IoT

MDPI

Review

A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art

Mohammad Shamim Ahsan and Al-Sakib Khan Pathan *

Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh; shamim19119@gmail.com

* Correspondence: sakib.pathan@gmail.com

Abstract: The Internet of Things (IoT) is a technologyof connecting billions of devices with heterogeneous types and capabilities. Even though it is an attractive environment that could change the way we interact with the devices, the real-life and large-scale implementation of it is greatly impeded by the potential security risks that it is susceptible to. While the potential of IoT is significant, the security challenges it faces are equally formidable. IoT security can be addressed from different angles, but one of the key issues is the access control model because among the many challenges, access control is a pivotal concern that determines the overall security of IoT systems. This eventually determines which device is given access to the IoT systems and which is denied access. In this work, we conduct a systematic and thorough survey on the state-of-the-art access control models in IoT. This study includes more than 100 related articles, including 77 best-quartile journal papers. We cover conventional as well as advanced access control models, taking the crucial period of various studies in this particular area. In addition, a number of critical questions are answered and key works are summarized. Furthermore, we identify significant gaps in existing models and propose new considerations and prospects for future developments. Since no existing survey explores both conventional and sophisticated access control models with essential challenges, trends and application domains analysis, and requirements analysis, our study significantly contributes to the literature, especially in the IoT security field.

Keywords: conventional model; flexibility; integration support; sophisticated model; taxonomy

Academic Editor: Tareq Hasan Khan

Received: 12 December 2024
Revised: 16 January 2025
Accepted: 21 January 2025
Published: 24 January 2025

Citation: Ahsan, M.S.; Pathan, A.-S.K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. *IoT* **2025**, *6*, 9. https://doi.org/10.3390/iot6010009

1. Introduction

The use of Internet of Things (IoT) devices (e.g., cameras, light sensors, thermostats, etc.) has increased very rapidly in the last few years. According to some recent reports, the number of devices in IoT may reach more than 60 billion by the year 2030 [1,2]. IoT provides a flexible and scalable platform that can offer various applications within a home setting, such as smart home for security, smart home for eldercare or childcare, smart home for energy efficiency, and smart home for a better life (music, entertainment, etc.) [3]. In addition to these, applications of the Internet of Things have been widely expanded to the fields of agriculture, industry, transportation, and infrastructure for different purposes, such as smart harvesting [4], disease monitoring [5], manufacturing [6], supply chain management [7]), real-time vehicle monitoring [8], smart city [9], etc. Interestingly, the study of the Internet of Drones (IoD) has also become popular in recent years [10]. This diversity

and scalability of IoT devices have an opposite side, too. Since these devices are connected to each other and all are then connected to the Internet (i.e., Cyberspace), hacking one of the devices can possibly turn into severe security breaches to all of them. Moreover, as day by day we see IoT is becoming mainstream, it will soon change the way we live, travel, work, and more. Therefore, to protect our data privacy as well as our homes, IoT security is imperative [11].

Authentication, access control, threat detection, and non-repudiation are the most crucial security services for securing IoT devices and networks. Among these, access control plays a pivotal role in handling the entrance of legitimate users to the system. The main goal of the access control mechanism is to restrict unauthorized individuals (or entities) from accessing confidential and protected resources. Typically, an access control solution consists of three basic components, such as (i) users, sensor nodes or subjects, (ii) resources or objects, and (iii) requested operations with a few specific defined policies (rules) for permitting legitimate rights. Ragothaman et al. [12] divide access control process into five functions, such as authentication function, administration function, access control function, managing policies' function, and audit function as depicted in Figure 1 (adopted from [12]). Authentication and access control functions operate trivially to verify identities and manage granting as well as deny access to users or devices, respectively. The main purpose of the administration function is to create, revoke, and manage different users, devices, groups, and policies. Additionally, the audit function is used to keep track of individual records and reviews for evaluating the sufficiency of access control mechanisms to maintain compliance with defined policies and procedures.

Interestingly, there is a clear need to identify, authenticate, and authorize for completing an entire access control model. In the existing literature, any access control system requires three different phases to develop. The first phase is the policy specification, in which a set of rules and conditions are defined for approving and denying access, considering different IoT scenarios and needs. In the next phase, these policies are implemented through access control models. Finally, various low-level hardware and software functions are required to deploy security control that are imposed by the predefined policies [13].

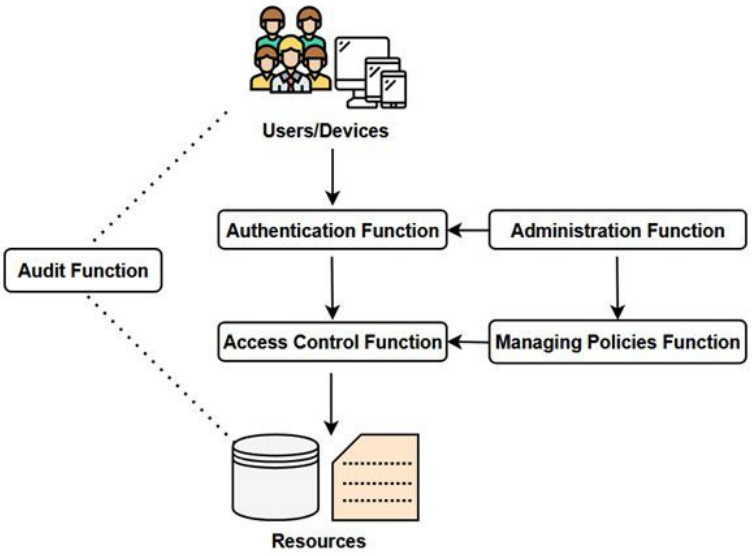

Figure 1. Access control functions in IoT.

Designing access control models in IoT is critical yet underdeveloped, leading to security risks such as data breaches and unauthorized access. In addition, IoT devices often operate on limited computational and processing power, which makes it difficult to develop an efficient and secure access control model. Moreover, due to the diversity of

IoT ecosystems, it is a significant challenge to deploy a scalable and reliable solution for a large array of interconnected devices that work on different local and global networks. Most of the IoT devices are not designed to patch security flaws through frequent updates. Consequently, the system becomes vulnerable to crucial cyber-attacks, data breaches, and even physical harm; thus, threat actors can seamlessly plant malware and spread it to the connected networks.

In this study, we partition access control models into two categories: conventional access control models and advanced access control models. Usually, conventional models set access rights based on roles, attributes, capabilities, usages, trusts, risks, protocols, and relations. The major drawback of these models is the difficulty of specifying, revoking, implementing, and managing policies, especially in complex scenarios. In fact, these frameworks are inappropriate in dynamic and fast-changing environments. Though these models offer scalability, the modeling requires high computational overhead. Additionally, some of them, for instance, organizational-based, protocol-based, trust-based, risk-based, etc., are inflexible in nature. Moreover, several conventional models are rigid and need continuous enforcement, which makes them arguably inefficient for dynamic environments like IoT. On the contrary, advanced access control models leverage blockchain technologies, machine learning (ML) techniques, deep learning (DL) algorithms, and hybrid frameworks. Consequently, they not only adapt to complex patterns and uncertain environments but also provide seamless flexibility as well as enhance security and trust. However, these models require high computational and storage costs since they handle large-scale data and resources. Although numerous research works have been conducted on the conventional access control models, in recent years, researchers tend to be more attracted to advanced models while considering the dynamicity and heterogeneity of the IoT environment.

1.1. Motivation

While there are a number of surveys that address security challenges in IoT, only a few of them study access control solutions for IoT [12–22]. Among this limited number of works, existing surveys mostly focus solely on conventional or advanced models without providing a comprehensive exploration. Although some studies [12,18,19] discuss both types, they are limited to specific models and do not provide a broad overview. Moreover, there is no analysis on the recent trends of IoT access control schemes and their application domains. Furthermore, most of them do not identify the access control requirements that should be satisfied by the existing frameworks. This is essential because the analysis of these requirements will reflect the necessity and feasibility of the existing models, as well as new aspects of development in the future.

1.2. Contributions

In this work, we present a survey on the available access control models along with the specific requirements for the IoT ecosystem. More precisely, we seek to answer the following questions: ***RQ1: What are the major security challenges that cause IoT devices to be vulnerable?*** We identify the main security concerns and challenges in the IoT environment from heterogeneity and scalability to privacy and trust. ***RQ2: What is the classification of access control frameworks for an IoT system?*** We study and categorize the access control models according to the existing research article in the literature. ***RQ3: What are the existing access control frameworks for authorization in IoT?*** We thoroughly study the access control models that exist in the current literature, spanning from role-based, attribute-based frameworks to blockchain-based, machine learning, and deep learning-based ones. In addition, we present a large-scale visualized taxonomy for IoT access control models. ***RQ4: What are the recent trends of access control models and their IoT application***

domains? We explore the mostly utilized models in different IoT application domains and report the analysis. ***RQ5: Which access control requirements are fulfilled by these models?*** In the end of this study, we analyze the access control criteria that are met by the existing models. In summary, our contributions are as follows:

- We analyze the major security issues and challenges that need to be considered while designing authentication and authorization solutions in the IoT ecosystem.
- We present a survey on the access control models for IoT environment, for the first time to date by covering almost all notable existing models from the conventional to the advanced and sophisticated ones.
- To better understand the scale of the existing IoT authorization models, we present a visualized taxonomy of the models on a large scale. Specifically, it will help researchers with a quick overview of the existing IoT access control models and insights into the potential development areas in the coming days.
- We examine the highly used frameworks, their trends in the last several years, and analyze the focus on different IoT application domains.
- We outline which access control requirements are attained by the existing models so that researchers can analyze them and bring about some new and robust solutions.
- Finally, we discuss some possible future challenges and prospects, including a few insightful ideas while developing access control models in IoT.

Before presenting the organization of this paper in the next subsection, let us clarify that here the term "Comprehensive" refers to the coverage area of our study, i.e., how widely this issue has been covered or addressed. Specifically, we explore the IoT access control models at a large scale, which means that both conventional and advanced solutions are investigated.

1.3. Organization

The remainder of the paper proceeds as follows. Section 2 provides the related work with limitations, research gaps, and distinguishing aspects of our work. Section 3 presents the procedure of this survey and data analysis. Next, Section 4 introduces the results of the survey, addressing the mentioned research questions, including the extensive study of the existing access control models. After that, in Section 5, we discuss some challenges including directions for future work. Finally, Section 6 concludes our work.

2. Related Works

2.1. Existing Surveys and Their Limitations

There are a few studies in the literature that explore the access control models in the IoT environment. The findings and limitations of these surveys are described below with categorization according to the access control models they focus on.

Traditional: The work in [13] scrutinized the expanding literature regarding access control for conventional models in the context of IoT. Specifically, the study did not cover advanced access control models that are based on blockchain, machine learning (ML), deep learning (DL), etc. Rather, the authors only reviewed traditional models for IoT. Similar to [13], Ouaddah et al. [14] analyzed and reviewed the authorization process in IoT considering different aspects, such as objectives, architectures, models, and mechanisms. In addition, they conducted both qualitative and quantitative evaluations of the strengths and weakness of each refereed solutions. However, it was incomplete because it did not address crucial aspects, such as clearly identifying the research problems or questions to be answered. Ravidas et al. [15] presented a thorough and comparative examination of authorization solutions for IoT, evaluating them based on predefined requirements and assessment criteria. Additionally, their study offered recommendations for crafting

an authorization framework customized to suit the unique requirements and limitations of prevalent IoT applications. Arguably, the researchers focused on the access control requirements rather than the existing models. Additionally, their study only covered models based on roles, attributes, organizations, and usages. Bertin et al. [16] provided an extensive survey of various models, encompassing access control models as well as access control architectures and protocols. Since they explored diverse aspects of authorization in IoT, they could study only a few conventional schemes.

