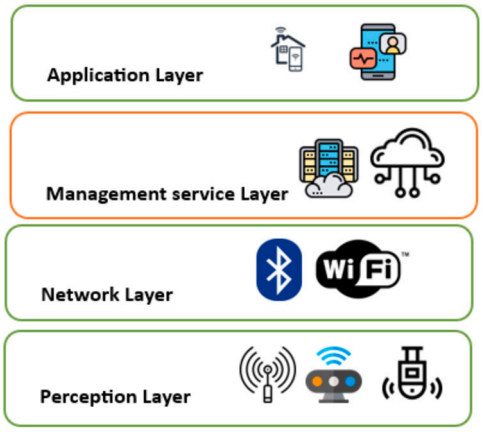

Fig. 2. Four-layer IoT architecture.

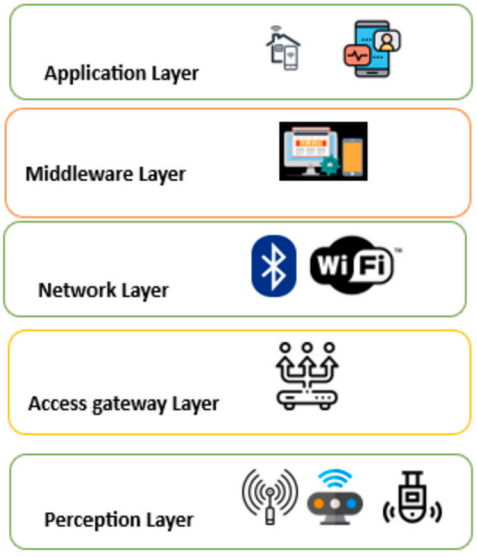

Fig. 3. Five-layer IoT architecture.

The five-layer architecture is a well-known architecture for IoT networks. This architecture is illustrated in Fig. 3. It has the same three layers with the same functionalities as the three-layer architecture and two additional layers which are access gateway layer and middleware layer. The access gateway layer facilitates the connection and communication among IoT devices and the network. It may support various communication protocols such as Wi-Fi, Bluetooth, Zigbee, cellular networks, etc. The middleware layer has as key functionality the management of data. It handles the collection, storage and management of data received from IoT devices.

3.2. IoT application domains

IoT technology has been applied in many application domains. In this section, we present only IoT domains that we will focus on their corresponding access control solutions, in the next sections. These domains are infrastructure-based IoT systems, SOHO systems and real-time IoT systems.

- Infrastructure-based IoT systems: This domain encompasses smart grid and smart cities applications. Smart cities (Hassan et al., 2021) aim to enhance the quality of life of citizens by using IoT technology. Their objectives include optimizing traffic management, tracking parking space availability and even notifying residents when trash containers reach full capacity. The most challenging

issue in this domain is ensuring security, scalability and heterogeneity management since there are numerous devices that need to cooperate together. Security issues in infrastructure-based IoT systems are caused essentially by the openness of the different IoT systems on the city scale. Effectively, such openness favors the collaboration and interaction among various IoT systems. However, it increases the vulnerability against attacks and hence weakening the security level of the IoT system.

- SOHO-based IoT systems: These systems encompass all application domains in smart homes. Smart homes utilize various smart objects such as thermostats, smart TV and smart fridge. These objects are remotely controlled by homeowners through an application on their smartphones. A smart home involves interactions among humans and machines and among machines themselves. The SOHO systems come with many challenges, including security, energy efficiency, connectivity and reliability. Security is of great importance in SOHO applications because they are tightly related to the private life of users. For example, having non-authorized remote access to a camera inside a home infringes the private life of its residents.
- Time-critical IoT systems: These systems use IoT to reduce the time required to make a critical decision. Healthcare systems are among the IoT time-critical ones. Medical IoT devices play a major role in patients' remote monitoring. When an emergency case is detected such as an asthma attack or heart failure, the IoT system reports instantly the emergency case to a doctor or to a nurse. This helps to save the life of many individuals. It is evident that such systems must be highly secured to avoid medical data alteration and/or disclosure. It is also crucial to protect medical IoT devices from unauthorized access.

4. Access control models

Access to resources is governed by access control models. These models specify the set of access control policies that should be implemented to ensure that only authorized parties can access protected resources. An access control policy can be delegated or revoked over time. The delegation of an access control policy refers to the process of transferring the decision-making power from a centralized authority to individuals or groups. In other words, each user can be responsible for enforcing and administering access control policies in specific contexts. The revocation of access policy refers to the process of canceling the authorization that allows someone to access certain resources.
There are several models that have been proposed. These models have different characteristics, which could impact the behavior of an access control mechanism for IoT. We provide in this section, an overview of the most popular access control models.

- **Discretionary Access Control (DAC) (Li, 2011)**: DAC is considered as an identity-based access control model where access rights are assigned to users based on their identity. In this model, only the resource owner is responsible for defining each subject's rights on the object. He can grant or restrict access to his resources. DAC does not provide strong accountability, as access control decisions are based on the discretion of the resource owner. DAC is often considered more flexible compared to other access control models. However, it may lead to complex and difficult-to-manage access control configurations in large systems.
- **Mandatory Access Control (MAC) (Osborn, 1997)**: MAC is also considered as an identity-based access control model. In MAC, access decisions are not left to the discretion of resource owners, but are instead determined by a central security policy that governs the system. Even the resource owners do not have the right to change the access rules. There are mainly two MAC types.
  - Multilevel Security: Where users and data are categorized according to their trust and sensitivity into different levels.
  - Multilateral Security: Where multiple parties are involved in establishing security policies.
- **Role-Based Access Control (RBAC) (Sandhu et al., 1996)**: RBAC presents an authorization framework that ensures users access to a resource based on their role. The users' roles are assigned statically by the system administrator. In this model, the roles reflect the users' jobs, functions, responsibilities, or levels of authorization within an organization. Each role is associated with a set of permissions that determine the actions a user with his specific role, can perform on the resources. Users performing similar functions can be grouped under the same role and access is given according to this role. Access decisions are made based on the roles rather than individual user identities. Hence, modifying a user's access rights requires changing his role.
- **Attribute-Based Access Control (ABAC) (Hu et al., 2013)**: ABAC model provides a more flexible mechanism than the three models presented above. In the ABAC model, access is granted based on attributes evaluation. There are mainly 4 categories of attributes:
  - Subject attributes: such as role, department, age.
  - Object attributes: such as type, ownership, classification.
  - Action attributes: such as read, write, execute.
  - Environmental attributes: such as time, location, network conditions.

  ABAC policies define access control rules using attribute conditions, enabling precise and context-aware access control decisions. This model allows organizations to align access controls with their specific attributes and to adapt them to changing environments. It ensures that resources are accessed only by authorized entities under specific conditions. The ABAC architecture includes the following components:
  - The Policy Enforcement Point (PEP) examines incoming requests and generates an authorization request, which then will be sent to the PDP.
  - The Policy Decision Point (PDP) serves as the central decision-making component of the architecture. It evaluates incoming requests against the policies it has been configured with and provides a decision of either authorizing or denying access.
  - The Policy Information Point (PIP) acts as a bridge between the PDP and the external sources of attributes. It retrieves the required attribute information from subjects (users, entities) and objects (resources, data) to supplement the decision-making process of the PDP.
- **Organization-Based Access Control (OrBAC) (Kalam et al., 2003)**: In some cases, members who want to communicate belong to different organizations. The access right is given according to the organization to which he belongs. OrBAC model introduces the notion of "organizational" as an additional dimension and separates between the concrete level (user, object, action) and the abstract level (roles, views, activities). As a result, there will be two types of permissions:
  - Abstract permission is defined as follows: Permission (Organization, Role, Activity, View, Context). For example Permission (Hospital, doctor, consult, medical folder, Emergency).
  - Concrete permission determines if a specific action between a subject and an object is permitted or not: Is_permitted (subject, action, object) or Interdiction (subject, action, object).

  OrBAC is only adapted to centralized structures. For this reason, several extensions have been defined. Toumi et al. (2012) proposed the Trust-OrBAC model which adds the notion of trust management to OrBAC. The trust evaluation is based on various parameters such as experience and knowledge or reputation. These parameters are combined to provide a trust value.
  SmartOrBAC (Bouij-Pasquier et al., 2015) introduces different functional layers: a constrained layer that groups the subjects and the objects, a less constrained layer that contains the access control system and an organization layer that is responsible for allocating

Table 3
Evaluation of different access control models.

Access control model	Complexity	Fine-granularity	Context awareness	Dynamicity	Scalability	Distribution	Suitability for IoT	Access control strategy
DAC	Medium	No	No	Yes	Medium	Yes	No	Specified by data owner
MAC	Complex	No	No	Yes	No	No	No	Central security
RBAC	Medium	No	Medium	Yes	Medium	Yes	Yes	Role-based
ABAC	Complex	Yes	Yes	Yes	No	Yes	Yes	Attribute-based
OrBAC	Medium	No	No	Yes	Medium	Basically centralized, with extensions, can be distributed	Yes	Organization-based
CapBAC	Lightweight	No	No	Yes	Yes	Yes	Yes	Capability-based
UCON	Complex	Yes	Yes	Yes	No	Yes	Yes	Mutable and dynamic attribute-based

roles and privileges. SmartOrBAC presents a distributed approach in which IoT devices are autonomous and handle authorization processes.

- **Capability-Based Access control (CapBAC) (Hernández-Ramos et al., 2013)**: In the CapBAC model, the permission to access an object is based on a token of authority. The key concept of this approach is the attribution of a token, a ticket, or a key that gives permission to access an entity. This key references a unique object with its associated set of access rights. The main idea behind this model is that access rights are determined by matching the correct capabilities rather than relying on the identity of the requesting entity. CapBAC in its original form relies on a central server that is responsible for access rights validations. To avoid the problem of a single point of failure and make the CapBAC applicable in the context of IoT, distributed CapBAC model has been proposed in (Hernández-Ramos et al., 2016). In this model, access rights validation is ensured by the IoT devices. However, due to the limited capabilities of IoT and the easiness of their compromising, such models are not reliable in untrustworthy IoT environments.
- **Usage Control (UCON) (Park and Sandhu, 2004)**: UCON is similar to ABAC model since it allows the specification of policies in terms of subject and object attributes. It supports two additional decision properties, namely mutability of attributes and continuity of decision. In other words, the behavior of entities can be changed while the access is in progress. Hence, the granted access can be revoked and the usage is canceled. With UCON, permissions are checked not only at access time but also during the entire usage. Hence, UCON offers a more fine-grained access control than the other models. For example, via UCON, it is possible to grant print access to a given user for a given number of times (Park and Sandhu, 2002), whereas, in the other models, either the print access is granted or revoked.

Table 3 summarizes the advantages and limitations of the above presented access control models, which are evaluated according to the following criteria: complexity, granularity, context awareness, dynamicity, scalability, distribution and suitability for IoT systems. We present in the following the reasons for choosing these criteria. We have chosen the complexity criterion because the level of complexity gives an idea about the level of effort needed to implement and maintain the model. The fine-granularity is also an important evaluation factor because there are some situations where complex and very particular authorization is needed which requires particularly a fine-grained access control model. The context-awareness criterion gives an insight on the ability of an access control model to be adapted to dynamic situations and provide suitable access based on the context. In dynamic environments, access decisions may change frequently. The evaluation of how quickly and efficiently the model can be accustomed to these changes without compromising security is of high importance. For this reason, we have considered dynamicity as an evaluation criterion. The IoT systems are unceasingly growing. For this reason, the access control model should be adapted to this growth without deteriorating their performance. So, we have added scalability as a quality indicator of access control models. Since most of the current IoT systems are distributed, it is important to evaluate the access control models according to the distribution in order to verify if they are able to manage the access control over these distributed systems.

DAC, MAC and RBAC solutions have some limitations. Effectively, they are complex and they are unable to offer fine-grained access control. CapBAC is lightweight, however, it does not offer fine-grained access control. ABAC and UCON models are fine-grained and are suitable for IoT systems, but they are complex. The OrBAC model introduces the notion of the organization but it is centralized.