Traditional and Blockchain: Ragothaman et al. [12] conducted a comprehensive examination of access control necessities, authorization frameworks, access control models, and policies. Their review encompassed various facets of access control, focusing particularly on conventional methods alongside blockchain-based models. Moreover, a few existing papers were studied regarding those models. Qui et al. [17] presented a survey where they initially delineated two primary categories of requirements: access control policy composition and access control policy authoring, aimed at facilitating access control in IoT. Subsequently, they examined existing literature to fulfill these requirements, introducing relevant models and systems. After that, they addressed policy combination and conflict resolution. Finally, the authors studied authorization models. However, one of the main drawbacks of this work is its limited review of both traditional and blockchain-based access control models, as their primary focus was not on authorization models exclusively. In addition, the study lacked ML, DL, trust, protocol-based, and hybrid models, which are sophisticated and state-of-the-art schemes.

Blockchain: Namane et al. [20] introduced a classification system for access control in IoT, based on blockchain technology, distinguishing between partially decentralized and fully decentralized approaches across various IoT applications. Pal et al. [22] examined current trends and essential requirements for utilizing blockchain-based approaches in IoT access control systems.

Others: Ahmed et al. [18] delved into the application of machine learning techniques to improve authentication and authorization within the IoT framework. Though they provided a study on ML-based authorization schemes, a few existing works were reviewed and there was no conceptual architecture. Pal et al. [19] discussed both hybrid and protocol-based access control methods for IoT systems, highlighting their potential to address the shortcomings of conventional access control systems. Similar to [12], different aspects of access control for IoT were studied in [21]. Specifically, the survey explored authorization requirements for IoT, categorizing them into various phases such as defining, administrating, evaluating, and imposing policies. Then, the authors discussed disparate technologies like authorization models, architecture, protocol, structure of data, etc. However, the study mentioned only a few traditional models.

2.2. Research Gap Analysis

In this work, we define an access control model as the mechanism with a set of defined policies and rules to protect resources (or objects) by restricting unauthorized subjects (users, or devices). Since IoT is a dynamic system comprising heterogeneous data from various interconnected devices, platforms, and technologies, access control management demands sophisticated strategies in particular. In the literature, most of the surveys have explored different aspects of access control for IoT, rather than explicitly focusing on access control models. Moreover, though a few works aimed at access control models, they covered only the traditional ones or lacked reviewing the advanced models. Consequently, as far as we have investigated, no work in the literature has studied all conventional and advanced state-of-the-art access control models for IoT at a large scale. Without an extensive investigation on both categories of solutions, the gradual evolutions as well as

the proper picture of the existing IoT access control security can hardly be understood. Consequently, the reasoning of adopting new technologies and the development of the future sophisticated models will be affected.

2.3. Distinction from Prior Work

This paper examines the existing access control models relevant to the Internet of Things (IoT). Our primary and differentiating goal is to study both conventional and advanced models. In particular, role-based (RBAC), attribute-based (ABAC), capability-based (CapBAC), usage control (UCON), organizational-based (OrBAC), trust-based (TBAC), blockchain-based, protocol-based (ProBAC), relationship-based (ReBAC), risk-based, temporal and spatio-temporal based, hybrid-based (HyBAC), ML-based, DL-based, and miscellaneous types of IoT access control models are studied in this work. In this way, we aim to address the research gap in providing a thorough survey of access control models for IoT. We also depict a large-scale taxonomy of the access control models, including qualitative evaluation of them according to certain criteria. Moreover, we analyze the recent trends of these models and the concentration on different specific IoT application domains alongside studying the access control requirements fulfilled by these schemes. An in-depth comparison with some existing works in terms of covering different access control models is depicted in Table 1.

Table 1. Comparison with other surveys that work on IoT access control models. "T&ADA" and "RA" represent "Trends and Application Domains Analysis" and "Requirements Analysis", respectively.

Work	Access Control Models															T&ADA	RA
	RBAC	ABAC	CapBAC	UCON	OrBAC	TBAC	BC-Based	ProBAC	ReBAC	Risk-Based	T&ST-Based	HyBAC	ML-Based	DL-Based	Others		
[12]	✓	✓	✓	✓	✓		✓		✓								✓
[13]	✓	✓	✓	✓	✓				✓								✓
[14]	✓	✓	✓	✓	✓			✓									
[15]	✓	✓		✓	✓												
[16]	✓	✓			✓												
[17]	✓	✓	✓	✓	✓		✓				✓						
[18]	✓	✓	✓											✓			
[19]								✓				✓					
[20]							✓										
[21]	✓	✓	✓				✓						✓				
[22]							✓										
Ours	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

3. Methodology of This Survey

3.1. Search Strategy

To conduct this study, at first, relevant works were searched in established and well-known online sources, such as IEEE Xplore digital library, ACM digital library, Elsevier, Springer, MDPI, and so on. For searching, we used some keywords related to specific access control models like "role-based IoT access control models", "machine learning-based IoT access control models", "trust-based IoT access control models", etc., as well as access control frameworks in general such as "access control models for IoT". Then, only the papers written in English were selected. In addition, the selected works were published between the years 2011 and 2024. Regarding exclusion, the papers not focusing on the IoT access control models were eliminated. Irrelevant and duplicate works were removed. Moreover, papers written in foreign languages were excluded. Apart from this, we explored related surveys and other IoT security papers, which were not included in the dataset. A list of paper selection criteria is outlined in Table 2.

Table 2. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Research papers published in English language were included	Papers written in other than English language were not selected
Peer-reviewed original research works satisfying the scope were selected	Papers not related to other aspects of access control (rather than "models") were removed
Research papers, conference proceedings, book chapters, or magazines relevant to the scope were selected	Papers not focused on IoT were removed
Research papers ranging in years from 2011 to 2024 were selected	Duplicate papers and survey papers were eliminated

3.2. Findings of Data Analysis

After applying the search strategy, we gathered a dataset consisting of 115 papers, containing both conference and journal works on access control models for IoT. Among these, 77 are journal papers and the rest of them are conference papers. Figure 2 shows the conference vs. journal distribution of our collected data.

Looking at the 115 papers, we can see that in recent times, a good number of researchers eagerly addressed the access control models, especially for IoT. Our collected data reveal that the highest number of works was published in 2023 and 2019 with 14 papers each, followed by 13 papers in 2017 and 2024 each, and 11 papers in both 2018 and 2020. Before 2017, the access control frameworks were not studied in such a focused way as depicted in Figure 3.

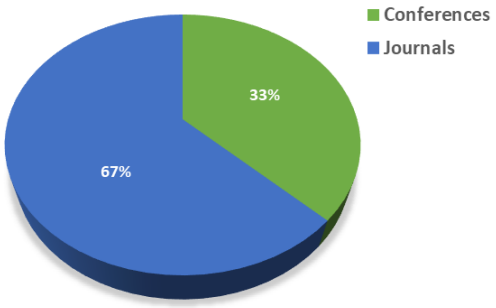

Figure 2. Percentile of conference vs. journal papers studied in this survey.

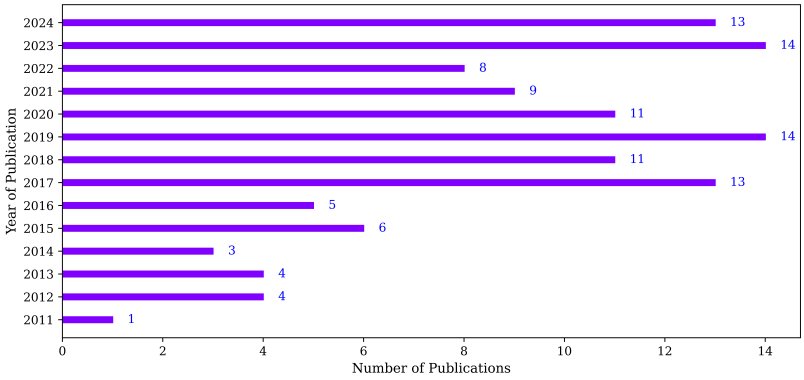

Figure 3. Year-wise publications for access control models in IoT, included in this survey.

Apart from this observation, we outlined the papers' volume related to each access control model for IoT. Notably, we found that blockchain-based access control models are explored in extensive manner having 22 journal papers and 4 conference papers. The second highest position is held by deep learning-based models with a total of 12 papers (8 journals and 4 conferences). Simultaneously, role-based, attribute-based, capability-based, protocol-based, and hybrid solutions are also studied in a decent manner. Figure 4 illustrates the dissection of the publication amount for individual works.

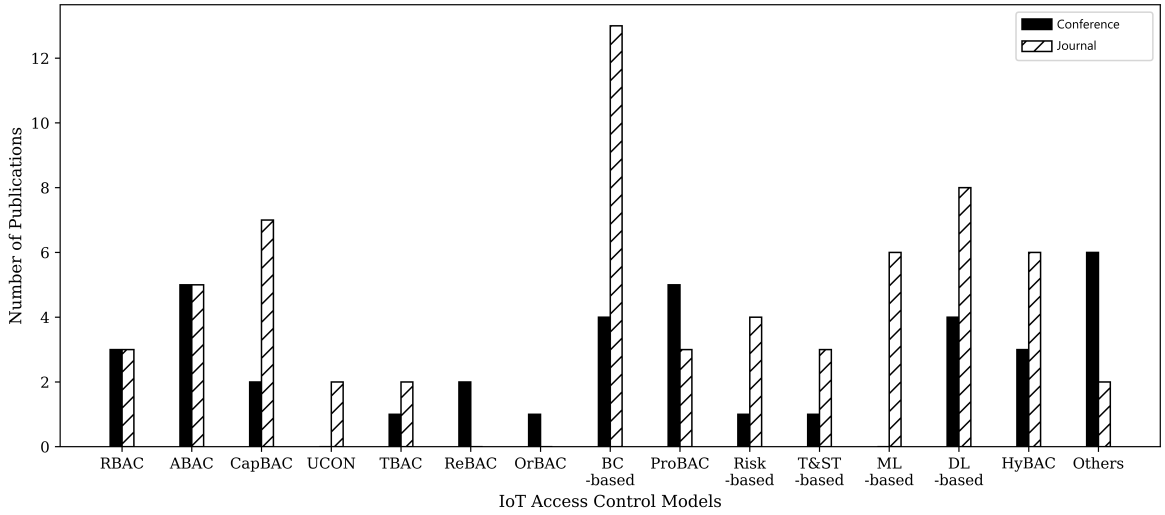

Figure 4. Number of conference and journal papers for different access control models in IoT, considered within this survey.

3.3. Investigation of Journal Papers

Further analysis on 42 journal papers reveals that they are collected from 37 journals in total, where almost half of them are ranked as Q1 journals. Simultaneously, the number of Q2 and Q3 journals is also significant. Notably, a negligible number of collected works are from Q4 journals, which indicates the inclusion of high-quality and well-established research in this survey. A donut plot is drawn in Figure 5 to illustrate the percentage of different quartile journals (according to Scopus) studied in this survey.

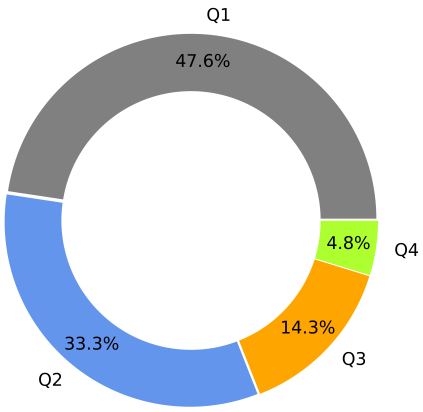

Figure 5. Percentile of different quartile journals included in this survey [Q1 = 20, Q2 = 14, Q3 = 6, Q4 = 2].

4. Outcome of This Survey

4.1. RQ1: What Are the Major Security Issues and Challenges in the IoT Environment?

Despite the considerable advantages of the increasing use of smart home IoT devices, security remains a significant concern for these devices, with various stakeholders expressing apprehension that could potentially hinder the pace of adoption [23]. Since IoT devices are connected and all are then connected to the Internet, this poses a great threat to security issues. This is because, if someone hacks into one of these devices, they can easily hack into all of them in a systematic manner. In this process, an attacker can compromise thousands of devices without anyone's notice, utilizing them via a command-and-control server to execute widespread attacks on critical systems. Consequently, the focus is on securing interconnected devices, safeguarding data, and fortifying networks within IoT.

One of the most critical issues is the substantial diversity across IoT ecosystems, exacerbating the security risks associated with the Internet. Specifically, the insecure web and mobile interfaces, loosely secure IoT devices and applications, insufficient physical security in urban areas, untrustworthy IoT databases, and infeasibility of the typical encryption techniques are the prime issues among them [24]. Hence, to address this, it is mandatory to devise effective cryptographic systems that can provide expected output and adapt lightweight security protocols that would provide a secure end-to-end correspondence network. To efficiently distribute the necessary credentials and aid in establishing the required session keys among associated devices, effective key management systems must be deployed [25]. In addition, traditional security mechanisms, such as strong encryption of data and communication, and countermeasures cannot be directly implemented in IoT technologies due to their constrained computational capabilities [23]. Consequently, these devices are compelled to operate using encryption algorithms with low computational overhead that execute quickly [26]. Moreover, most of the IoT devices are "closed" and "secure by design" ("Built-in Security"); that is, manufacturers typically do not handle security patching and system upgrades for IoT devices post-sale, unlike the process followed for other computing systems such as personal computers [27]. Furthermore, the proliferation of connected devices poses scalability challenges. Therefore, delivering scalable and reliable solutions for the vast array of interconnected devices spanning various local or global networks presents a significant challenge.

Security concerns such as Man-In-The-Middle (MITM) attacks, Denial of Service (DoS/DDoS) attacks, conflicts in WLAN applications, and potential risks associated with IPv6 usage [28], as well as application-specific security issues like user authentication, information access, and platform management [29] impede the implementation of IoT security measures. Moreover, regarding specific IoT devices, vulnerabilities and privacy issues of security cameras, especially in the surveillance systems, are studied widely in the literature [30–32]. Specifically, these devices are prone to severe cyber-attacks like visual layer attacks, covert channel attacks, Denial-of-Service (DoS) attacks, and jamming attacks. Therefore, to enhance usability and gain user acceptance, it is crucial to establish effective security, privacy, and trust models tailored to the context of IoT applications [25]. In terms of security, advanced user authentication and authorization mechanisms are required to mitigate unauthorized access as well as there should be a guarantee for data confidentiality, integrity, and anonymity. To adhere to privacy standards, it is crucial to ensure the security and confidentiality of users' sensitive information when dealing with IoT devices. Ultimately, trust [33,34] must be built up in the IoT ecosystem, ensuring that heterogeneous data are processed and managed in alignment with user requirements and rights. Above all, addressing privacy and security concerns have to be considered with a significant level of adaptability [35].

4.2. RQ2: What Is the Classification of Access Control Frameworks for IoT System?

In the literature, access control models, especially for IoT, can be partitioned into two major categories: conventional access control models and advanced access control models (see Figure 6). Usually, conventional frameworks set access rights based on roles, attributes, capabilities, usages, trusts, risks, protocols, and relations. On the other hand, advanced models leverage blockchain technologies, machine learning (ML) techniques, deep learning (DL) algorithms, and hybrid frameworks. There are a few other schemes that rely on historical data, identities, and privileges. Since these schemes are not notably studied in the literature, we do not include these for Figure 6. However, these models can be considered as conventional ones. Typically, the traditional models are rigid and need continuous enforcement, which make them arguably inefficient for heterogeneous environments like

IoT. On the contrary, the state-of-the-art models can adapt to complex patterns and uncertain environments. However, these frameworks require high computational and storage costs since they handle large-scale data and resources.

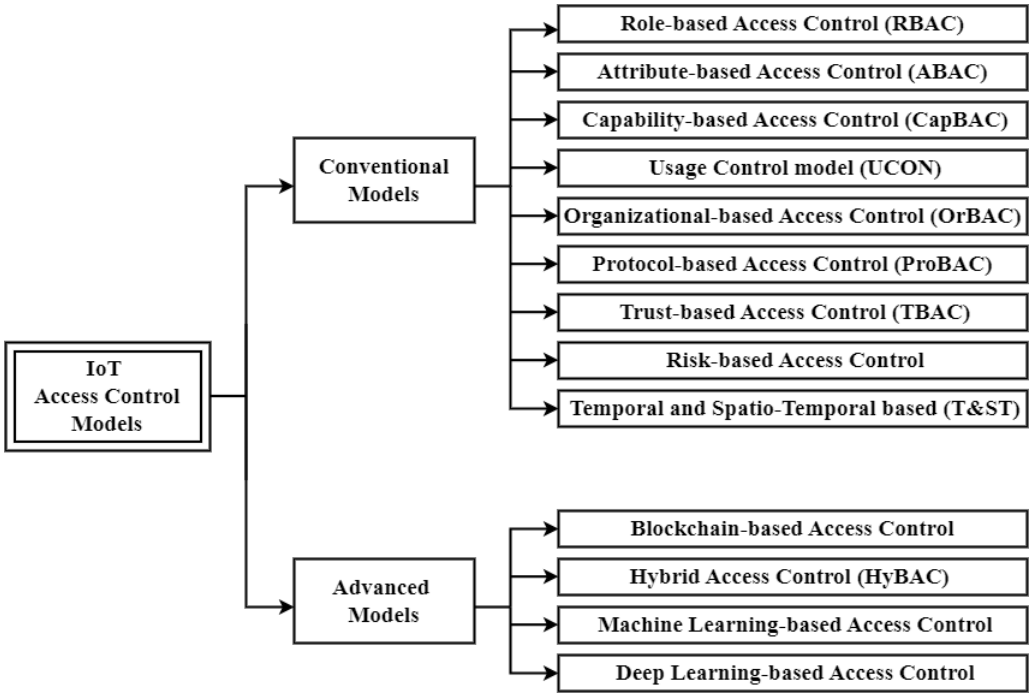

Figure 6. Classification of the existing IoT access control models.

4.3. RQ3: What Are the Existing Access Control Models to Protect IoT Systems?

Access authorization stands out as a crucial security challenge for IoT, particularly concerning resource sharing and safeguarding information. Numerous studies and surveys have explored the challenges and requirements of access control models in IoT applications [12,14–16,18,21,36]. Our analysis focuses specifically on the various access control models documented in the literature. For precise understanding, we present a large-scale IoT access control model taxonomy in Figure 7.

We now explore and examine various types of existing access control models for IoT, including necessary architectural designs.

4.3.1. Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Identity-Based Access Control (IBAC)

As per the Trusted Computer System Evaluation Criteria (TCSEC), access control models can be categorized into mandatory access control (MAC) [37] and discretionary access control (DAC) [38]. MAC is the strictest control method, where access privileges are determined by rules established by a central authority or an administrator, and all the access control settings and configurations are only accessible to the authority. Though this model has some advantages of robustness, high security, and centralized resource management, it is not appropriate because of its lower management efficiency and usability.

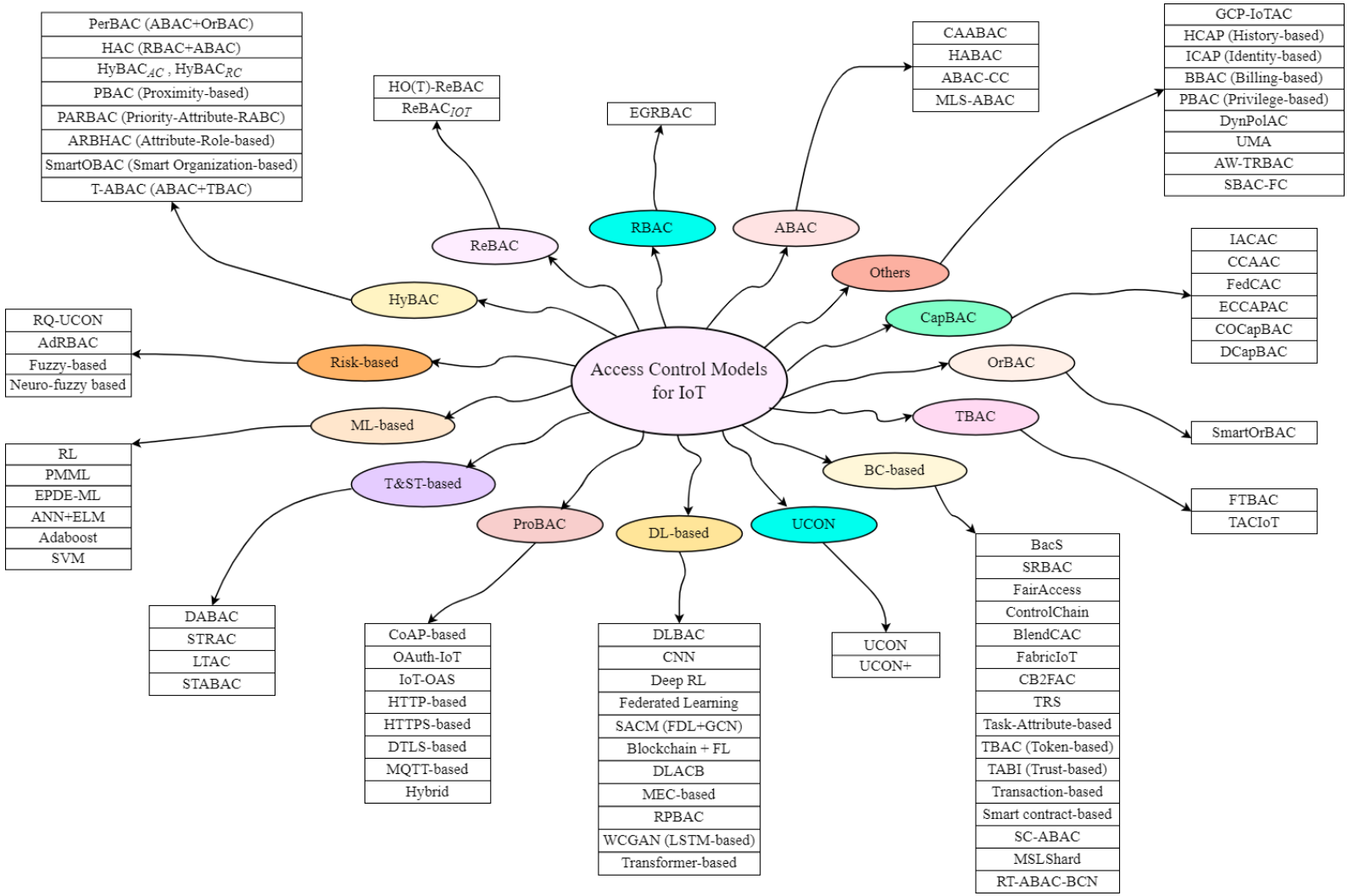

Figure 7. Taxonomy of different IoT access control models.