5. Access control solutions

In this section, we present the different access control solutions. We propose to classify them according to the taxonomy presented in Fig. 4. The access control solutions may be classified according to their used access model. At the end of this classification, we can better understand the different access control models and we can develop a clear comparison of access control solutions according to the adopted model. Besides, we adopt an architectural classification. Effectively, the various access control approaches are either centralized or distributed. First, we present and discuss the centralized approaches. Then, we present distributed approaches. These approaches can be classified into two sub-classes: non-blockchain solutions and blockchain-based solutions. By categorizing solutions as either distributed or centralized in terms of their architecture, the identification of the characteristics, advantages and limitations of each approach becomes straightforward. This allows researchers, practitioners and decision-makers to choose the appropriate architecture when implementing access control mechanisms according to their specific requirements. We can classify the access control solutions depending on the used layers. Access control solutions use either one layer including all the IoT devices or use additional layers such as fog and/or cloud layers to support the limited resources of IoT devices and offer them more efficient access control. This classification highlights the benefits of using fog nodes in terms of cost and efficiency. Access control solutions can address only one organization and/or tackle inter-organizational access control. The grouping of inter-organizational solutions makes it possible to study the requirements and specifications of these solutions. In this way, it becomes possible to develop and implement access control solutions that are specifically tailored to meet the needs of each context. We have also a class that includes all the access control solutions that are based on cryptography. This class allows readers to study and understand how cryptography can be used to ensure efficient access control. It is worth noting that the proposed classes presented in Fig. 4 are not mutually exclusive. There are effectively numerous overlapping classes. For example, we can have an access control solution that is at the same time distributed, using the

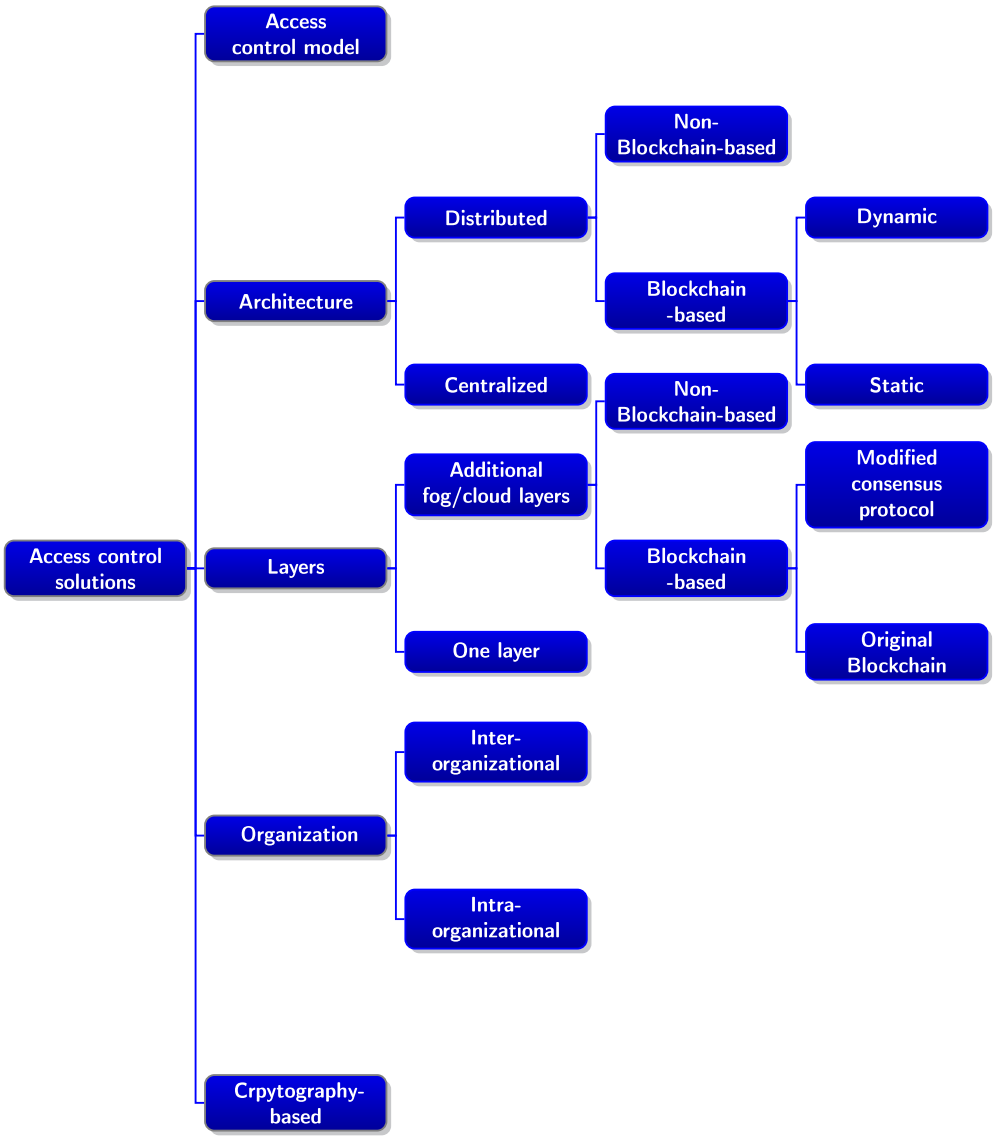

Fig. 4. Classification of access control solutions.

fog computing layer and treating the inter and intra-organizational access control.

5.1. Centralized solutions

The typical access control solutions (Bokefode Jayant et al., 2014) are built around the notion of trust where a centralized trusted entity is always introduced. Most of these solutions use an authorization server to save access control policies. The difference among approaches is the choice of the access control model. Bouadjemi and Abdi (2020) implemented a centralized RBAC model and defined an extension of it. This extension adds an exception situation. When the user is aware of an exception situation, he can request permission from the administration.

RBAC benefits are not sufficient to meet the needs of large organizations. For this reason, Thakare et al. (2020) proposed an integration of the ABAC and RBAC models. The resulted model retains the flexibility offered by ABAC while maintaining the RBAC advantage of easier administration. Based on the type of attributes, a role is allocated to the client. Before deciding the policy, the priority-based condition is also evaluated for making fine-grained decisions. The most important advantage of these approaches is the simplicity of management of access control policies. However, the central entity in these solutions presents their main drawback since it may lead to a single point of failure. Also, the data owner is not able to define access control to his own data. Riad and Cheng (2021) introduced a new adaptive XACML scheme that extends the typical XACML by integrating access code generation and verification for heterogeneous distributed IoT environments. In their work, they introduced a validity time constraint to make sure that the generated access codes can only be used during the predetermined validity period. Also, they defined a set of conditions that are essential for the access control mechanism.

Gupta et al. (2021) introduced an ABAC model specifically tailored for cloud-enabled industrial smart vehicles. Their work highlights the importance of considering contextual information for access control decisions in the context of industrial smart vehicles. The proposed framework incorporates contextual attributes such as location, time and vehicle status. Guo et al. (2022) presented a dynamic deployment method of security services based on malicious behavior knowledge base. In their solution, the database of malicious behavior is integrated with the existing detection system. They establish a mechanism to gather feedback on the detection results. This feedback will help improve the accuracy and effectiveness of the system over time. Saxena et al. (2015) introduced a messaging service known as Simple Messaging and Access Control (SMAC). In their approach, access control has been shifted

from the device or shared server to the communication ports directly. The SMAC server comprises a various number of ports that can be assigned to different devices. It can be assumed that only the respective device possesses the knowledge of which port to utilize leading to an instant verification of the user's identity when communicating through that port. This solution offers a significant advantage by eliminating the requirement to store and manage an Access Control List (ACL), which can cause high complexity when the network size increases. Zhang and Gong (2011) proposed a conceptual framework to extend the UCON (Usage Control) model for IoT network. In their work, the authors identified the need to deal with the unique characteristics of the IoT environment, such as flexibility and heterogeneity. To address this, they devised a mapping scheme to associate the abstractions from the UCON model with the various entities found in IoT, ensuring compatibility and effectiveness within the IoT context.

5.2. Distributed solutions

We present in this section two types of distributed solutions: non-blockchain-based solutions and blockchain-based solutions.

5.2.1. Non-blockchain based solutions

Distributed access control helps to overcome the drawbacks of centralized access control solutions. Gusmeroli et al. (2013) developed access management for IoT based on CapBAC. This access management supports delegations and revocations. The proposed approach is flexible and fine-grained. The capability tokens are represented by digitally signed XML files. The delegation process is simple and does not require centralized services. It is based on a simple standalone application that subject A can utilize to transfer access privileges to subject B, guided by subject A's access capabilities.

A token-based approach is presented in (Cirani and Picone, 2015). This work requires the resource owner's involvement in the issuing of tokens. In particular, it accounts for three operational modes to obtain the tokens: owner-to-owner, in which a user registers his own device and obtains a token to gain control of the object, reactive owner-to-any, in which the owner grants permission after a user's request and proactive owner-to-any, in which the owner grants permission to a user without a prior request. To ensure a dynamic and fine-grained access control in IoT, Nobi et al. (2022) proposed a neural network taking users and devices metadata as input and access control decision as output.

A Convolutional Neural Network (CNN) is employed in (Thilagam et al., 2022) to extract the data using a dedicated security module and ensure data privacy. A Federated Deep Learning (FDL) methodology is used to improve the accuracy of the access control. Mahalle et al. (2013) proposed a fuzzy trust-based access control model in which access is granted based on the trustworthiness of the requester. They introduced a combination of the access control model based on attributes (ABAC) and the trust mechanism named Trust-ABAC model. The access decision is ensured by three main components. The first one is the entities of the trust-ABAC model in which the authorization decision is based on the attributes of the various entities involved in making access control decisions and the trust value. The second component is the recommendation manager which acts as an interface between the model and IoT network. It is responsible for filtering the received recommendations. It evaluates the trust level of the recommendation message and detects the collision attack in order to filter the inappropriate recommendations. After that, it sends only the trusted recommendations to the broker which is the last component. The broker is a mediator between the Trust-ABAC model and the recommendation manager. It manages requests for trust values of the Trust ABAC model. Also, it is responsible for backing up feedback ratings received for objects that request access after each transaction, in order to update the trust value of the accessing object stored in its local database. Finally, it sends the recommendations requests to the recommendation manager.

Xu et al. (2018b) presented a federated capability-based access control mechanism for IoT. Their work relies on identity-based capability token management strategy, which involves registering, propagation and revocation of the access authorization. The proposed solution consists of three levels: cloud computing layer which is a global profile database and policy decision making center. A fog computing layer which is responsible for delegation of domain-specific access authorization policies and identity management tasks. An edge computing layer which is composed of different devices that play the role of service providers offering access control authorization.

5.2.2. Blockchain-based solutions

Several approaches have chosen blockchain technology to develop distributed and immutable access control solutions.

Blockchain definition and benefits

A blockchain (Reyna et al., 2018) is an immutable ledger that contains a set of linked blocks, which have been validated by the miners in a peer-to-peer (P2P) network. The main characteristics of blockchain can be summarized as follows:

- Decentralization: The decentralized aspect of blockchain can eliminate any single points of failure, thereby improving the fault tolerance. The IoT devices can interact with each other without the involvement of any intermediary using blockchain.
- Distribution: Blockchain as a distributed ledger, has the ability to store and distribute data. The validation system is ensured over various nodes.
- Immutability: Data in the blockchain cannot be altered. Indeed, the blockchain is a sequence of blocks that hold a complete list of transactions. Each block points to the previous block via a reference that is essentially a hash value of the previous block. Any modification in a block results in a disconnection among the blocks which ensures immutability.
- Scalability: Blockchain technology can control the collection and processing of data issued from a large number of IoT devices.
- Anonymity: It is possible to interact with a general address. Personal information is not necessary to add a transaction.