In the DAC model, the users retain control over their resources, enabling data owners and information systems to determine both the individuals who can access the resources and the extent of their access through authorization via access control lists (ACLs). Authorized users have the capability to access objects, such as data entities, either as individuals or as part of groups, and some users have the ability to independently assign access permissions to objects they possess to other users. However, DAC is unsuitable for IoT search since this model requires managing users, authorities, and resources manually, resulting in high-complexity management work [36]. Another conventional access control method, called identity-based access control (IBAC), is not well-suited for IoT systems due to the vast number of unidentified identities in IoT, making it nearly impractical to generate ACL for each one.

4.3.2. Role-Based Access Control (RBAC)

In this model, permissions are linked with roles, and users are assigned to relevant roles, thereby inheriting the permissions associated with those roles [39]. Since traditional access control models encountered difficulties addressing large-scale authorization management, RBAC was developed to restrict system access to authorized users fulfilling complex application layer access requirements [40]. In [41], Liu et al. proposed an authentication and access control solution for IoT, advocating for the establishment of an architecture where each object would register in advance with the nearest reliable gateway, referred to as the registration authority (RA). Ameer et al. [42] presented an extended generalized role-based access control model (EGRBAC), which integrates the concept of roles associated with both devices and environments. Later, they proposed a dynamic, fine-grained access control model for Home-IoT based on an attribute called HABAC [43]. They also provided strategies to convert a HABAC specification to EGRBAC and vice versa.

Liu et al. [44] introduced an access control framework designed for resource sharing in Manufacturing Internet of Things (MIoT), utilizing RBAC principles. This model aimed to facilitate authorization across services, organizations, and regions, optimizing authorization routes to minimize permission dissemination for incoming requests. Yavari et al. [45] presented a role-based data obfuscation method, which is lightweight and easily scalable for various IoT applications. This technique employs digital watermarking to allow authorized users to reverse the obfuscation applied to the data. Scalability is improved by restricting access according to roles and managing the collection of IoT device data through server authorization. In another work presented in [46], an access control model is deployed based on roles to secure e-health IoT data.

4.3.3. Attribute-Based Access Control (ABAC)

Classic access control models like MAC, DAC, and RBAC, which are tailored for closed environments, rely on user identity when requesting permissions to perform actions (such as writing) on objects (like files). This can occur either directly or via predetermined attribute categories like roles or groups associated with the user. However, it has been reported that these models are not adapted and rather cumbersome to manage in computing environments like IoT, where there is a requirement to assign capabilities directly to users, their roles, or groups. Moreover, the identity, roles, and group qualifiers used by requesters often fall short in accurately expressing real-world access control policies [47]. Addressing this issue, attribute-based access control (ABAC) has emerged as a proposed alternative.

In ABAC, the authorization for subject requests to execute operations on objects is determined by considering the attributes assigned to the user, attributes assigned to the object, environmental conditions that are globally acknowledged and pertinent to the policies, along with a defined set of policies formulated in terms of these attributes and

conditions [48]. Hemdi et al. [49] utilized a cloud server to enforce certain ABAC policies and authenticated access requests via the server. Das and Namasudra [50] introduced a ciphertext policy attribute-based encryption method leveraging elliptic curve cryptography to achieve precise access control over data or resources of IoT devices within healthcare systems. They alleviated the computational overhead on end users by delegating the decryption process to a data user assistant. Arfaoui et al. [51] devised a dynamic context-aware attribute-based access control, referred to as CAABAC, that integrates contextual details with the ciphertext–policy attribute-based encryption to guarantee data security and provide flexible contextual privacy. Ray et al. [52] proposed an ABAC-based healthcare plane (H-plane) model which utilizes the NIST Next-Generation Access Control (NGAC) framework to manage access policies. Salonikias et al. [53] presented a decentralized access control system leveraging identities as well as attributes for Intelligent Transport System (ITS) scenarios in fog-enabled architecture.

Gupta et al. [54] introduced ITS-ABACG, an authorization model based on ABAC to facilitate geographically targeted and time-sensitive notifications for cloud-supported industrial smart vehicles and the Internet of Vehicles (IoV). Specifically, the authors defined various attributes to create separate groups and allocated them into different smart units. Salonikias et al. [55] proposed another deployment for ABAC in one of the most challenging and diverse Industrial IoT (IIoT) systems. Particularly, the model devised a three-layered approach comprising an object layer, an application layer, and a middle-layer, which encompassed both virtual and cloud service layers. Alnefaie et al. [56] introduced a decentralized framework for healthcare, integrating the ABAC model and fog edge scheme to distribute authorization functions among sensors, fog, and cloud layers. The approach escalated availability, decreased latency, and minimized the cloud server overhead. Bhatt et al. [57] proposed ABAC-CC, an access control and communication control model for defining policies based on attributes of entities and ensuring secure data flow in the Cloud-enabled IoT (CE-IoT) architecture. Aghili et al. [58] proposed MLS-ABAC, a modified attribute-based model that includes multi-level security leveraging both static and dynamic user attributes. In this scheme, users have to utilize both attribute and access tokens to fulfill the security level as well as specific policies for granting access inside the system. Recently, two access control models have been proposed in the healthcare and agriculture domains [59,60]. In [59], the authors utilized ciphertext policy attribute-based signcryption for protecting electronic health records, whereas in [60], a metaheuristic optimization technique (Chimp Optimization) was applied to improve the elliptical curve cryptosystem model for authorizing and monitoring file access to the legitimate users.

4.3.4. Capability-Based Access Control (CapBAC)

In the CapBAC scheme, an owner of a device issues a capability token, i.e., a set of access rights, to a subject. Only the subject holding the capability token is allowed to manipulate the device. Mahalle et al. [61] presented IACAC, an access control model integrating CapBAC and identity authentication schemes. Anggorojati et al. [62] introduced CCAAC, an authorization framework utilizing identities, capabilities, and dynamic contextual information for federated IoT networks. The prime focus of this work was to offer a secure way to delegate authority with resilience to the highly decentralized environments. Xu et al. [63] introduced a FedCAC model in wide-ranging fog-assisted IoT environments. Specifically, the framework included a federated capability mechanism based on propagation trees to manage the distribution of access permissions and identity-dependent capability token management, facilitating register, circulation, and invalidate access authorization. Ahamed et al. [64] enhanced the access control model introduced in [62] by adding trust values, collected from social relations, in capability tokens for authentication in a

healthcare IoT system. The approach outperformed RBAC with respect to the computing time, especially round-trip time. Hussein et al. [65] proposed a capability-based model, where access privileges are determined according to the community standards considering the resources availability within decentralized IoT domains. Specifically, the focus was on managing access within IoT communities that share common goals like hosting guests in a smart home, coordinating activities in the kitchen, etc. Nakamura et al. [66] presented a capability-dependent framework leveraging information flow in IoT sensors, actuators, and hybrid devices. A significant feature of the work is the implementation of a time-based operation interruption (OI) protocol to prevent both illegal and late information flows, addressing limitations present in the traditional CapBAC model.

Hernández-Ramos et al. [67] proposed a decentralized capability-driven approach that enabled certification and authorization to be performed without relying on intermediary entities to implement access control logic. Gusmeroli et al. [68] also developed a model where access control is managed through capabilities, especially tokens that dynamically grant specific access rights to entities in the constantly evolving IoT environment. Ramos et al. [69] introduced a DCapBAC model which allows devices with limited computational and memory resources to perform authorization by customizing communication technologies and data interchange formats, which enhances the efficiency and speed of communication between the IoT devices.

4.3.5. Usage Control Model (UCON)

UCON was introduced as a framework aimed at safeguarding digital assets encompassed by digital rights management (DRM), which integrated authorizations, obligations, and conditions [70]. In 2011, Zhang and Gong [71] suggested an abstraction for the UCON model designed to tackle the complexities of the dynamic and dispersed environment of IoT, prioritizing adaptability, and diversity. Additionally, they presented access control policies and procedures to strengthen security and authorization mechanisms. However, this model is not practical since no detail on the implementation of the monitoring process was stated. Recently, Hariri et al. [72] introduced an enhanced version of existing UCON models, called UCON+, which offers some improvements in scalability, performance, and modularity metrics. Specifically, UCON+ incorporates continuous monitoring prior to authorization grant and after authorization revocation, along with policy administration and delegation functionalities.

4.3.6. Organizational-Based Access Control (OrBAC)

OrBAC extends the RBAC model by introducing an additional aspect known as "organization" [73]. Similar to its predecessor, it is deemed inappropriate for heterogeneous and dynamic IoT environments. Later, Pasquier et al. [74] introduced SmartOrBAC, an authorization access framework that is built upon the OrBAC model, refining it to suit IoT environments. In particular, the model divides the task into distinct functional layers, allocating processing burdens between resource-limited devices and those with more resources. At the same time, it tackles collaboration with an innovative solution.

4.3.7. Trust-Based Access Control (TBAC)

TBAC has two sub-categories as follows:

(a) Fuzzy Trust-based: The notion of trust levels within identity management was used by Mahalle et al. [75] who developed a novel method called Fuzzy Trust-Based Access Control (FTBAC). By assigning fuzzy trust values to access permissions, the authors effectively regulated access in IoT environments. This approach basically employed linguistic variables such as experience, knowledge, and recommendation as inputs.

The proposed method demonstrated promising outcomes on different scales of devices, which makes it well-suited for scalable IoT environments.

(b) Trust-aware: Bernabe et al. [76] introduced TACIoT, which is a flexible access control system designed for IoT environments. Fuzzy logic was used in this, which implements a multi-dimensional approach, and it considers some factors such as quality of service (QoS), reputation, security considerations, and social relationships to calculate trust values associated with IoT devices. Butt et al. [77] proposed a trust mechanism for role-based access control (RBAC) within Electronic Healthcare Systems (EHS). For deployment, the authors considered cloud infrastructure.

4.3.8. Blockchain-Based Access Control

BacS [78] was developed by Shi et al., which is an access control scheme built on blockchain technology specifically designed for distributed IoT environments. In this work, researchers addressed the limitations of conventional centralized access control methods by utilizing the node's account address within the blockchain as its identity for accessing the Domain Management Server (DMS). The permissions were redefined for accessing data from IoT devices and to store them on the blockchain. Abushmmala et al. [79] in their work introduced a secure smart healthcare IoT solution using blockchain technology which employs the RBAC architecture. The authors divided the network into distinct roles, each with specific privileges, and handled authentication and data transfer meticulously. In [80,81], an ABAC scheme was proposed, leveraging blockchain technology to enhance security, simplify management, and ensure the integrity of attribute distribution in IoT systems.

Chen et al. [82] presented a task-attribute-based scheme to strengthen IoT security by dynamically managing access rights via blockchain. Recently, a fine-grained and adaptable access control model named CB2FAC, leveraging capabilities and blockchain, was introduced in [83], where new capability authorization rules were defined and an authorization tree was designed alongside a capability revocation list (CRL) aiming to address the requirements for flexibility and promptness in capability revocation. Liu et al. [84] introduced a token-based access control model called TBAC which combined blockchain, Trusted Execution Environment (TEE) technologies, and tokoins (adding "token" to "coin" for digitalized and transferable access rights) to establish a reliable and protected access control framework for IoT. Pathak et al. [85] introduced TABI, which leverages edge computing technology to avoid the problems associated with direct blockchain implementation on IoT networks. Specifically, it integrates trust evaluation mechanisms, implemented as a trust calculation contract (TCC) on edge devices using Hyperledger Composer, and an ABAC scheme deployed on the Hyperledger blockchain through smart contracts, to address malicious IoT users and devices.

In [86], a Trust and Reputation System (TRS) was created for IoT access control utilizing blockchain technology. The authors' model continuously assessed and computed trust and reputation scores for each node involved, enabling a self-adjusting access control mechanism. Additionally, they integrated trust and reputation directly into the ABAC framework, allowing different nodes to receive different access permissions, resulting in adaptive access control policies. Sabrina [87] devised an access control model based on structural relationships (SRBAC) that employed smart contracts and public blockchain technology. This model grants resource access rights to users while ensuring that the resource owner retains complete control. Ouaddah et al. [88] introduced FairAccess, a completely decentralized access control model that ensures pseudonymity and privacy. This model allows users to own and manage their data, using blockchain-based cryptocurrencies like Bitcoin to grant, obtain, delegate, and revoke access rights. Figure 8 illustrates the overall

architecture of FairAccess, working among different autonomous organizations. In this model, every user, whether a resource owner (RO) or requester, utilizes a "wallet" to store their credentials and transactions. Typically, this wallet functions as an authorization manager point (AMP), allowing users to register their resources and set access control policies. The primary roles of the blockchain are to store all access control policies and handle auditing functions, working as a logging database.

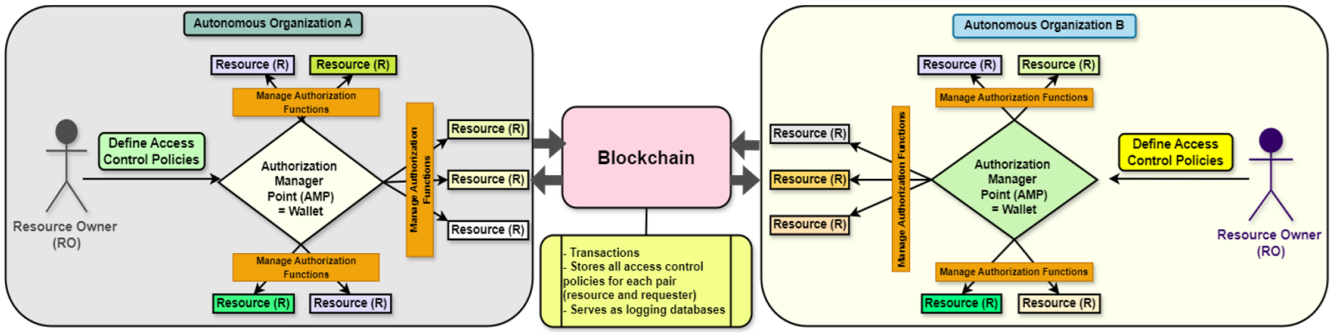

Figure 8. Architecture of FairAccess.

Mesa et al. [89] introduced an approach based on blockchain technology for issuing resource access rights and facilitating their decentralized transfer among users. Zhang et al. [90] suggested a framework based on smart contracts to establish distributed and reliable access control in IoT systems. Specifically, the model comprises several access control contracts (ACCs) for managing access between various subject–object pairs. In addition, it includes a judge contract (JC) for assessing subject misbehavior and a register contract (RC) for overseeing the ACCs and JC. Nonetheless, as the client base grew, the storage expenses escalated, constraining the scalability and adaptability of this method within expansive IoT environments. Xu et al. [91] introduced BlendCAC, a distributed capability-based access control scheme, which was implemented using smart contracts to handle the registration, propagation, and revocation of access authorizations, forming a robust strategy for managing capability tokens based on identity. Again, Liu et al. [92] introduced Fabric-iot, an access control system leveraging the Hyperledger Fabric blockchain framework and ABAC scheme for IoT applications that offers decentralized, detailed, and adaptable access control management. In this system, users are divided into two categories: admin and common user. Admin can add, upgrade, and manage smart contracts, whereas the owner of the device, that is, a common user, can retrieve URL of the resources by requesting (attribute-driven) access to the blockchain through API, followed by pursuing a certificate authority (CA). In the fabric blockchain, all data are kept as a decentralized ledger in <key, value> pairs to form a modifiable "World State", which is composed of two databases: Couch DB and Level DB (see Figure 9). As soon as a device creates a new resource request, a message with the resource URL is sent to the smart gateway. The gateway receives this message and records the URL on the blockchain.

Dukkipati et al. [93] introduced an access control approach utilizing blockchain where blockchain serves as a decentralized access manager to ensure secure data access. Pinno et al. [94] introduced ControlChain, a blockchain-based framework for managing IoT access permissions. ControlChain addressed issues found in both FairAccess and traditional architectures by offering an authorization process that is both distributed and easily observable. Additionally, the model provided a secure method for establishing relationships, allocating attributes, and incorporating them into access control procedures.

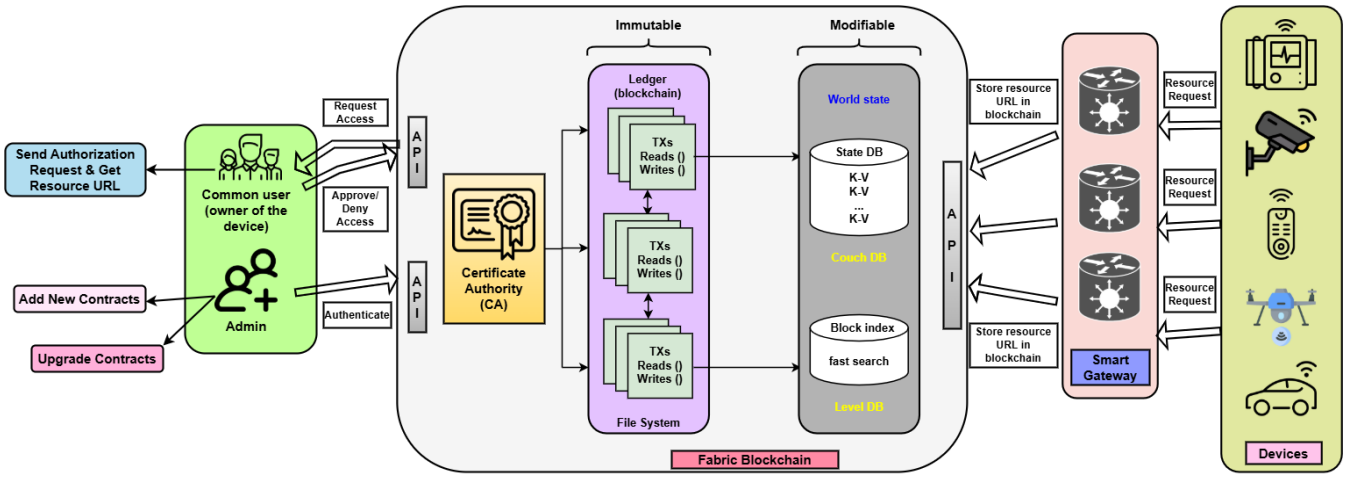

Figure 9. Architecture of Fabric-iot.

Recently, there has been a clear trend of integrating blockchain technology to develop access control schemes [95–103]. For example, Zhonghua et al. [95] leveraged blockchain and edge computing technologies to develop an access control model. Specifically, the authors utilized smart contracts and attributes for faster consensus and data consistency. Since the ABAC model results in high computational overhead, a new access control framework has been proposed by incorporating roles and hyper-ledger blockchain in [99]. Particularly, the entire access control procedure was accomplished by three contracts: a policy contract, a device contract, and an access contract. As a result, the scheme can deal adaptively with the dynamic industrial IoT environment. Velmurugan et al. [101] also used hyper-ledger blockchain technology, but for transferring sensitive records in the healthcare systems. Another interesting work is [103], where the authors focused on safe communication and interaction between the autonomous cars in the decentralized IoV system. Specifically, they leveraged the Ethereum blockchain for secure financial transactions.

Considering this aspect, there could be mainly two types of access control strategies:

(a) Transaction-based: Transactions can authorize, assign, or withdraw access rights. However, the primary drawback of this approach is that access decisions rely on a centralized node. There are a few transaction-based access control models [80,88].

(b) Smart contract-based: Smart contracts have the capability to assess access requests and determine outcomes according to the access policies set by the resource owner. Nevertheless, this method could result in substantial overheads as it entails the generation of contracts among nodes. Most of the access control models that leverage blockchain technology are based on smart contracts [78,79,81–85,88,90–92,94–98].

The summary of Blockchain-based Access Control Models (that we took into consideration) is shown in Table 3.

Table 3. Summary of Blockchain-based Access Control Models in IoT.

Work	Methodology	Key Findings
[78]	Develops BacS, an access control scheme built on blockchain technology specifically designed for distributed IoT environments. Utilizes node's account address within the blockchain as its identity to access the Domain Management Server (DMS). Redefines the permissions for accessing data from IoT devices and stores them on the blockchain. Uses a lightweight symmetric encryption algorithm.	Addresses the limitations of conventional centralized access control methods by accessing DMS through the wallet address. When the number of devices is smaller, BacS performs worse than traditional models. The viability and effectiveness of the model in ensuring security and privacy is verified by experimental models built on an Ethereum private chain.

Table 3. *Cont.*

Work	Methodology	Key Findings
[79]	Proposes a secure smart healthcare IoT solution based on blockchain, employing the RBAC architecture. In particular, the network is divided into distinct roles, each with specific privileges, and handles authentication and data transfer meticulously.	A real-life experiment reveals that an Android app utilizing blockchain technology performs much more safely than the app using the MQTT protocol while maintaining integrity and privacy.
[80]	Introduces an ABAC scheme, leveraging blockchain for documenting attributes' distribution.	Utilization of blockchain technology prevents single-point failure as well as data manipulation. The proposed framework can protect IoT systems from multiple attacks.
[81]	Presents a blockchain-based ABAC model. Blockchain technology is used to record attributes. Additionally, smart contracts are used for storing encrypted data.	Manages access more effectively since access control lists (ACLs) are not needed for individual devices. The scheme decreases computational overhead and time but has unresolved scalability issues.
[82]	Proposes a task-based and attribute-based access control scheme, incorporating blockchain technology for IoT. To prevent data manipulation and authenticate users, the authors use message authentication techniques, such as hash functions and digital signatures.	Addresses the single-point failure problem. Additionally, for specific tasks, the proposed model assigns the least privileges to the users in real-time.
[83]	A novel scheme, called CB2FAC, is developed combining the advantages of the CapBAC model and blockchain technology.	The model includes an authorization tree and a capability revocation list, easing security of both capability revocation and granularity control.
[84]	Introduces TBAC, a token-based access control framework, leveraging blockchain and TEE technology. Devises a cryptographic coin referred to as "Tokoin" that reforms the "virtual" access capabilities to transferable and digital assets.	Gains secure inspection and monitoring of access activities through blockchain and TEE-based trusted access control object (TACO).
[85]	Presents TABI, combining ABAC scheme and trust evaluation mechanisms with blockchain technology to secure Edge-IoT networks.	Results in higher throughput and detection rate, along with lower latency than Fabric-IoT.
[86]	Proposes a self-adjusting access control mechanism through continuous computation of trust and reputation scores. To generate dynamic access control policies, an ABAC framework is integrated with the model.	Manages trust efficiently in decentralized IoT access control and results in minimal processing delays.
[87]	Develops a model based on structural relationships, using smart contracts and blockchain to manage authorization of internal and external users in a smart city.	Demonstrates the trustworthy implication of the framework in a real-world scenario through a smart city use-case by managing access for IoT devices in urban environments.
[88]	Introduces FairAccess, a decentralized authorization model, where users access and manage data using blockchain-based cryptocurrencies like Bitcoin.	Offers a robust and transparent access control solution utilizing the consistency provided by blockchain-enabled cryptocurrencies.
[89]	Proposes a new blockchain-based technique, where access policies and rights are visible to all users through distributed transfer.	Provides distributed auditability that prevents a group from falsely refusing access rights granted by a legally enforceable policy.
[90]	Suggests a model consisting of several access control contracts (ACCs), a judge contract (JC), and a register contract (RC) for managing access between various subject–object pairs, assessing subject misbehavior, and overseeing ACCs and JC.	Guarantees the trustworthiness of a single authorization through execution and verification of ACCs by most participants.
[91]	Presents BlendCAC, a blockchain-integrated scheme based on capability. Utilizing smart contracts, the framework manages capability tokens based on identity.	Incurs significantly less computational overhead (0.74 ms) than traditional RBAC (2.47 ms) and ABAC (2.07 ms) models. Offers expandability since access rights validation relies on capability tokens.
[92]	Devises a hyperledger fabric blockchain-based access control system referred to as fabric-iot combined with an ABAC scheme for IoT applications. To implement the ABAC model, policy management, and device resource management, three smart contracts are designed separately.	Demonstrates high throughput even in environments with a large volume of requests. Maintains the coherence of data by achieving consensus in a distributed system.