Types of blockchain

Blockchain types can be classified into three categories:

- Public (permission-Less): In the public blockchain, everyone can join the network and can participate in the validation process of the transactions (mining).
- Private (permissioned): Private blockchain is the opposite of public blockchain, since it is a restricted network where each member wanting to join the network must be authorized by an organization.
- Consortium (hybrid): A consortium blockchain is a combination of private and public blockchain. The validation process is done by a selection of participants.

Blockchain-based access control solutions can be divided into two subclasses: Static solutions in which the definition of access control is in the beginning and dynamic solutions in which the policy can change dynamically due to different circumstances.

Blockchain platforms

- Bitcoin: Bitcoin (John et al., 2022) is the first and most well-known cryptocurrency and blockchain platform. It was first conceived for secure and decentralized transactions in cryptocurrency. Each transaction is added onto blockchain after a validation process called mining.
- Ethereum: Ethereum (Tikhomirov, 2018) is a decentralized blockchain platform that is based on the creation and execution of smart contracts. The latters automatically execute actions based on predefined conditions. Ethereum relies also on mining to validate transactions. However,

the mining process in Ethereum is lighter and simpler than the mining in Bitcoin.

- Hyperledger: Hyperledger (Dalla Palma et al., 2021) offers a secure, modular and flexible approach for private and permissioned blockchain networks. There are numerous Hyperledger projects like Hyperledger Fabric, Sawtooth and Indy. Their main aim is to offer features like permissioned access, scalability and privacy for the network of networks.

Static Access control solutions

Ouaddah et al. (2016a) proposed a distributed access control framework based on Bitcoin technology named FairAccess. In order to authorize users, a token defined as a digital signature is used, allowing them to access resource based on their addresses. This approach uses the blockchain as a database that maintains the access-control policies. Dorri et al. (2017) presented a solution for the management of access control in inter-smart home devices. Each home has a node that connects to the blockchain and maintains access-control policies stored in a local private blockchain.

Novo (2018) proposed a real-time decentralized access control architecture. The blockchain is separated from the IoT network. This means that IoT devices do not participate in the transactions validation process which preserves their resources. The proposed approach consists of managers, an agent node and management hub entities. The manager is responsible for defining the access-control policies. The agent node is responsible for controlling and deploying the smart contract into the system. Since the IoT devices are not connected directly to the blockchain, the authors opted to use a node called management hub which is an interface that translates the information encoded by the IoT devices into messages understandable by the blockchain nodes. It is connected directly to a blockchain node. A management hub can request information about any IoT device freely and obtain the result instantly from the blockchain node. All the operations in the system are defined and enforced using a single smart contract. This solution is scalable due to the fact that numerous constrained networks can be connected simultaneously to the blockchain network using specific nodes called management hub nodes. Additionally, the possibility of having different management hubs provides a high flexibility to this solution.

Xu et al. (2018a) defined a capability access control based on blockchain technology for IoT systems named BlendCAC. They used the concept of smart contract for registration, propagation and revocation of the access authorization using private Ethereum technology. In their work, the IoT devices are connected directly to the blockchain. Being part of the blockchain network increases the security and the efficiency of the access control, however, it overwhelms the IoT devices with resource-consuming tasks, which has a negative impact on the performance of the IoT network. Dukkipati et al. (2018) presented a blockchain attribute-based access control for IoT environments. In their system, the policies are stored in an external database while the URL links of the policies are stored in the blockchain. Such a strategy avoids storing important amounts of data in the blockchain. However, since the policies are stored in an external database, they can be easily tampered with without being detected.

Ali et al. (2017) presented a blockchain-based access control in order to protect data privacy. They used the blockchain and InterPlanetary File System (IPFS) to achieve a decentralized access-control mechanism. In their work, they employed two categories of blockchain: private and consortium. The private blockchain provides an immutable log of all IoT data operations including sensor data creation and IoT data access, while the consortium blockchain is responsible for the management of access requests for any user of IoT data. In the IPFS, they store all these IoT data. Maesa et al. (2017) developed an ABAC access model based on Bitcoin. Their work ensures the management of access control policies and offers the ability to transfer the rights from one user to another. The storage of policies is made in a local database. In the blockchain, they store only a representation of the right to access a resource. The authors represented the rights to access resources in a simplified manner and these rights can be transferred among different users. The main purpose of using blockchain in this solution is to serve as a distributed and immutable storage for access control policies.

An access control management solution for medical data and devices owned by several organizations was introduced by Malamas et al. (2019). Access to data is granted by smart contracts. The medical data are stored in the IPFS. The blockchain system is authenticated by a proof-of-medical-stake consensus mechanism. This is considered as the most suitable mechanism for medical applications. A private Ethereum implements the consensus mechanism using smart contracts. Cruz et al. (2018) proposed a solution that integrates RBAC with blockchain. This solution authenticates users based on their ownership roles. The authors employed a smart contract that enables users to access resources belonging to different organizations depending on their roles. However, it is usually hard to extract the concrete roles in dynamic environment.

Alphand et al. (2018) introduced a fully decentralized access control architecture for IoT resources named IoTChain. IoTChain is a hybrid system that consists of an OSCAR (Vučinić et al., 2015) server and a blockchain. The OSCAR server is used as a manager and distributor of keys to other servers. The blockchain is used for guaranteeing the authorization of devices. This is based on Authorization for Constrained Environments (ACE) framework (Seitz et al., 2017). In their work, the authorization process performs as follows: First, the owner of the resource defines access policies in smart contracts, which are self-executed to generate access tokens to the users when the required conditions are satisfied. When a user wants to access a resource, he must enter the required information for validation in the data field such as the public key. This type of request is broadcasted so that all devices will receive the transaction and proceed with validation. Once the validation is completed, the smart contract is executed, which will generate a token for the user. Now, the user needs to own the decryption key to read the resource. So he sends a request to the keys server, which will verify the identity of the requester. Finally, the user can download the resource and decrypt it with the key he obtained.

An access authorization architecture in the IoT using the ABAC access model with public and private blockchain was introduced in (Pal et al., 2019). The main contribution of this work is to provide a flexible framework for transferring access rights in large-scale IoT systems. The feasibility of the study is evaluated by using the Ethereum blockchain network. This delegation model leverages the property of identityless, asynchronous and distributed nature of communication. Ding and Sato (2023) proposed an authorization framework based on a consortium blockchain named Bloccess. In this solution, they have introduced an identity administration system that is connected directly to blockchain in order to manage access. Bloccess has some limitations. Indeed, this solution faces security and scalability issues.

Dynamic access control solutions

Typically, access control solutions assign access permissions based on static considerations such as identity, roles or attributes. However, the high dynamic nature of IoT makes the prior definition of access control difficult and unsuitable. For this reason, researchers proposed dynamic access control solutions.

Liu et al. (2020) designed and implemented an open-source access control system that combines ABAC with the Hyperledger Fabric blockchain framework named Fabric-IoT. Their solution provides dynamic management of permissions, decentralized architecture to separate devices and users and fine-grained access control. Three contracts named Access Contract (AC), Policy Contract (PC) and Device Contract (DC) were implemented. The first manages the ABAC model, the second ensures the policies management, and the third represents the device resource management. The fabric-IoT system allows the device to grant access to the data resources based on a URL.

Hwang et al. (2018) proposed a dynamic access control scheme. The idea is to automatically generate access rights after requesting access.

All the access permissions are stored in the blockchain. The creation of a dynamic policy is done by the manager upon receiving a data request. The validation of the requested access permission is ensured by using a smart contract.

A proposal of a dynamic access control framework with blockchain technology and machine learning was presented by Outchakoucht et al. (2017). In this solution, the smart contract learns from past experiences and tries to capture the best possible knowledge to make accurate business decisions. Zhang et al. (2020) proposed an ABAC framework for smart cities using Ethereum. The proposed framework consists of a Policy Management Contract (PMC), a Subject Attribute Management Contract (SAMC), an Object Attribute Management Contract (OAMC) and an Access Control Contract (ACC). They defined the policy as a combination of a set SA of subject attributes, a set OA of object attributes, a set A of actions and a set C of context information. For the sake of simplicity, they use start time and end time as attributes for establishing a dynamic access control.

Kumar and Tripathi (2021) proposed an enhanced Bell-Lapadula model to support the dynamic behavior of the peers and access control policies using smart contracts for healthcare systems. The traditional Bell-Lapadula (BLP) introduced three security policies: simple security policy (ss-policy) in which the subjects cannot read the object with a higher sensitivity level (security level), star policy (*-policy) which allows the subject to write its own sensitive level or higher sensitive level and discretionary security policy (ds-policy) which implies that if the permissions of the subjects are assigned and matched with the existing policy then the access of objects will be permitted. The BLP model is static. Kumar and Tripathi (2021) introduced dynamic rules in the BLP model to support the dynamic behavior of the peers and access control policies using smart contracts. They addressed the scalability problem in blockchain technology and improved the dynamic behavior of the access control model. In fact, each peer is associated with a level and can access the specific transaction. The peer does not have to maintain the complete state of the transaction history of all access control policies.

Han et al. (2022) introduced an auditable access control model leveraging the capabilities of a consortium blockchain technology. Their solution employs four deployable smart contracts to facilitate various functionalities. The first smart contract oversees access control policy management, while the second smart contract facilitates request and response interactions between the data owner and the data requester. The third smart contract focuses on private data management within the IoT context and the fourth smart contract handles the management of access records.

Deebak et al. (2023) presented a protocol that combines blockchain technology and seamless authentication to address authentication and data privacy challenges in IoT applications. The protocol not only focuses on resolving current issues but also considers future integration with other applications. The authors conducted research on the traffic patterns of interconnected devices and integrated them within authentication processes, aiming to enhance communication metrics such as packet loss ratio and latency.

Bera et al. (2021) introduced a novel decentralized blockchain-based access control protocol in an IoT-enabled smart-grid system called DBACP-IoTSG. The blockchain is composed of the providers of the service and smart meters. Data among them are exchanged in a secure manner through a private blockchain. The process of access control has basically two tasks. The first task is node authentication where the joined nodes must verify their authorization and prove that they are legitimate registered nodes in order to access services from other nodes. The second task is the key establishment that involves a newly deployed node establishing a shared secret pairwise key with its neighboring nodes once mutual authentication has been successfully completed. A shared secret pairwise key is a cryptographic key generated and shared between two parties in a secure communication system. The established secret keys are then used by the nodes for secure communication. The validation process in this approach is based on a voting consensus algorithm.

5.3. Inter-organizational access control

We can classify different access control solutions from an organizational point of view. Many researchers proposed intra-organizational access control solutions. They only focused on data exchange and resource access in the same organization. However, since the IoT environment encompasses several application domains that interact together, we need an access control solution that controls the access among different organizations. For these reasons, several researchers proposed inter-organizational access control solutions.

The IoT devices in (Bai et al., 2021) are divided into domains. Each domain has its own access control rules. Every node belonging to a given domain should have an attribute certificate issued from a certificate authority that belongs to that domain. If a given node belonging to domain A wants to access another object belonging to domain B, it should have a new certificate. A Trusted Third Party (TTP) processes the access request, maps its attributes in domain A to new attributes in domain B and creates a new attributes certificate that allows its access to the new domain.

In FairAccess (Ouaddah et al., 2016a), authors developed a Bitcoin-based framework that ensures communication among different organizations. Access tokens are considered as resource access rights and the access control process is done by transferring access tokens. The access token is expressed in script language and publicly broadcasted to the blockchain network in order to realize verification and transaction confirmation. This work enables the resource owner to control his data by creating an access token using a smart contract. Each user even from another organization that has this token can access the resource, otherwise, he is unable to access it.

Novo (2018) used smart contracts to implement access control for Industrial IoT (IIoT). They created a single smart contract to define all the policy rules. This solution ensures the communication among different organizations represented by various networks through blockchain. The proposed solution is partially decentralized because a manager is responsible for defining the access control rules and administering the permissions. BlendCAC (Xu et al., 2018a) is also an inter-organizational access control solution based on Ethereum. The principle of this work is similar to the one presented in (Ouaddah et al., 2016a). The owner of a resource is responsible for access verification via the generation of a capability token.