Table 3. *Cont.*

Work	Methodology	Key Findings
[93]	Suggests a blockchain-based IoT authorization framework where blockchain operates as the decentralized access manager.	Enhances users' privacy through separating blockchain as public and private. Provides transparency since the current user accessing a resource is visible to all others. Local blockchain databases enable faster processing.
[94]	Proposes a decentralized framework, ControlChain, that utilizes blockchain technology to manage access permissions in IoT. It allocates attributes and integrates them with access control procedures for securely establishing relationships among users, devices, and groups.	Handles unresolved issues in FairAccess and traditional architectures by developing a distributed and easily observable authorization process.
[95]	Presents an attribute and smart contracts-based access control model. Leverages blockchain and edge computing technology	Lesser energy consumption than the traditional PoW unit. Faster consensus convergence and constant time of the policy addition and judgment process.
[96]	Proposes a blockchain-based framework having two phases: adaptive network sharding scheme and multidimensional subjective logic. The first part is based on the network distance, node credibility, and access frequency, whereas the second one replicates the heterogeneity among the edge nodes.	Minimizes storage pressure of the nodes and enhances scalability. Ensures trust and cooperation among the edge nodes.
[97]	Introduces an access control model integrating smart contracts and GTRBAC scheme.	The cost of access control operations rises linearly with proportion to the policy constraints volume.
[98]	Combines blockchain with ciphertext–policy attribute-based encryption technique, especially for healthcare systems.	Lessens the complexity of monitoring remote patients. Reduces complexity of the resource-intensive authentication and blockchain communication.
[99]	Utilizes roles and hyper-ledger blockchain strategies.	Chain-code computation overhead and time overhead notably drops.
[100]	Introduces reputation value as an attributes in an ABAC scheme and integrates it with the blockchain network. In addition, stores resources of IoT in the Inter-Planetary File System (IPFS).	Refined attributes result in minimizing the difficulty of access control management. Provides adaptive access control with high system throughput and low time delay.
[101]	Uses hyper-ledger blockchain technology for transferring sensitive records in the healthcare systems. Devises modified key policy attribute-based encryption technique.	Allows secure electronic health record transfer between professionals with protecting patients' privacy and reduces the likelihood of mistakes.
[102]	Integrates blockchain to expand the ABAC scheme in the IoT-based medical systems. Utilizes mobile agents for mutual and anonymous authentication process.	Efficient in regards of communication, computation, and storage costs.
[103]	Leverages the Ethereum blockchain for the interaction among the cars in the decentralized IoV system.	Ensures secure financial transactions and safe interaction between the autonomous cars.

4.3.9. Protocol-Based Access Control (ProBAC)

The ProBAC model represents a tailored set of protocols chosen for IoT access control to meet specific access control requirements [19,22]. Pereira et al. [104] introduced a service-level authorization strategy based on a constrained application protocol (CoAP) aimed at lightweight IoT devices. They contended that their framework resolved the challenge of fine-grained access control, which was not achievable with other connection control systems such as DTLS and IPsec. Authentication of Things (AoT), a collection of cryptographic protocols, was presented in [105] by integrating identity-based and attribute-based cryptography alongside the ABAC scheme to deliver robust authentication and adaptable access control throughout the entirety of the IoT product life cycle. Sciancalepore et al. [106]

proposed OAuth-IoT, a versatile authentication and authorization framework designed to provide secure authorization for HTTPS using the widely adopted OAuth protocol.

In another paper [107], Cirani et al. introduced IoT-OAS architecture, utilizing OAuth-based service authorization. Their sole focus was on integrating HTTP/CoAP services into an authorization framework that incorporated OAuth-based authorization services (OAS). Similar to [107], Wu et al. [108] presented an access control framework designed for smart home using CoAP and explored its incorporation with HTTP to enhance the adaptability of current web-based services. To protect extremely sensitive physiological data from possible threats and adversaries, Kumar and Gandhi [109] presented a framework for authentication and authorization using smart gateways, integrating DTLS and CoAP authentication mechanisms. Later, in [110], an IoT access control approach was devised by integrating IoT devices with web-based services, treating specific IoT communication elements like MQTT as resources. Specifically, the primary aim of the research was to establish a cohesive access control system across diverse IoT devices. After that, a universal access control enforcement system was designed by Colombo and Ferrari [111] using MQTT. Specifically, this system integrated ABAC to govern message transmission according to user preferences, employing corresponding access control techniques.

4.3.10. Relationship-Based Access Control (ReBAC)

User-to-user, user-to-device, and device-to-device relationships are recognized as a potential identity and access management system for the IoT [112]. Relationship-based Access Control (ReBAC) allows the inclusion of user relationships in determining access control choices and facilitates customized policy implementation. Arora et al. [113] introduced a higher-order relationship-based access control model referred to as HO(T)-ReBAC where authorization decisions were taken based on the history of relationship changes. Later, Praharaj et al. [114] proposed ReBACIoT, a comprehensive and adaptable access control framework tailored for socially integrated smart IoT systems. Notably, the model incorporated social relationships among users in addition to attributes.

4.3.11. Risk-Based Access Control

The risk-based access control model employs security risk levels to determine whether access requests should be granted or denied. In the realm of access control, security risk refers to the potential for information exposure and subsequent harm that may arise from system access [115]. Atlam et al. authored a series of papers [116–118] focusing on risk for developing access control models for IoT systems, which also included a literature review [119]. Recently, they proposed a neuro-fuzzy system model aimed at evaluating the security risk level linked with each access request across diverse Internet of Things applications [120]. Jiang et al. [121] presented RQ-UCON, integrating risk quantification and a UCON scheme to safeguard the privacy of healthcare big data. This model involved quantifying, updating, and computing risk values for doctors by analyzing their past access behaviors and real-time access patterns. Subsequently, doctors were granted access based on the alignment of their risk assessment with the operational risk parameters.

4.3.12. Temporal- and Spatio-Temporal-Based (T&ST-Based) Control

Conventional access control models do not consider environmental factors when making access decisions, which may render them unsuitable for IoT environments. Guo et al. [122] introduced DABAC, a spatio-temporal domain access control framework based on smart contracts. The system included domain elements to enforce physical location restrictions on dynamic IoT devices, offering enhanced control by integrating spatial and temporal data for more flexibility and precision. Again, STRAC was introduced [123], which integrated space, time, and reputation to manage access to information within the

sensing layer of the IoT. The authors in this approach adopted a lattice-based method to reduce the complexity of policy bases, utilized nondeterministic and stochastic authorizations to enhance communication reliability, and introduced two update mechanisms based on attributes and election to adjust node reputations. Lee et al. [124] proposed LTAC, an access control system that integrated location, time, and security levels to regulate object access within the IoT sensing layer. In particular, their focus was on resolving the challenge of determining the timing and location for granting access requests, as well as defining authorized users. Additionally, they employed the concept of an access lattice to reduce the complexity of the policy base. Similarly, Abdunabi et al. [125] introduced an STABAC model, which incorporated environmental attributes like location and time, to govern access decisions for healthcare information systems in such networks that often generate sensitive data collected by IoT devices.

4.3.13. Hybrid Access Control (HyBAC)

Attia et al. [126] proposed a hybrid AC model using ABAC and RBAC and claimed that the model simplified the expression of detailed security policies for systems without causing an increase in the number of roles or rules within the security policy. Particularly, the framework takes into account the users, resources, and environmental attributes to make access control decisions. In one part, the active role of the specific user is extracted, followed by the second part (executing simultaneously) where the type of the resource, whether shared or private, is obtained. Based on a predefined set of rules and access mode requested by the user, a few unique as well as shared rules are produced and evaluated to decide whether the authorization should be approved or rejected. Figure 10 shows the hybrid access control mechanism as a whole.

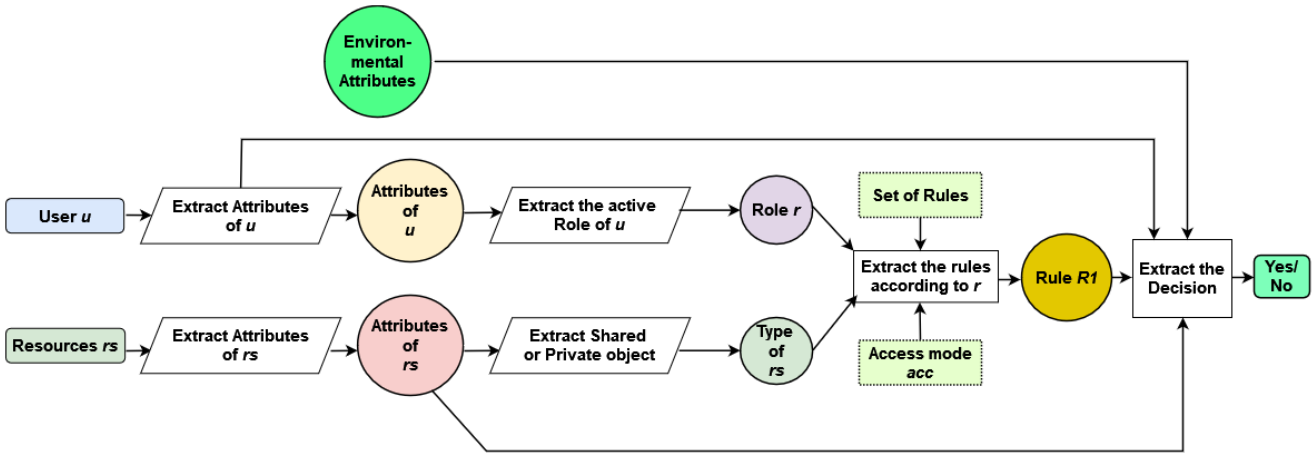

Figure 10. Workflow of a hybrid AC model using ABAC and RBAC (the arrows in this figure represent the normal directional flows).

In [127], PerBAC was proposed for tailoring the pervasive and dynamic nature of IoT environments. Particularly, the model integrates ABAC and OrBAC to offer robust, context-aware, and scalable access control. In 2020, Thakare et al. [128] developed a model based on priority and attribute called PAR-BAC which was designed for a considerably expansive medical context within the Azure IoT cloud. Aftab et al. [129] combined the features of traditional RBAC and ABAC models to address the secure localization of IoT-enabled smart vehicles. They employed a dynamic Conflict of Interest (COI) alongside their proposed HAC model to mitigate overload and latency issues in access control. Ameer et al. [130] proposed two hybrid models, HyBACRC and HyBACAC, which merged the benefits of

ABAC and RBAC. These models adopted role-focused and attribute-focused strategy in their development, respectively.

Other hybrid models are proximity-based and ABAC [131], attribute and role-based (ARBHAC) [132], trust and attribute-based (T-ABAC) [133], and policy-based [134].

The summary of Hybrid Access Control Models in IoT is presented in Table 4.

Table 4. Summary of Hybrid Access Control Models in IoT.

Work	Methodology	Key Findings
[126]	RBAC + ABAC	Complexity reduction in security policies Enables the precise specification of system details, keeping the volume of rules or roles unchanged in the policies.
[127]	ABAC + RBAC + OrBAC	Enables optimal authorization decisions based on adaptive rules and entities. Supports decentralized architecture where users gain advantages from various organizations using contractual agreements. Particularly, the model achieves this through the cooperation of access control layers across multiple organizations.
[128]	Priority + ABAC + RBAC	Resolves the handling inefficiency in large dynamic organizations, where similar resources are requested at a time by multiple users. Assists each user in uniform implementation of policies by accessing resources rights to multiple users through integrating priorities, attributes, and roles.
[129]	RBAC + ABAC	Contributes to the localization of IoT as well as Satellite-based vehicles. Reduces administrative burdens, increases adaptive behaviors, and improves security.
[130]	RBAC + ABAC	Combines the advantages of EGRBAC and HABAC model features to deploy hybrid models with similar expressiveness power. The proposed models support not only static attributes but also dynamic attributes that make them more suitable for controlling access to IoT environment.
[131]	Proximity-based + ABAC	Supports more appropriate policy specifications to control access as well as filter information in Intelligent Transportation System (ITS) and Location-Based Services (LBS). Enables policy definitions and enforcement according to application domain contexts.
[132]	ABAC + RBAC	Reduces the complexity of RBAC and ABAC schemes for assigning permissions and managing policies. Demonstrates the viability of the proposed model through an example of WeChat.
[133]	TBAC + ABAC	Allows authorization of multiple static attributes. To enhance security, it takes into account the dynamic trust attributes of users. Specifically, if the behavior of a user causes any change in his trust level, the model adjusts the user's permissions to the system accordingly.
[134]	ABAC + RBAC + CapBAC	Notable reduction in the volume of policy specifications. Results in negligible amount of extra overhead compared to other standard CapBAC models.

4.3.14. Machine Learning-Based Access Control

Outchakoucht et al. [135] proposed a comprehensive machine learning-driven framework for IoT access control. They introduced the concept of an organizational notion, significantly mitigating the issue of role explosion, a primary challenge faced by RBAC and ABAC schemes. In a later paper, Outchakoucht et al. [136] leveraged blockchain technology and reinforcement learning to achieve both distribution and dynamic optimization of security policies, ensuring adaptability and self-adjustment. Zhao et al. [137] proposed a PMML scheme, a method for access control policy maintenance in IoT systems based on machine learning modules. Specifically, it comprised automated Policy Generalization (PG) and Policy Evaluation (PE) modules for post-deployment rule set maintenance. In addition, it incorporated a new measurement concept called resource similarity and quantitative rule assessment to enhance policy mining and ensure high-quality rule sets.

Liu et al. [138] introduced EPDE-ML, a machine learning-based approach for access control permission decisions. This scheme translated ABAC requests into permission decision vectors, reframing the access control problem as a binary classification task. As a result, the operation of the system remained independent of policy scale or entity count. Again, Usman et al. [139] proposed an automated hybrid access control system for the supervisory control and data acquisition (SCADA)-enabled IIoT. Particularly, they utilized a refined artificial neural network (ANN) and extreme learning machines to determine user access rights to resources and guarantee privacy and security. By leveraging advanced machine learning techniques, it addresses the complexities of role engineering in IIoT setups. Likewise, Zhou et al. [140] also leveraged machine learning, specifically Adaboost and Support Vector Machines to accomplish similar purposes. Bhansali and Hiran [141] utilized hashing and signature to the classic context policy attribute-based encryption technique and leveraged a federated learning approach to ensure a secure data access for the IoMT.

A summary of the studied ML-based Access Control Models in IoT is presented in Table 5.

Table 5. Summary of ML-based Access Control Models in IoT.

Work	Methodology	Key Findings
[135]	Introduces a multiple-layer authorization framework incorporating ML and OrBAC techniques. Notably, rather than relying on any specific learning approach, the model varies algorithms based on the hardware resources of the system. But in most of the scenarios, reinforcement learning (RL) and resource-intensive supervised learning (SL) are used considering the diversity and complexity of the IoT environment.	Mitigates a major drawback of RBAC and ABAC schemes, the role explosion problem, by integrating organization notion with comprehensive machine learning approaches.
[136]	Leverages reinforcement learning and blockchain technology.	Achieves not only distribution of the security policies but also optimization, dynamicity, and self-adjustability of these policies.
[137]	Proposes an ML-based scheme called PMML for the maintenance of the authorization policies in IoT. In particular, the model comprises of two modules: automated Policy Generalization (PG) and Policy Evaluation (PE).	The PG module enhances policy mining and the PE module ensures high-quality policy rule sets. Consequently, the model becomes qualitatively and quantitatively effective.
[138]	Introduces EPDE-ML, an ML-based engine for access control permission decisions, specifically using the random forest algorithm.	The decision time tends to be unchanged as the number of policies or entity volume increases, provided that the attribute category is stable. Results in better comprehensive permission decisions while comparing with different methods, such as lightgbm, logistic regression (LR), k-nearest neighbor (KNN), support vector machine (SVM), and decision tree (DT).
[139]	Determines user access rights to resources by utilizing a feedforward neural network (multilayer perception) and an extreme learning machine (ELM).	Addresses the complexities of role engineering, particularly in the IIoT setups, by leveraging advanced machine learning techniques.
[140]	Utilizes Adaboost and Support Vector Machine techniques.	Automation of the role assignment process.
[141]	Includes hashing and signature to the classic context policy attribute-based encryption technique. Leverages federated learning approach to ensure a secure data access for the IoMT.	Protects the privacy, confidentiality, and integrity of healthcare documents hosted on a cloud server.

4.3.15. Deep Learning-Based Access Control

Nobi et al. [142] introduced DLBAC, a DL-based access control system that bypasses the need for attribute or role engineering, policy formulation, and similar tasks by utilizing an end-to-end method that directly processes user and resource metadata. In addition, this approach addresses prior concerns regarding the lack of transparency in neural network-based access control systems [143]. Specifically, the model generates a decision engine to extract these metadata and convert them into a binary format, and a trained neural network

uses the transformed metadata to make access control outcomes. The entire working process of DLBAC is depicted in Figure 11.

Thilagam et al. [144] introduced a deep learning-driven system for access control and data analytics aimed at securing IoT healthcare environments. Particularly, this access control model makes use of social graphs to differentiate between legitimate and malicious users and employes a Convolutional Neural Network (CNN) to grant user-specific authorizations. Furthermore, it incorporates a deep reinforcement learning (DRL) approach and a federated learning (FL) framework to monitor access control limits, thereby safeguarding patient privacy and maintaining the integrity of medical data. Lin et al. [145] introduced a secure access control system which they term as SACM, which is tailored for IoT healthcare based on attributes, incorporating federated deep learning (FDL). Graph convolutional networks are used to analyze the social graph, unveiling the correlation between users' social characteristics and their trust levels. Again, Singh et al. [146] introduced a secure framework to safeguard privacy in smart healthcare scenario by integrating blockchain and federated learning (FL) technologies. A blockchain-powered IoT cloud platform is used for building this framework with a goal to enhance both security and privacy.

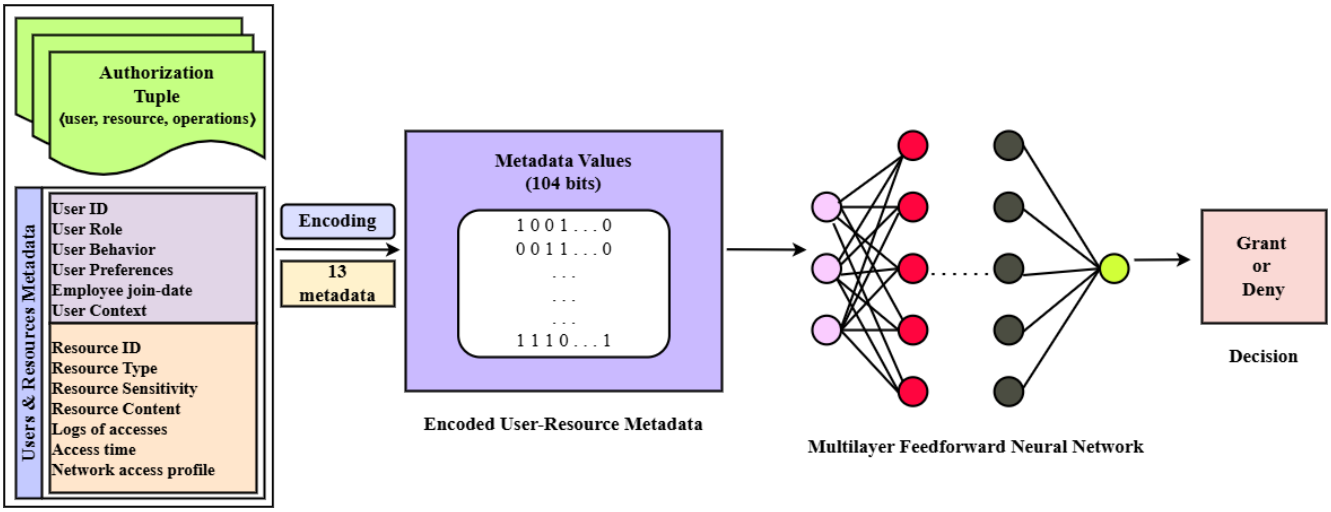

Figure 11. Architecture of DLBAC.

Identity-based encryption is used to regulate access to smart vehicles in work by Zhou et al. [147]. DL methodologies are used in this work to block potentially harmful data packets. Yu et al. [148] in their work introduced an approach for access control for edge computing devices within an IoT framework. DL techniques are used in this work as well. The authors also devised a unique edge-computing network structure for supporting this strategy which dynamically assigns resources for specific services taking into account current demands. A DLACB access control system was proposed by Akbarfam et al. [149] which merges DL with blockchain technology. This framework is integrated into a DL model coupled with prioritization rules to intelligently allocate user permissions for various types of resources. Here, blockchain is employed for administering access control policies and facilitating data retrieval processes. Xu et al. [150] in their work introduced another access control approach which is rooted in Multi-Access Edge Computing (MEC) in order to optimize system efficiency in an eco-friendly IoT environment.