The paper (Ali et al., 2017) has proposed an IoT network architecture called a modular consortium network. In this work, communication in the same organization is done using a private blockchain. However, the communication among different organizations is ensured by a consortium blockchain. This one is responsible for securely logging any incoming access request for any user's IoT data and performing access control for those incoming requests. In the blockchain-based inter-organizational access control solution proposed in (Qin et al., 2021), each organization is an attribute authority that is responsible for creating user attribute. The access is based on these attributes. In FabricIoT (Liu et al., 2020), inter-organizational access control is ensured thanks to the designing of a channel system by Fabric to isolate the blockchain data of the different organizations. In each channel, there is an independent private ledger and a blockchain.

Song et al. (2021) introduced a supply-chain system based on consortium blockchain. They used smart contracts to call traditional access control lists and designed a penalty mechanism to control the use of resources. This work facilitates access control among the different organizations. Effectively, each organization has an IoT gateway and some IoT devices. Each one runs a node and all organizations maintain the same blockchain. Each access request goes through the organization's node. This node has the right to decide the action to be performed. Truong et al. (2022) proposed CapBlock, a blockchain-based access con-

trol solution based on the distributed capability-based access control model (DCapBAC). They used the XACML standard for the definition of access control policies and the Hyperledger Fabric for the blockchain network. The capability token is generated in a secure way by the organization. So, the organization is responsible for granting or revoking access. CapBlock controls the access to information in federated IoT organizations. It takes into account the difference among the access control policies belonging to different organizations.

A blockchain-based energy trading market has been proposed in (Khalid et al., 2020) to remove the monopolism of the main energy grid and to offer the possibility to smart homes to act as producers (prosumers). All prosumers are connected to the utility grid. Additionally, they have direct communications among each other to facilitate the energy transfer among them. The market users are nodes in the blockchain. Each prosumer wanting to sell energy should be a member of the market and should specify its trading conditions through a smart contract. Each consumer wanting to buy energy should fulfill the requirements indicated in the smart contract to get served. In this system, the authors implemented a reputation mechanism. They incorporate reputation scores into the Proof-of-Work consensus algorithm, called PoWR, in order to reduce the block creation time and latency.

Shi et al. (2021) designed a blockchain-based access control scheme called BacS for use in inter-domain IoT. A redefinition of the access control permissions of the data services is deployed and stored on the private Ethereum. Each IoT domain is identified and accessed through an account address of the blockchain node. They use Symmetric Encryption Algorithm (SEA) to ensure the various distributed systems privacy.

Feng et al. (2021) proposed a novel access control framework for 5G-enabled Industrial IoT. In this work, the solution is constructed based on Hyperledger Fabric and the chaincodes are designed to implement different access control functions. These chaincodes are distributed in two channels. Channel-A stores different access control policies and channel-B stores behavior characteristic data of the different IIoT domains and serves related applications for domain credit evaluation. The authors divided each industrial edge gateway and its connected IIoT devices as an IIoT domain. IIoT devices interact with the gateway through the lightweight protocol for data interaction related to access control. Abdi et al. (2022) proposed a lightweight hierarchical blockchain-based multi-chaincode access control for IoT systems. The architecture of the proposed solution contains three main components: an edge blockchain manager that is responsible for authenticating and authorizing constrained devices locally, an aggregated edge blockchain manager, which is responsible for managing ABAC policies and a cloud consortium blockchain manager that is responsible for authenticating and authorizing external requesters to access IoT data. Every external request goes through this manager.

A decentralized blockchain-based solution that is able to validate transactions between two different parties is introduced in (Ameer et al., 2022). In this work, a smart contract needs to be signed between the two platforms. This contract ensures access to resources between these two platforms. This implies that if an application from the first platform comes with a specific coupon, it will get access to resources available in the second platform. This contract also contains information about the conditions in which the access will be granted (several times or unlimited during a time window). To guarantee its integrity, contracts are cryptographically signed by their issuing platform. The authors designed the architecture of this approach but they didn't implement it.

In all the aforementioned blockchain-based solutions, a fine-grained verification through the smart contract should be done to grant or revoke access. It is evidently highly secure but it consumes a lot of resources and time especially when the number of requests increases. To overcome this limitation, Trabelsi et al. (2023) proposed an access control solution in inter-organizational IoT networks based on blockchain and Virtual Private Network (VPN) technology. To avoid the high resources consumption and the time needed for access control, the IoT devices belonging to different organizations and cooperating frequently are grouped unto the same VPN. A smart contract verifies the conditions to belong to a given VPN. Another smart contract controls the access to a given resource per VPN. This means that unlike the ABAC-based blockchain solutions, the smart contract verifies only if a given requester belongs to an authorized VPN to grant it access. This saves time and energy.

A blockchain-based attribute-based zero-trust access control model for IoT is presented in (Awan et al., 2023). This work ensures secure device-to-device communication. The limitation of this solution is that access request consumes a lot of time and energy. This is caused by the complex implementation of ABAC access control mechanisms through smart contracts.

Khalid et al. (2023) introduced a blockchain-based smart contract solution in order to define the rules and penalties related to an agreement. In this work, all access requests go through the Software-Defined Internet of Things SD-IoT controller in the beginning. This controller is connected directly to blockchain in order to read access policies. The evaluation of this approach shows that there is a slight increase in resource access delay.

5.4. Fog-based access control

Numerous access control solutions for IoT have found in fog computing a suitable remedy to offer access control tasks near to IoT devices without overloading them and without threatening their limited resources. We start with overviewing fog computing. Then, we will present fog-based solutions. We divide the fog-based access control solutions into two sub-classes: blockchain-free access control and blockchain-based access control.

5.4.1. Fog computing

Vaquero and Rodero-Merino (2014) defined fog computing as follows " *Fog computing is a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralized devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without the intervention of third parties. These tasks can be for supporting basic network functions or new services and applications that run in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so.*" Fog computing acts as a bridge between the physical layer which encompasses various IoT devices and the cloud computing layer. Fog layer is also called edge layer. The main advantages of using fog computing can be summarized in the following points:

- Minimize latency and network congestion.
- Provide local storage in proximity to data generation points.
- Execute complex tasks near to their sources for quicker and more scalable processing.
- Ensure cloud-like services near end devices.
- Prevent unnecessary access and excessive utilization of cloud resources.

Fog nodes refer to network devices that possess both storage and computing capabilities, in addition to network connectivity. They are distributed and can be static or mobile.

5.4.2. Blockchain-free access control

In the contribution proposed in (Salonikias et al., 2016), the PIP and the PDP that ensure the access control evaluation are deployed on fog nodes to take profit from their rich resources. An additional layer called edge layer is responsible for the PEP. Whenever there is any modification in the PEP policies, a synchronization process is ensured in PDP.

5.4.3. Blockchain-based access control

Enforcing access control in IoT environments is so important. Integrating new technologies such as blockchain brings multiple values as we have already stated. In spite of the advantage of blockchain in the access control, it is injudicious to apply it directly on the IoT devices due to their limited resources and their critical amount of energy. There are hence three ways to deal with these constraints:

1. Reduce the tasks of blockchain (for example employ a very simple consensus protocol) to make them suitable for IoT. This improves the network performance but reduces drastically the security level of blockchain which in turn reduces the security level of the access control solution.
2. Use blockchain and IoT as two separated layers. The blockchain layer will be managed by cloud computing where there are no resource constraints. The IoT devices communicate normally and access the blockchain via the cloud. In this way, blockchain is employed in its original form to keep its high-security level. However, this leads to additional delays due to the important distance between the cloud and the IoT devices.
3. Use blockchain over the fog computing layer (Fersi, 2021). Since fog nodes have more powerful resources and are physically close to the IoT devices, they emerge as an ideal environment for blockchain deployment. We can classify the blockchain-based access control solutions that are applied on fog nodes into two main classes (Fersi, 2021):

- Original blockchain: Blockchain is deployed with all its features on the fog nodes, without any modification.
- Changed consensus protocol: The basic consensus protocols like Proof of Work (PoW) for Bitcoin and Proof of Stake (PoS) for Ethereum are of high security but they consume a lot of resources which may reduce the performance of the fog nodes. There are some access control solutions that have proposed new consensus protocols that are lighter and more appropriate for IoT.

Original blockchain

A distributed and dynamic fine-grained access control for IoT is proposed in (Liu et al., 2021). The contribution is based on blockchain and fog computing. Every access to other smart objects is ensured through fog nodes. Once data are generated and uploaded to the edge nodes, these latter specify their corresponding access control attributes and upload them to the blockchain. Each data access request is sent to the PEP. After the specification of the attribute-based access requests, the PEP sends it to the PDP. Depending on the policies of the resource owner and on the predefined attributes, the PDP takes the access decision and sends it to the PEP that sends in turn data to its requester if the access is accepted.

In (Stanciu, 2017), the access control based on IEC 61499 standard is ensured by the application of Hyperledger Fabric blockchain over fog nodes using micro-services architecture. The function blocks are implemented by the Docker containers and are considered as smart contracts. The orchestration of the containers execution among fog nodes is ensured using Kubernetes.

BSKM-FC (Gowda et al., 2023) is a novel blockchain-based approach that aims to ensure efficient access control and secure communication among fog nodes and IoT devices. It offers a blockchain-based authentication among smart devices. After that, the fog nodes in the system generate session keys using a one-way hash chain and store them in the blockchain to ensure their immutability. The use of fog nodes improved the time of block preparation and reduced the computation time of key generation.

The contribution presented in (Almadhoun et al., 2018) proposed a blockchain-based user authentication and access control scheme. The network administrator creates a smart contract and specifies in it all the access control rules and manages through it the set of IoT and fog devices and the set of allowed end-users. When an end user requests access, he should get explicit permission in the smart contract. The security process in (Almadhoun et al., 2018) is consolidated by the use of messages digital signature to ensure the sender authentication and non-repudiation. The proposed contribution also ensured the availability objective since it fixes in the smart contract the set of allowed users who can access the IoT devices to protect them from malicious users' overuse. Hence, the services will be always available.

Modified consensus protocols

In the paper (Wu and Ansari, 2020), the Access Control Lists (ACL) are stored in the blockchain nodes that are also fog nodes. Each network access approval or declination is stored in blockchain and every change in the ACL should be also stored in it. The network is made up of multiple fog nodes clusters and each fog nodes cluster has the same ACL. In order to reduce the computational resources needed to generate the adequate hash value for a new block, a heuristic algorithm has been proposed to compute cooperatively the hash value by the different fog nodes in the same cluster.

Zahoor et al. (2023) designed a private blockchain using a Physically Unclonable Function (PUF) to ensure efficient access control. This protocol ensures the data transfer in an efficient and secure manner among Service Providers (SPs) and Smart Meters (SMs) in smart power grid systems. In this schema, each participating SP employs a voting-based consensus mechanism to verify the block before including it in the blockchain.

5.5. Cryptography-based solutions

In this section, we will present solutions that use cryptographic mechanisms in their access control solutions. Li et al. (2022) presented Traceable and Revocable Access Control (TRAC) for mobile health (mHealth) in 5G-enabled Industrial IoT (IIoT). In TRAC, the authors combine Ciphertext Policy and Attribute-Based Encryption (CP-ABE). In their solution, a personal health record (PHR) owner can define any access policy over attributes and can select proper potential readers for his/her personal health data. These access policies are stored in the cloud. The main contribution of this work is that the decryption algorithm is not complicated and the time of decryption is constant.

Hernández-Ramos et al. (2016) proposed a solution named DCapBAC which demonstrated the feasibility of CapBAC access control logic in constrained devices. In fact, they presented a lightweight solution based on Elliptic Curve Cryptography (ECC) that is responsible for key generation to ensure end-to-end authentication, integrity and non-repudiation. DCapBAC allows smart devices to autonomously make decisions. The operation of pending access rights can be summarized into these steps: First of all, the issuer entity, usually instantiated by the device owner, issues a capability token to the subject to be able to access that device. The subject attempts to access the device data. Once the device receives the access request, the application checks the validity of the token as well as the rights. Finally, when the authorization process is completed, the device generates a response based on the authorization decision.

Ye et al. (2014) proposed an efficient authentication and access control method. They established a key between the user and nodes for secure communication. Their work is based on ECC authentication and the ABAC policy to achieve mutual authentication between user and nodes and fine-grained access control. The proposed approach is made up of two parts: The first one is the authentication part which ensures only the legitimate user to access the network. It is between the user and terminal nodes. The second one is the key establishment part in which session keys are created between the user and nodes for secure communication. A blockchain-based framework for data sharing in decentralized systems was proposed in (Wang et al., 2018). This framework includes an IPFS decentralized storage system, Ethereum blockchain and Attribute-Based Encryption (ABE). In this work, data owners control their own data. They have the ability to distribute keys for users as needed to obtain access control. First, they use the AES algorithm to encrypt the file and upload it to IPFS. After that, they encrypt the file location and send it to the blockchain. Although anyone

can see the information, a user whose attribute does not meet the access policy cannot decrypt the file encryption key and cannot download the encrypted file from IPFS even if he knows the secret key, since he doesn't know the file location. In this way, the authors achieved fine-grained and secure access control over data. However, they didn't take into consideration access policy updates and user attribute revocation.

Qin et al. (2021) provided Lightweight Blockchain-based Access Control (LBAC). It is based on both ABE and Hyperledger Fabric blockchain technology (Androulaki et al., 2018). In the LBAC solution, the access is dynamically adjusted after measuring the user's credibility based on the user's abnormal access. The credibility computation is based on abnormal access analysis. Yu et al. (2021) proposed an ABAC scheme for the smart factory that supports traceability and revocation. The blockchain network is responsible for unified identity authentication and the storage of all public keys, user attribute sets and revocation list. Compared with other schemes, the size of the public key and the private key is shorter and the time overhead is smaller in the public key generation, data encryption and data decryption stages. In the work (Yu et al., 2021), malicious users can be tracked and revoked at any time. Das and Namasudra (2023) proposed a multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure in order to reduce the complexity of CP-ABE solutions. In this approach, the key generation process is distributed among different attribute authorities, each one is responsible for generating the private and public key pair for an attribute set that belongs to its domain.

A three-tier architecture made up of cloud, fog and IoT layers is proposed in (Xu et al., 2021, 2020) to ensure efficient access control among the IoT devices. The process starts with the system parameters initialization and keys generation by the key generation center. Then, the cloud service provider ensures the accommodation of cipher texts issued from a given fog node and the sharing of these cipher texts with the other fog nodes. The fog layer ensures the cipher text aggregations and orchestrates also the data requests and cipher texts transfer to receivers. The IoT device uses an encryption key that is bounded to a set of sender attributes. It uses this key to encrypt collected data and send them to its corresponding fog node. The cipher text is associated with a decryption policy. The receiver that satisfies the decryption requirement is able to read the plain text.

Authors in (Huang et al., 2017; Zhang et al., 2018) have stated that ABE is a suitable cryptography method that ensures efficient access control. However, it consumes a lot of resources which cannot be supported efficiently by IoT devices. For this reason, they proposed a fog-based encryption approach in which they outsource the encryption/decryption tasks to the fog nodes. Each user uses the fog nodes to encrypt his cipher text using ABE and send it to the cloud. Each user wanting to decrypt the cipher text should satisfy the access policy specified in the attributes. The contribution (Zhao et al., 2021) has the same principle as the two aforementioned approaches since it delegates the encryption-decryption tasks to fog nodes. The main difference of this work in comparison to the other ones is that it offers a dynamic access control enabling attributes revocation. Lohachab and Karambir (2018) presented a hybrid access control solution. They used a Quantum Key Distribution (QKD) which uses Quantum Cryptography (QC) for distributing a secret key in a secure manner. They also used another encryption technique which is ABE in order to achieve data protection at fine granular levels. At the device level, they employed the UCON model, which manages access control throughout the entire data transfer process, including before, during and after transfer. If any modifications resulting in an unsatisfactory condition occurs, access privileges are revoked. On the user's side, they leverage the advantages offered by the CapBAC model. Subsequently, a policy is established, specifying that a user can only access device data if their access capability is greater than or equal to the attributes of the data producers.

Table 4
Access control solution evaluation according to access control model.

Papers	Access control Model	Advantages
Bouadjemi and Abdi (2020), Cruz et al. (2018)	RBAC	allows the creation of hierarchical levels of permission with inheritance
Dukkipati et al. (2018), Maesa et al. (2017), Pal et al. (2019), Liu et al. (2020), Zhang et al. (2020), Gupta et al. (2021), Mahalle et al. (2013),	ABAC	granularity, context awareness
Gusmeroli et al. (2013), Hernández-Ramos et al. (2016), Xu et al. (2018a), Xu et al. (2018b)	CapBAC	flexibility, lightweight
Ouaddah et al. (2016a), Ouaddah and Bellaj (2021)	OrBAC	Inter-organizational access control
Zhang and Gong (2011), Lohachab and Karambir (2018)	UCON	provides fine-grained access control policies

6. Discussion and open issues

In this section, we delve into a deep discussion of the research solutions we have investigated, while also highlighting the open issues that access control solutions in the IoT environment are currently confronting.

6.1. Discussion

In this section, we evaluate the IoT access control contributions that we have surveyed in this paper. For this purpose, we first categorize the proposed solutions based on their chosen access control model. Table 4 classifies these solutions according to the used access control model. For each access control model, we specify its features. We notice from our conducted study that 60% of the access control solutions that have been cited in this paper, do not rely on a specific access control model. 20% of the studied solutions have proposed contributions that are based on ABAC, 8.33% are based on CapBAC, 3.33% based on OrBAC, 3.33% based on RBAC, 3.33% based on UCON and 1.66% based on the combination of ABAC and RBAC. Such findings lead us to conclude that most researchers prefer to propose their own access control solutions without being imprisoned in the boundaries of a particular access control model. Effectively, since the IoT systems have flexible architectures and are generally modular, the researchers prefer customized access control solutions that fit well with the specificity of their studied IoT system. Furthermore, these access control models, in spite of their high granularity and access control efficiency, are generally complex and require important resources that cannot be offered by the IoT devices. They require high processing time, which raises many challenges for IoT applications. It is also worth noting that even if most of the IoT access control solutions do not rely explicitly on a specific access control model, they are inspired by the existing models. For example, Virtual Private Network Blockchain-based Dynamic Access Control (VPNBDAC) is inspired by the overall concept of ABAC and OrBAC models without using identically all their principles and settings.

There are some access control solutions that are based on central authority management. In such a setting, access policies management is easily handled since a centralized server is kept for all access control policies. Centralized environments are suitable for networks with a limited number of IoT devices like the case of smart homes. However, when

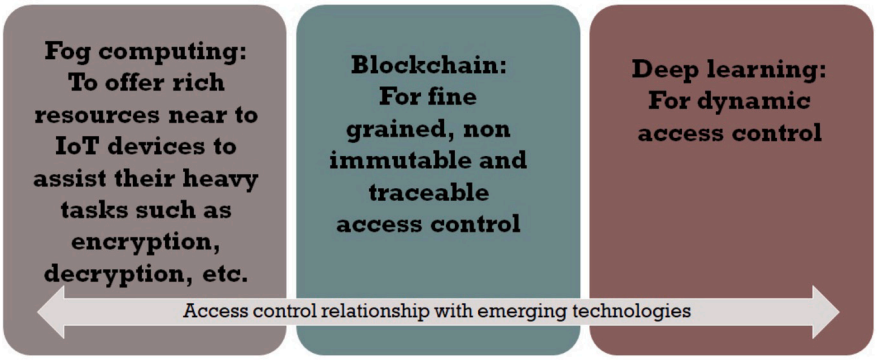

Fig. 5. Impact of emerging technologies on access control techniques.

the number of nodes increases, which is the case of infrastructure-based IoT systems, scalability issues appear and the performance of the IoT network decreases because an overwhelming number of access requests should be treated simultaneously by the same server. Additionally, the centralized IoT access control models face the problem of a single point of failure. Furthermore, they don't follow a user-centric approach as users are unable to control or share their own data. To overcome these drawbacks, fully decentralized solutions have been proposed. These solutions have many challenges that need to be carefully dealt with.

To evaluate the investigated access control solutions, we have defined the following set of requirements that must be considered when designing an access control solution in IoT networks:

- Scalability: An IoT system connects a huge number of devices. The access control system must have the capability to handle this growing number.
- Distribution: The access decision should be managed by a distributed set of nodes to increase the reliability and performance of the access control system and avoid single point of failure.
- Complexity: A lightweight feature is recommended to develop any IoT access control solution due to the constrained resources of IoT devices that cannot handle high computational processes.
- Time efficiency: Any requester should get the access decision quickly to save time. This is a crucial need for time-critical IoT systems.
- Dynamicity: The behavior of the different IoT users may change over time. It is hence crucial to design dynamic access control solutions that handle these changes at run time.
- User-centric: The owner of a resource should be able to control the access of his devices and his resources.
- Granularity: The more the access control policies are fine-grained, the more the solution is reliable. Indeed, fine-granularity ensures a more precise and efficient access control. It offers organizations a more detailed level of access control definition, such as individual users, roles, or specific data elements. This minimizes the risk of unauthorized access or data breaches.

The approaches already mentioned have been evaluated in terms of the above introduced features. Table 5 shows a comparison of access control approaches for IoT. It is clear from Table 5 that most centralized solutions cannot scale well since they rely on a central server. This also affects their response time. In fact, when the number of requests increases, the central server that is responsible for studying these requests may be overloaded and requires additional time to proceed with them. They are hence unsuitable for time-critical IoT systems.

Furthermore, we notice that distributed solutions offer fine-grained access control. We note that many recent access control solutions for IoT systems rely on emerging technologies such as fog computing, blockchain and deep learning as depicted in Fig. 5. Fog computing played a major role in the improvement of access control solutions. Indeed, by offering more powerful resources closer to the IoT devices, the fog nodes help the access control solutions in their resource-demanding tasks such as ABE encryption, decryption, certificate issuing etc.

Likewise, blockchain has brought many advantages to IoT access control. Thanks to smart contracts, blockchain is able to offer fine-grained access control in a totally distributed manner. Using blockchain ensures non-immutable traceability that can help improving access control policies and decisions in the future. However, most blockchain-based access control solutions are complex because they rely on smart contracts that ensure meticulous verification of the requester's information to take the appropriate decision. The more the smart contracts verification is fine-grained and meticulous, the more the solutions become complex and require more time to be achieved. There are a few solutions such that in (Trabelsi et al., 2023) that have overcome this limitation by the combination of VPN and blockchain.

Access control dynamicity and adaptability are of high importance for IoT systems. Indeed, user requirements as well as the execution environment may evolve during system execution. Here, deep learning strategies play a major role since they can learn from past events, detect abnormal access and system vulnerabilities and from the collected data, they can take the appropriate access control decision which allows to get proactive access control.

From our deep study, we can point out the following limitations in the existing approaches. First, we notice that the majority of the proposed solutions are not implemented in reality. However, it is crucial to verify the behavior of the system and to study the impact of adding access control solutions on its performance in the real world. Also, although most of the access control solutions are technically sound and promising, there is a lack of evaluation of the behavior of these solutions in front of real security attacks that try to bypass the access control strategies. Even if theoretically, these solutions face a lot of security attacks, it is essential to verify their efficiency and reliability against real attacks.

Moreover, we noted that despite the multiplicity and the technological progress of the investigated solutions, none of them has treated the integration problem. In fact, there are already numerous existing security systems. It would be very interesting to be able to integrate new security measures into the existing security systems without rebuilding them from scratch. This would certainly save time and cost, but raises new integration and interoperability challenges. There is an urgent need to address such a scenario because it is almost frequent in reality.

Finally, there are only few approaches like (Bai et al., 2021) that have spotted the light on certificates management. Nevertheless, this step is of high importance in IoT access control. Effectively, proposing an efficient approach for certificates management ensures efficient authentication and secure communication. Furthermore, since certificates can contain additional information such as roles and attributes related to their owners, the access control can be easily defined according to this information which allows ensuring lightweight fine-grained access control. Certificates ensure dynamic access control by offering the pos-

Table 5
Comparison of access control approaches for IoT.

Solution	Scalability	Distribution	Complexity	Time efficiency	Dynamicity	User-centric	Granularity
RBAC extension (Bouadjemi and Abdi, 2020)	No	No	Medium	No	Yes	No	Medium
PARBAC (Thakare et al., 2020)	No	No	Medium	No	Yes	No	Medium
DCapBAC (Hernández-Ramos et al., 2016)	Yes	Yes	Lightweight	Yes	No	Medium	Medium
XACML (Riad and Cheng, 2021)	No	Yes	Medium	No	No	Medium	Medium
FairAccess (Ouaddah et al., 2016a)	Medium	Yes	Complex	No	No	Yes	No
FairAccess2.0 (Ouaddah and Bellaj, 2021)	Medium	Yes	Complex	No	No	Yes	Yes
(Dorri et al., 2017)	No	Yes	Lightweight	Yes	No	No	No
Blockchain Meets IoT (Novo, 2018)	Yes	Yes	Medium	Yes	No	No	No
BlendCAC (Xu et al., 2018a)	Yes	Yes	Lightweight	No	No	No	Medium
(Dukkipati et al., 2018)	No	Yes	Complex	No	No	No	Yes
(Wang et al., 2018)	Medium	Yes	Complex	No	No	Yes	Yes
(Ali et al., 2017)	Yes	Yes	Medium	No	No	Yes	No
(Maesa et al., 2017)	Medium	Yes	Medium	No	No	Yes	Yes
(Malamas et al., 2019)	Yes	Yes	Medium	Yes	No	No	Yes
RBAC-SC (Cruz et al., 2018)	No	No	Medium	No	No	No	No
IoTChain (Alphand et al., 2018)	No	Yes	Medium	No	No	Yes	No
(Pal et al., 2019)	No	Yes	Complex	No	No	Yes	Yes
LBAC (Qin et al., 2021)	Yes	Yes	Lightweight	No	Yes	No	No
Fabric-IoT (Liu et al., 2020)	Yes	Yes	Lightweight	Yes	Yes	No	Yes
(Hwang et al., 2018)	Yes	Yes	Lightweight	Yes	Yes	No	No
(Outchakoucht et al., 2017)	Medium	Yes	Complex	No	Yes	No	No
(Zhang et al., 2020)	No	Yes	Complex	No	Yes	Yes	Yes
(Kumar and Tripathi, 2021)	Yes	Yes	Lightweight	Yes	Yes	No	No
VPNBDAC (Trabelsi et al., 2023)	Yes	Yes	Lightweight	Yes	Yes	Yes	Yes
(Salonikias et al., 2016)	Medium	Yes	Medium	Yes	Yes	No	Medium
(Xu et al., 2021) (Xu et al., 2020)	Medium	Yes	Medium	Medium	No	Yes	Yes
(Huang et al., 2017)	Medium	Yes	Medium	Medium	Yes	Yes	Yes
(Awan et al., 2023)	Medium	Yes	Complex	No	Yes	No	Yes
(Khalid et al., 2023)	Yes	Yes	Medium	Medium	Yes	Yes	Yes
Bloccess (Ding and Sato, 2023)	No	No	Lightweight	Yes	No	No	Yes
(Mihaljević et al., 2023)	Yes	Yes	Lightweight	Yes	Yes	No	Yes
(Gusmeroli et al., 2013)	Yes	Yes	Lightweight	Medium	No	Medium	Yes
(Gupta et al., 2021)	Medium	No	Complex	No	No	No	Yes
(Das and Namasudra, 2023)	Medium	Yes	Lightweight	No	No	No	Yes
(Han et al., 2022)	Medium	Yes	Complex	No	Yes	No	Yes
(Deebak et al., 2023)	Medium	Yes	Medium	No	Yes	No	No
(Yu et al., 2021)	Medium	Yes	Medium	No	Yes	No	Yes
DBACP-IoTSG (Bera et al., 2021)	No	Yes	Medium	No	Yes	No	No
TRAC (Li et al., 2022)	Medium	No	Medium	No	Yes	No	Yes
(Wang et al., 2023)	Medium	Yes	Lightweight	Medium	Yes	No	No
SMAC (Saxena et al., 2015)	Yes	No	Lightweight	Yes	No	No	No
(Cirani and Picone, 2015)	Yes	Yes	Medium	No	No	Yes	Yes
(Mahalle et al., 2013)	Yes	Yes	Complex	No	Yes	No	Yes
(Xu et al., 2018b)	Yes	Yes	Lightweight	Yes	Yes	No	Yes
(Lohachab and Karambir, 2018)	Medium	No	Medium	No	Yes	No	Medium
(Zhang and Gong, 2011)	No	No	Complex	No	No	No	Yes
(Song et al., 2021)	Medium	Yes	Medium	No	Yes	No	No
(Truong et al., 2022)	Medium	Yes	Lightweight	No	No	No	No
(Khalid et al., 2020)	Medium	Yes	Complex	No	Yes	No	No
BacS (Shi et al., 2021)	Medium	Yes	Medium	No	No	No	No
(Feng et al., 2021)	Medium	Yes	Medium	No	No	No	No
(Abdi et al., 2022)	Medium	Yes	Complex	No	No	No	Yes
(Ameer et al., 2022)	Medium	Yes	Complex	No	No	No	Yes
(Zahoor et al., 2023)	Medium	Yes	Medium	No	No	No	No
(Nobi et al., 2022)	Medium	Yes	complex	No	Yes	No	Yes
(Thilagam et al., 2022)	Yes	Yes	Complex	No	No	No	Yes
(Liu et al., 2021)	Medium	Yes	Complex	No	Yes	No	Yes
(Stanciu, 2017)	No	Yes	Medium	No	No	No	No
(Gowda et al., 2023)	No	Yes	Medium	No	No	No	No
(Almadhoun et al., 2018)	No	Yes	Medium	Medium	No	No	No
(Wu and Ansari, 2020)	No	Yes	Complex	No	No	No	No

sibility to revoke a certificate when its owner has an abnormal behavior that may harm the IoT system and its users. Hence, further focus should be attributed to the certificates management to reinforce the IoT system security.

6.2. Open issues

We start this subsection by giving our survey limitations. Then, we specify the open issues of the IoT access control field.

6.2.1. Survey limitations

Our survey has only focused on access control solutions for infrastructure-based, SOHO and time-critical IoT systems. There are other interesting application domains that require different access control solutions like the case of IIoT. It would be interesting to cover other domains. Also, it is alluring that the survey studies the various security attacks that an IoT system may face and specify for each proposed access control solution if it is able or not to face a given attack and how.

6.2.2. IoT access control solutions issues

Based on the study that we have conducted in this paper, we can state that despite the progress in IoT access control solutions, these latter still face some challenges that should be solved. The IoT acclivity, heterogeneity and its multi-party resource sharing raise new challenges and open issues for IoT access control solutions. We outline in the following some of these open issues:

- Conflicting access control policies:

Having only one owner entity for all IoT devices is a straightforward task for most access control solutions. However, this task becomes of great complexity if the IoT devices belong to various entities belonging to different organizations and use disparate access control policies that might be, in some situations, conflicting. It is hence, required to have a cross-organizational access control approach that manages perfectly and efficiently the inter-organizational access control.

- Imperfect policy conversion:

When we have an IoT consortium made up of muli-parties, it is likely that each one of them uses a different access control model. As a first step to handle this difference, all the models should be converted into a single one. The most likely model to be used in IoT is ABAC. However, converting other models to ABAC may raise new problems, because it is not always possible to find adequate and suitable attributes if the model is not an ABAC from the beginning.

Lack of effective exploitation of fog computing:

One of the most important issues in IoT access control solutions is the resource shortage of IoT devices. This has led them to rely on central servers to manage the access control. However, this hinders the resource owners to manage freely the access to their devices, in addition to the problem of scalability and single point of failure. As we have already stated, there are some contributions that have applied access control solutions onto fog nodes to avoid the excessive use of IoT devices and to get a reduced decision time. However, we notice that these solutions are still in their infancy and that they do not profit properly from the different features that can be offered by fog computing. In fact, in the existing solutions, we didn't observe effective collaboration among fog nodes in the access control. Such collaboration will probably lead to better decisions with less time. Also, a fog node might receive a high number of access requests and this would lead to its overloading. Hence, it is crucial to study this problem while applying load balancing techniques among the fog nodes.

Conflicting fog computing characteristics

It is evident that fog nodes require to collaborate with each other to improve their quality of service and offer a better user experience. However, delegating some tasks to other fog nodes may lead to confidential data leakage from one fog domain to another. Such task offloading issues may even contradict some access control rules. Also, the use of fog computing may cause the disclosure of the location of the IoT device which infringes the privacy of its user.

Trust in fog nodes

It is obvious that each IoT device will be associated with the nearest fog node to it. However, how to be sure that this fog node is trustworthy? It may be possible that an attacker integrates some fog nodes to provoke private data leakage and disturb the entire system. The use of authentication protocol may help IoT devices to know the identity of the fog nodes. However, they are unable to evaluate its trust level. The use of a centralized trusted authority may be helpful but the centralization as we stated above will add new problems. Also, the centralized trust authority is unable to detect the misbehavior of a fog node that was trustful but has been attacked and become a rogue node.

Blockchain applicability

In spite of the fact that blockchain has improved access control solutions, it has brought new challenges regarding its highly demanding resources. The use of blockchain over fog nodes has relieved some of these challenges but it has not eradicated them. In fact, fog nodes are not very powerful and their work in the access control is not restrained to the blockchain tasks but they are generally responsible for encryption, decryption etc. All these tasks require lots of resources which decrease the performance of the network. Most of the proposed solutions concentrate on the performance evaluation of the security and on the efficiency of the proposed access control scheme. However, it is of extreme importance to know the impact of the proposed solution on the overall network performance and on its functional requirements.

7. Conclusion and future direction

This paper provided a survey of different access control solutions in IoT environments. It is expected to be an effective guide that facilitates further understanding of access control solutions. We started by introducing the existing access control models. Then, we classified access control solutions into centralized and distributed solutions. We have noticed that centralized solutions are simpler and easier to administrate and manage. They offer also a uniform access control policy and centralized auditing. In practice, these solutions are suitable for smart homes that have a limited number of IoT devices. However, they do not scale well since they rely on a central authority that can be overloaded when the number of devices and requests increases. For larger environments and bigger systems such as smart cities, distributed access control solutions are more efficient than the centralized solutions because they handle efficiently the increasing number of devices, scale well and are fault-tolerant.

Such categorization into centralized and distributed approaches is of extreme importance for industries and organizations since it helps them to choose the most appropriate architecture that responds to their specific requirements. It opens up avenues for further exploration, such as looking over hybrid models combining centralized and distributed approaches to take advantage of both of them.

Because of the large-scale IoT network, different organizations need to cooperate with each other. The scenario where a given IoT device belonging to an organization requests to access resources, belonging to other organizations is very frequent. It is hence crucial to control the access between them. For this reason, we have provided a study on inter-organizational access control solutions. This classification illustrated the requirements of inter-organizational solutions such as dynamicity, distribution and scalability.

Based on our deep analysis of the access control solutions from a wide range of IoT applications, we have found that using emergent technologies like blockchain, fog computing and deep learning improves the efficiency of the access control solutions. Effectively, the most efficient access control researches have combined the use of encryption/decryption techniques with blockchain applied in fog nodes near to the IoT devices to reduce latency. In fact, blockchain offers benefits over traditional access control solutions in the IoT domain. These benefits include enhanced security, privacy and improved interoperability and scalability. Deep learning offers a dynamic access control that can change the access decision according to users' behavior, network status, etc.

These findings are of great importance because they help security specialists to improve the efficiency and the security of their deployed security solutions by leveraging the emergent technologies that allow them to design a dynamic access control solution with improved interoperability and scalability. This would certainly revolutionize industries relying on IoT applications by offering increased levels of trust, efficiency and flexibility in access control processes. However, in spite of the great progress that the access control solutions have reached, there

are still some challenges and open issues that need more investigation to optimize them and improve their security level with keeping a good network quality of service. Also, we stress the fact that having appropriate access control schemes is not sufficient to ensure the required security level in IoT systems. This comes essentially from the specificities of IoT devices that are extremely tiny and portable. Hence, they can be easily stolen and their content can be revealed. It is then required to dig into techniques of physical locking, theft protection and concealment of access ports and to combine them with the studied access control solutions to reinforce their security.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Abdi, A.I., Eassa, F.E., Jambi, K., Almarhabi, K., AL-Ghamdi, A.S.A.-M., 2020. Blockchain platforms and access control classification for IoT systems. Symmetry 12.

Abdi, A.I., Eassa, F.E., Jambi, K., Almarhabi, K., Khemakhem, M., Basuhail, A., Yamin, M., 2022. Hierarchical blockchain-based multi-chaincode access control for securing IoT systems. Electronics 11, 711.

Abdulrahman, E., Alshehri, S., Cherif, A., 2021. Blockchain-based access control for the Internet of Things: a survey. In: 2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, pp. 1–6.

Akhuseyinoglu, N.B., Joshi, J., Al-Tudjman, F., Imran, M., 2020. Access control approaches for smart cities. In: IoT Technologies in Smart-Cities: From Sensors to Big Data, Security and Trust. IET, p. 1.

Al-Qaseemi, S.A., Almulhim, H.A., Almulhim, M.F., Chaudhry, S.R., 2016. IoT architecture challenges and issues: lack of standardization. In: 2016 Future Technologies Conference (FTC), pp. 731–738.

Ali, M.S., Dolui, K., Antonelli, F., 2017. IoT data privacy via blockchains and IPFS. In: Proceedings of the Seventh International Conference on the Internet of Things. IoT '17. Association for Computing Machinery, New York, NY, USA.

Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K., 2018. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA). IEEE, pp. 1–8.

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L., Zanichelli, F., 2018. IoTChain: a blockchain security architecture for the Internet of Things. In: 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, pp. 1–6.

Alshehri, A., Sandhu, R., 2017. Access control models for virtual object communication in cloud-enabled IoT. In: 2017 IEEE International Conference on Information Reuse and Integration (IRI). IEEE, pp. 16–25.

Ameer, S., Benson, J., Sandhu, R., 2022. An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach. Information 13, 60.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference. EuroSys '18. Association for Computing Machinery, New York, NY, USA.

Awan, S.M., Azad, M.A., Arshad, J., Waheed, U., Sharif, T., 2023. A blockchain-inspired attribute-based zero-trust access control model for IoT. Information 14, 129.

Bagga, P., Das, A.K., Chamola, V., Guizani, M., 2022. Blockchain-envisioned access control for Internet of Things applications: a comprehensive survey and future directions. Telecommun. Syst. 81, 125–173.

Bai, L., Fan, K., Bai, Y., Cheng, X., Li, H., Yang, Y., 2021. Cross-domain access control based on trusted third-party and attribute mapping center. J. Syst. Archit. 116, 101957.

Bera, B., Saha, S., Das, A.K., Vasilakos, A.V., 2021. Designing blockchain-based access control protocol in IoT-enabled smart-grid system. IEEE Int. Things J. 8, 5744–5761.

Bertin, E., Hussein, D., Sengul, C., Frey, V., 2019. Access control in the Internet of Things: a survey of existing approaches and open research questions. Ann. Telecommun. 74, 375–388.

Bokefode Jayant, D., Ubale Swapnaja, A., Apte Sulabha, S., Modani Dattatray, G., 2014. Analysis of DAC MAC RBAC access control based models for security. Int. J. Comput. Appl. 104, 6–13.

Bouadjemi, A., Abdi, M.K., 2020. Towards an extension of RBAC model. Int. J. Comput. Digit. Syst. 10, 1–11.

Bouij-Pasquier, I., Ouahman, A.A., Abou El Kalam, A., de Montfort, M.O., 2015. SmartOrBAC security and privacy in the Internet of Things. In: 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA). IEEE, pp. 1–8.

Cirani, S., Picone, M., 2015. Effective authorization for the Web of Things. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, pp. 316–320.

Cruz, J.P., Kaji, Y., Yanai, N., 2018. RBAC-SC: role-based access control using smart contract. IEEE Access 6, 12240–12251.

Dalla Palma, S., Pareschi, R., Zappone, F., 2021. What is your distributed (hyper) ledger? In: 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). IEEE, pp. 27–33.

Das, S., Namasudra, S., 2023. Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure. IEEE Trans. Ind. Inform. 19, 821–829.

Deebak, B.D., Memon, F.H., Dev, K., Khowaja, S.A., Wang, W., Qureshi, N.M.F., 2023. TAB-SAPP: a trust-aware blockchain-based seamless authentication for massive IoT-enabled industrial applications. IEEE Trans. Ind. Inform. 19, 243–250.

Maesa, D. Di Francesco, Mori, P., Ricci, L., 2017. Blockchain based access control. In: Distributed Applications and Interoperable Systems: 17th IFIP WG 6.1 International Conference, DAIS 2017, Held as Part of the 12th International Federated Conference on Distributed Computing Techniques, DisCoTec 2017, Neuchâtel, Switzerland, June 19–22, 2017, Proceedings 17. Springer, pp. 206–220.

Ding, Y., Sato, H., 2023. Bloccess: enabling fine-grained access control based on blockchain. J. Netw. Syst. Manag. 31, 6.

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2017. Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, pp. 618–623.

Dukkipati, C., Zhang, Y., Cheng, L.C., 2018. Decentralized, blockchain based access control framework for the heterogeneous Internet of Things. In: Proceedings of the Third ACM Workshop on Attribute-Based Access Control. ABAC'18. Association for Computing Machinery, New York, NY, USA, pp. 61–69.

Feng, Y., Zhang, W., Luo, X., Zhang, B., 2021. A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT. IEEE Trans. Ind. Inform. 18, 2840–2848.

Fersi, G., 2021. Fog computing and Internet of Things in one building block: a survey and an overview of interacting technologies. Clust. Comput. 24, 2757–2787.

Gowda, N.C., Manvi, S.S., Malakreddy, B., Lorenz, P., 2023. BSKM-FC: blockchain-based secured key management in a fog computing environment. Future Gener. Comput. Syst.

Guo, Q., Li, M., Wang, W., Liu, Y., 2022. A dynamic deployment method of security services based on malicious behavior knowledge base. Sensors 22, 9021.

Gupta, M., Awaysheh, F.M., Benson, J., Alazab, M., Patwa, F., Sandhu, R., 2021. An attribute-based access control for cloud enabled industrial smart vehicles. IEEE Trans. Ind. Inform. 17, 4288–4297.

Gusmeroli, S., Piccione, S., Rotondi, D., 2013. A capability-based security approach to manage access control in the Internet of Things. Math. Comput. Model. 58, 1189–1205.

Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., Li, K.-C., 2022. A blockchain-based auditable access control system for private data in service-centric IoT environments. IEEE Trans. Ind. Inform. 18, 3530–3540.

Hassan, R.J., Zeebaree, S.R.M., Ameen, S.Y., Kak, S.F., Sadeeq, M.A.M., Ageed, Z.S., AL-Zebari, A., Salih, A.A., 2021. State of art survey for IoT effects on smart city technology: challenges, opportunities, and solutions. Asian J. Res. Comput. Sci. 8, 32–48.

Hemmati, A., Rahmani, A.M., 2022. The Internet of Autonomous Things applications: a taxonomy, technologies, and future directions. Int. Things 20, 100635.

Hernández-Ramos, J.L., Jara, A.J., Marin, L., Skarmeta, A.F., 2013. Distributed capability-based access control for the Internet of Things. J. Internet Serv. Inf. Secur. 3, 1–16.

Hernández-Ramos, J.L., Jara, A.J., Marín, L., Skarmeta Gómez, A.F., 2016. DCapBAC: embedding authorization logic into smart things through ECC optimizations. Int. J. Comput. Math. 93, 345–366.

Hu, V.C., Ferraiolo, D., Kuhn, R., Friedman, A.R., Lang, A.J., Cogdell, M.M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., et al., 2013. Guide to attribute based access control (ABAC) definition and considerations (draft), NIST Spec. Publ. 800, 1–54.

Huang, Q., Yang, Y., Wang, L., 2017. Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things. IEEE Access 5, 12941–12950.

Hussain, H.A., Mansor, Z., Shukur, Z., 2021. Comprehensive survey and research directions on blockchain IoT access control. Int. J. Adv. Comput. Sci. Appl. 12.

Hwang, D., Choi, J., Kim, K.-H., 2018. Dynamic access control scheme for IoT devices using blockchain. In: 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, pp. 713–715.

John, K., O'Hara, M., Saleh, F., 2022. Bitcoin and beyond. Annu. Rev. Financ. Econ. 14, 95–115.

Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G., 2003. Organization based access control. In: Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks. IEEE, pp. 120–131.

Khalid, M., Hameed, S., Qadir, A., Shah, S.A., Draheim, D., 2023. Towards SDN-based smart contract solution for IoT access control. Comput. Commun. 198, 1–31.
Khalid, R., Javaid, N., Almogren, A., Javed, M.U., Javaid, S., Zuair, M., 2020. A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid. IEEE Access 8, 47047–47062.
Kumar, R., Tripathi, R., 2021. Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model. J. Ambient Intell. Humaniz. Comput. 12, 2321–2338.
Li, N., 2011. Discretionary Access Control. Springer US, Boston, MA, pp. 353–356.
Li, Q., Xia, B., Huang, H., Zhang, Y., Zhang, T., 2022. TRAC: traceable and revocable access control scheme for mHealth in 5G-enabled IIoT. IEEE Trans. Ind. Inform. 18, 3437–3448.
Liu, H., Han, D., Li, D., 2020. Fabric-IoT: a blockchain-based access control system in IoT. IEEE Access 8, 18207–18218.
Liu, Y., Zhang, J., Zhan, J., 2021. Privacy protection for fog computing and the Internet of Things data based on blockchain. Clust. Comput. 24, 1331–1345.
Lohachab, A., Karambir, 2018. Next generation computing: enabling multilevel centralized access control using UCON and CapBAC model for securing IoT networks. In: 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), pp. 159–164.
Mahalle, P.N., Thakre, P.A., Prasad, N.R., Prasad, R., 2013. A fuzzy approach to trust based access control in Internet of Things. In: Wireless VITAE 2013. IEEE, pp. 1–5.
Malamas, V., Dasaklis, T., Kotzanikolaou, P., Burmester, M., Katsikas, S., 2019. A forensics-by-design management framework for medical devices based on blockchain. In: 2019 IEEE World Congress on Services (SERVICES), vol. 2642. IEEE, pp. 35–40.
Malik, N., Nanda, P., He, X., Liu, R.P., 2020. Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology. Wirel. Netw. 26, 4207–4226.
Mihaljević, M.J., Knežević, M., Urošević, D., Wang, L., Xu, S., 2023. An approach for blockchain and symmetric keys broadcast encryption based access control in IoT. Symmetry 15, 299.
Namane, S., Ben Dhaou, I., 2022. Blockchain-based access control techniques for IoT applications. Electronics 11, 2225.
Nobi, M.N., Krishnan, R., Huang, Y., Shakarami, M., Sandhu, R., 2022. Toward deep learning based access control. In: Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy. CODASPY '22. Association for Computing Machinery, New York, NY, USA, pp. 143–154.
Novo, O., 2018. Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Int. Things J. 5, 1184–1195.
Osborn, S., 1997. Mandatory access control and role-based access control revisited. In: Proceedings of the Second ACM Workshop on Role-Based Access Control. RBAC '97. Association for Computing Machinery, New York, NY, USA, pp. 31–40.
Ouaddah, A., Bellaj, B., 2021. FairAccess2.0: a smart contract-based authorisation framework for enabling granular access control in IoT. Int. J. Inf. Comput. Secur. 15, 18–48.
Ouaddah, A., Abou Elkalam, A., Ouahman, A. Ait, 2016a. Fairaccess: a new blockchain-based access control framework for the Internet of Things. Secur. Commun. Netw. 9, 5943–5964.
Ouaddah, A., Mousannif, H., Abou Elkalam, A., Ouahman, A.A., 2016b. Access control in IoT: survey & state of the art. In: 2016 5th International Conference on Multimedia Computing and Systems (ICMCS). IEEE, pp. 272–277.
Ouaddah, A., Mousannif, H., Abou Elkalam, A., Ouahman, A.A., 2017. Access control in the Internet of Things: big challenges and new opportunities. Comput. Netw. 112, 237–262.
Outchakoucht, A., Hamza, E.-S., Leroy, J.P., 2017. Dynamic access control policy based on blockchain and machine learning for the Internet of Things. Int. J. Adv. Comput. Sci. Appl. 8.
Pal, S., Rabehaja, T., Hill, A., Hitchens, M., Varadharajan, V., 2019. On the integration of blockchain to the Internet of Things for enabling access right delegation. IEEE Int. Things J. 7, 2630–2639.
Pal, S., Dorri, A., Jurdak, R., 2022. Blockchain for IoT access control: recent trends and future research directions. J. Netw. Comput. Appl., 103371.
Park, J., Sandhu, R., 2002. Towards usage control models: beyond traditional access control. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, pp. 57–64.
Park, J., Sandhu, R., 2004. The UCONABC usage control model. ACM Trans. Inf. Syst. Secur. 7, 128–174.
Patil, P., Sangeetha, M., Bhaskar, V., 2021. Blockchain for IoT access control, security and privacy: a review. Wirel. Pers. Commun. 117, 1815–1834.
Qin, X., Huang, Y., Yang, Z., Li, X., 2021. LBAC: a lightweight blockchain-based access control scheme for the Internet of Things. Inf. Sci. 554, 222–235.
Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., Fang, B., 2020. A survey on access control in the age of Internet of Things. IEEE Int. Things J. 7, 4682–4696.
Ragothaman, K., Wang, Y., Rimal, B., Lawrence, M., 2023. Access control for IoT: a survey of existing research, dynamic policies and future directions. Sensors 23.
Ravidas, S., Lekidis, A., Paci, F., Zannone, N., 2019. Access control in Internet-of-Things: a survey. J. Netw. Comput. Appl.
Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., Iranmanesh, M., 2023. The Internet of Things (IoT) in healthcare: taking stock and moving forward. Int. Things 22, 100721.
Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 88, 173–190.
Riabi, I., Ayed, H.K.B., Saïdane, L.A., 2019. A survey on blockchain based access control for Internet of Things. In: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), pp. 502–507.
Riad, K., Cheng, J., 2021. Adaptive XACML access policies for heterogeneous distributed IoT environments. Inf. Sci. 548, 135–152.
Rouhani, S., Deters, R., 2019. Blockchain based access control systems. In: State of the Art and Challenges, 2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 423–428.
Saha, R., Kumar, G., Conti, M., Devgun, T., Kim, T.-h., Alazab, M., Thomas, R., 2022. DHACS: smart contract-based decentralized hybrid access control for industrial Internet-of-Things. IEEE Trans. Ind. Inform. 18, 3452–3461.
Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., Zhang, Y., 2020. A smart-contract-based access control framework for cloud smart healthcare system. IEEE Int. Things J. 8, 5914–5925.
Salonikias, S., Mavridis, I., Gritzalis, D., 2016. Access control issues in utilizing fog computing for transport infrastructure. In: Critical Information Infrastructures Security: 10th International Conference. CRITIS 2015, Berlin, Germany, October 5-7, 2015. Springer, Berlin, Germany, pp. 15–26. Revised Selected Papers 10.
Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E., 1996. Role-based access control models. Computer 29, 38–47.
Saxena, A., Duraisamy, P., Kaulgud, V., 2015. SMAC: Scalable access control in IoT. In: 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), pp. 169–176.
Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., Tschofenig, H., 2017. Authentication and authorization for constrained environments (ace), Internet Engineering Task Force. Internet-Draft draft-ietf-aceoauth-authz-07.
Shi, N., Tan, L., Yang, C., He, C., Xu, J., Lu, Y., Xu, H., 2021. BacS: a blockchain-based access control scheme in distributed Internet of Things. Peer-to-Peer Netw. Appl. 14, 2585–2599.
Singh, I., Singh, B., 2022. Access management of IoT devices using access control mechanism and decentralized authentication: a review. Meas. Sens., 100591.
Song, Q., Chen, Y., Zhong, Y., Lan, K., Fong, S., Tang, R., 2021. A supply-chain system framework based on Internet of Things using blockchain technology. ACM Trans. Internet Technol. 21, 1–24.
Sookhak, M., Jabbarpour, M.R., Safa, N.S., Yu, F.R., 2021. Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. J. Netw. Comput. Appl. 178, 102950.
Soumyalatha, S.G.H., 2016. Study of IoT: understanding IoT architecture, applications, issues and challenges, 1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. Int. J. Adv. Netw. Appl. 478.
Stanciu, A., 2017. Blockchain based distributed control system for edge computing. In: 2017 21st International Conference on Control Systems and Computer Science (CSCS). IEEE, pp. 667–671.
Stolojescu-Crisan, C., Crisan, C., Butunoi, B.-P., 2022. Access control and surveillance in a smart home. High-Confid. Comput. 2, 100036.
Thakare, A., Lee, E., Kumar, A., Nikam, V.B., Kim, Y.-G., 2020. PARBAC: priority-attribute-based RBAC model for azure IoT cloud. IEEE Int. Things J. 7, 2890–2900.
Thilagam, K., Beno, A., Lakshmi, M.V., Wilfred, C.B., George, S.M., Karthikeyan, M., Peroumal, V., Ramesh, C., Karunakaran, P., 2022. Secure IoT healthcare architecture with deep learning-based access control system. Am. J. Nanomater., 2022.
Tikhomirov, S., 2018. Ethereum: state of knowledge and research perspectives. In: Foundations and Practice of Security: 10th International Symposium. FPS 2017, October 23-25, 2017. Springer, Nancy, France, pp. 206–221. Revised Selected Papers 10.
Toumi, K., Andrés, C., Cavalli, A., 2012. Trust-OrBAC: a trust access control model in multi-organization environments. In: Information Systems Security: 8th International Conference. ICISS 2012, Guwahati, India, December 15-19, 2012. Springer, pp. 89–103.
Trabelsi, R., Fersi, G., Jmaiel, M., 2023. Private network blockchain-based dynamic access control solution for inter-organizational large scale IoT networks. In: 17th International Conference on Risks and Security of Internet and Systems. CRISIS 2022, Sousse, Tunisia.
Truong, H., Hernández-Ramos, J.L., Martinez, J.A., Bernal Bernabe, J., Li, W., Marin Frutos, A., Skarmeta, A., 2022. Enabling decentralized and auditable access control for IoT through blockchain and smart contracts. Secur. Commun. Netw., 2022.
Vaquero, L.M., Rodero-Merino, L., 2014. Finding your way in the fog: towards a comprehensive definition of fog computing. Comput. Commun. Rev. 44, 27–32.
Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., Guizzetti, R., 2015. OSCAR: object security architecture for the Internet of Things. Ad Hoc Netw. 32, 3–16.
Wang, S., Zhang, Y., Zhang, Y., 2018. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access 6, 38437–38450.
Wang, W., Huang, H., Yin, Z., Gadekallu, T.R., Alazab, M., Su, C., 2023. Smart contract token-based privacy-preserving access control system for industrial Internet of Things. Digit. Commun. Netw. 9, 337–346.
Wu, D., Ansari, N., 2020. A cooperative computing strategy for blockchain-secured fog computing. IEEE Int. Things J. 7, 6603–6609.
Xu, R., Chen, Y., Blasch, E., Chen, G., 2018a. BlendCAC: a blockchain-enabled decentralized capability-based access control for IoTs. In: 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). IEEE, pp. 1027–1034.
Xu, R., Chen, Y., Blasch, E., Chen, G., 2018b. A federated capability-based access control mechanism for Internet of Things (IoTs). In: Sensors and Systems for Space Applications XI, p. 106410U.
Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X., Deng, R.H., 2020. Match in my way: fine-grained bilateral access control for secure cloud-fog computing. IEEE Trans. Dependable Secure Comput. 19, 1064–1077.
Xu, S., Ning, J., Ma, J., Huang, X., Pang, H.H., Deng, R.H., 2021. Expressive bilateral access control for Internet-of-Things in cloud-fog computing. In: Proceedings of the 26th ACM Symposium on Access Control Models and Technologies. SACMAT '21. Association for Computing Machinery, New York, NY, USA, pp. 143–154.
Ye, N., Zhu, Y., Wang, R.-c., Malekian, R., Lin, Q.-m., 2014. An efficient authentication and access control scheme for perception layer of internet of things. Natural Sciences Publishing Cor.
Yu, K., Tan, L., Aloqaily, M., Yang, H., Jararweh, Y., 2021. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE Trans. Ind. Inform. 17, 7669–7678.
Zahoor, A., Mahmood, K., Shamshad, S., Saleem, M.A., Ayub, M.F., Conti, M., Das, A.K., 2023. An access control scheme in IoT-enabled Smart-Grid systems using blockchain and PUF. Int. Things, 100708.
Zhang, G., Gong, W., 2011. The research of access control based on UCON in the Internet of Things. J. Softw. 6, 724–731.
Zhang, P., Chen, Z., Liu, J.K., Liang, K., Liu, H., 2018. An efficient access control scheme with outsourcing capability and attribute update for fog computing. Future Gener. Comput. Syst. 78, 753–762.
Zhang, Y., Yutaka, M., Sasabe, M., Kasahara, S., 2020. Attribute-based access control for smart cities: a smart-contract-driven framework. IEEE Int. Things J. 8, 6372–6384.
Zhao, J., Zeng, P., Choo, K.-K.R., 2021. An efficient access control scheme with outsourcing and attribute revocation for fog-enabled e-health. IEEE Access 9, 13789–13799.

Rahma Trabelsi graduated in Computer Science engineering from the Higher Institute of Applied Science and Technology of Sousse (ISSATso), Tunisia, in 2019. Since December 2020, she has joined the Research Laboratory of Development and Control of Distributed Applications (ReDCAD) at the National School of Engineering of Sfax (ENIS) as a Ph.D. candidate. Her current research focuses on Security, Internet of Things, Access control solutions and Blockchain technology.

Ghofrane Fersi graduated in Computer Science engineering from the National School of Engineers of Sfax (ENIS), Tunisia, in 2008. She received her M.S. degree (DEA) in Systems of Information and dedicated New Technologies (NTSID) in 2009, from ENIS. Since December 2010, she has joined the Research Laboratory of Development and Control of Distributed Applications (ReDCAD) at the National School of Engineering of Sfax (ENIS) as a Ph.D. candidate. She received the Ph.D. degree in computer science from ENIS, University of Sfax in 2014. Since 2013, she has been an Assistant Professor in the Department of computer science in the university of Sousse, Tunisia. She becomes Associate Professor since 2016. Currently, she is an assistant professor at The National School of Engineers of Sfax (ENIS), University of Sfax, Tunisia. Her current research focuses on fog computing, security, Internet of Things protocols, architectures and applications.

Mohamed Jmaiel graduated as a Computer Engineer from the University of Kiel (Germany). He received the Ph.D degree in Computer Science from the Technical University of Berlin in 1996. Since 1995, he has been an assistant professor at The National School of Engineers of Sfax (ENIS), University of Sfax, Tunisia. He becomes an Associate Professor since 2003. Since January 2009, he is a Professor in Computer Science at the National School of Engineers of Sfax (ENIS).