An authorization system leveraging DL technique was proposed by Rahman et al. [151], who implemented it on the Hyperledger fabric private blockchain. Particularly, smart contracts are used to define the ABAC policies, with the ANN model enhancing these policies to accurately detect and segregate harmful anomalies, thereby thwarting unauthorized access from malicious devices. Liu et al. [152] proposed an innovative access control

framework, named RPBAC, which utilizes risk prediction to dynamically allocate access privileges to a node. Specifically, this is a three-tiered model, comprising a behavior feature selection module, followed by a risk prediction module, ending with an access rights decision module. Behavior features are selected as sequences to pass as inputs in a four-layered neural network (according to Figure 12, the input layer, the first hidden layer, the second hidden layer, and the output layer are represented by pink, blue, red, and yellow colors, respectively). To address the challenge of insufficient training dataset, an enhanced Generative Adversarial Network (GAN) called WCGAN is presented within the risk prediction component, leveraging Long Short-Term Memory (LSTM) as a generator and a CNN as a discriminator to address the challenge of insufficient training datasets (see Figure 12). Finally, the last module decides the access rights based on a pre-established strategy.

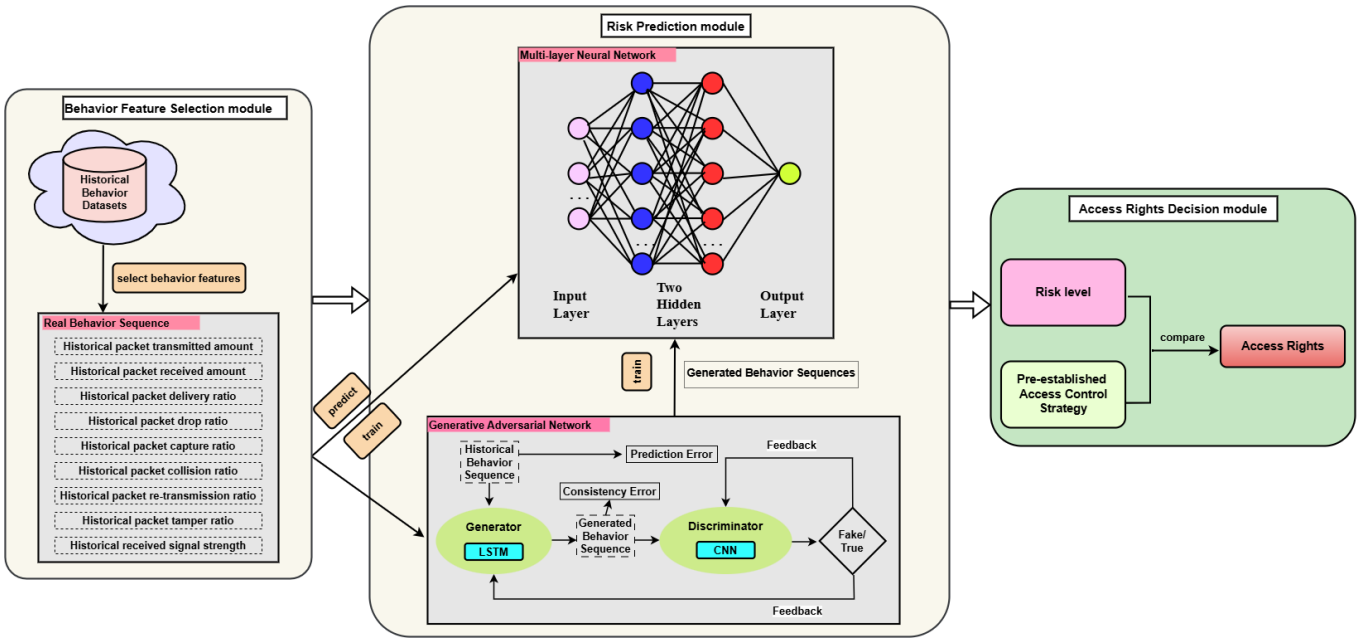

Figure 12. Architecture of RPBAC. The arrows represent the normal directional flows.

Chu et al. [153] introduced a novel approach to multi-access control in IoT systems, integrating battery prediction alongside energy harvesting and harnessing the capabilities of reinforcement learning. Their method employed a two-tier LSTM network: the initial layer forecasted and generated the sensor node's battery status while the subsequent layer incorporated channel data and predictions to formulate access control strategies. Heaps et al. [154] developed an automated transformer-based deep learning approach to generate access control details from a collection of user narratives outlining the software product's functionalities. By leveraging agile software development principles, the authors automated policy specification, which encompasses actors, data entities, and their operational interconnections using the iterative integration of user narratives in system development. Table 6 summarizes the DL-based access control models in IoT.

Table 6. Summary of DL-based Access Control Models in IoT.

Work	Methodology	Key Findings
[142]	Introduces DLBAC, which eliminates attribute or role engineering required in typical access control models. Generates a decision engine to extract users and resources metadata, as well as a trained neural network to transform these metadata to make access control outcomes.	Addresses the lack of transparency issues in prior neural network-based access control systems. Outperforms EPDE-ML[138], meaning that DL-based policy mining techniques show more accuracy in decision making as well as exhibit higher generalization than traditional ML ones.
[144]	Utilizes social graphs for differentiating authorized and unauthorized users. Leverages a CNN model to allow user-specific authorizations. Integrates a deep RL and a federated learning framework to monitor access control limits.	Experimental evaluation demonstrates that the model ensures effective preservation of patients' privacy and high integrity of medical data. Achieves 95% precision, recall, and f1-score, along with 98% accuracy when the number of users increases.
[145]	Proposes an FDL and attribute-based access control model called SACM. To analyze the social graphs and unveil the correlation between users' social characteristics and trust levels, graph convolutional networks are designed.	Results in high privacy and data integrity in IoT healthcare systems.
[146]	Leverages blockchain and federated learning technologies to enhance both security and privacy measures.	Enhances the robustness and resilience of the system since the framework facilitates decentralized data management through the integration of DL and blockchain. Reduces latency and increases generalizability for various smart healthcare applications.
[147]	Combines identity-based encryption with deep learning methodologies for not only controlling access but also blocking harmful data packets in smart vehicular systems.	The system exhibits 99.72% accuracy in detecting malicious packets.
[148]	Employs deep reinforcement learning techniques for edge computing devices within an IoT framework.	Dynamically and flexibly assigns resources for specific services. Demonstrates viability as well as more efficient use of resources under constrained conditions.
[149]	Presents DLCAB, a merged model of deep learning and blockchain. On the one hand, the model assigns permission to resources by integrating the deep learning model coupled with prioritization rules. On the other hand, it uses blockchain to administer access control policies and facilitate data retrieval processes.	DLBAC keeps consistent in processing time even with an excessive number of requests. Offers not only automatic access control but also improved security through blocking data breaches.
[150]	Introduces a deep convolutional network for optimizing authorization in energy harvesting IoT devices. Specifically, an LSTM is designed for predicting energy level at these devices.	The model improves system efficiency through a convenient training strategy and an appropriate reward technique.
[151]	Devises a model deployed on the Hyperledger fabric private blockchain, which utilizes smart contracts to define ABAC policies and an ANN model to create a dynamic and robust access control system.	DL enables the system to make decisions intelligently and adaptively, thus detecting and segregating harmful anomalies accurately with blockage of unauthorized access from malicious devices. It automates the access control policies with the help of the Hyperledger fabric blockchain.
[152]	Presents RPBAC, employing risk prediction to dynamically allocate access privileges to a node. Additionally, it introduces extended GAN (WCGAN) within the risk prediction component, utilizing an LSTM as generator and a CNN as discriminator to address the challenge of insufficient training datasets.	The proposed WCGAN converges faster than traditional GAN. Improves the performance of the NN while using WCGAN-generated datasets. RPBAC achieves significantly higher (87%) efficiency compared to RBAC (72%) and ABAC (75%), although it takes slightly more time.
[153]	Develops a reinforcement learning-based multi-access control approach, leveraging a two-tier LSTM network where one layer predicts battery status followed by another layer that defines access control strategies.	The proposed deep LSTM network minimizes the aggregated battery prediction loss and maximizes long-term discounted sum rate of partial users.
[154]	Introduces an automated transformer-based deep learning approach to generate access control details from a collection of user narratives outlining the software product's functionalities.	Enhances accuracy and consistency in policy generation, hence minimizing the risk of overlooking critical access controls, resulting in secure software systems.

4.3.16. Other AC Models

Gupta et al. [155] devised a structured model called GCP-IoTAC enhancing access control within Google Cloud Platform (GCP), aiming to enhance access control for IoT applications. Their proposal included extensions based on attributes to enable more precise access regulation within GCP and its IoT infrastructure. Tandon et al. [156] presented HCAP, a capability system rooted in historical data, building upon the identity-based capability system (ICAP) [157] aiming to enforce permission sequencing constraints through security automata (SA) within a distributed authorization setup tailored for IoT devices.

SENSEI [158] was a large-scale project which offered an access control model based on billing (BBAC) and privilege (PBAC) [14]. In BBAC, access control decisions are determined by the business model, prioritizing rewards over user identity, allowing services to be granted to anyone who offers sufficient compensation. In contrast, PBAC operates based on organizational policies, valuing user identity and considering the inherent security sensitivity of the service to the involved organization(s), ensuring access is restricted to specific users. Karimibiuki et al. [159] proposed a dynamic policy-driven system called DynPolAC to protect information within IoT settings. Their approach involves creating a new language for access control policies and building an access control engine comprising a rule parser and a checker. This engine operates dynamically, continually processing and updating policies in real time with the goal of reducing service interruptions.

In [160], a new framework for home gateways was introduced, allowing seamless integration of diverse IoT devices, protocols, and services from various vendors. Alongside this, a novel access control system tailored for specific smart home situations was developed. Rivera et al. [161] suggested utilizing User-Managed Access (UMA) to establish a cohesive access control framework that can accommodate various entities in a hybrid setup comprising IoT devices and intelligent agents, regardless of their individual characteristics. Uddin et al. [162] proposed AW-TRBAC, an innovative framework that improves upon RBAC by dynamically assigning access privileges to users and ensuring access governance. The scheme is built on the concept of dynamic segregation of duties (SoD) and process workflows, emphasizing task-specific limitations for role restrictions, access governance, and logging. Omolola et al. [163] designed a novel authorization technique based on policies for IoT and smart city environments. Specifically, they utilized the concept of trust policies and delegations adjusted from the LIGHTest project, resulting in a flexible, simple, and fine-grained access control mechanism for dynamic and heterogeneous IoT devices. Table 7 depicts the other Access Control (AC) models in this research area. lists different access control models in IoT based on their sources. Recently, a signature-based authorization scheme, SBAC-FC, has been proposed for fog computing-enabled big data applications. This scheme was tested under various ML models to estimate the cardiac arrhythmia in patients, resulteing in around 72%∼83% accuracy.

Table 7. Other Access Control Models in IoT at a glance.

Work	Methodology	Key Findings
[155]	Proposes GCP-IoTAC, which includes ABAC enhancements to enable more precise access regulation within GCP and its IoT platform. Particularly, the authors employ dynamic roles, attribute-oriented, and role-oriented approaches while implementing attribute-based extensions.	Experimental results disclose a role-centric strategy offer most suitable for detailed access control within GCP.
[156]	Develops a historical data-dependent capability-based system (HCAP) to necessitate access control policy constraints.	Prevents replay attacks and guarantees resiliency to untrustworthy user actions.
[159]	Presents an adaptive policy-driven system named DynPolAC deploying an access control engine with a new language for processing and updating access control policies.	Shows faster responses and more sensibility than eXtensible Access Control Markup Language (XACML)-based methods. Consequently, it reduces service interruptions.
[160]	Employs a hybrid method integrating the OSGi User Admin service with XACML.	Offers consistent and resilient authorization that minimizes vulnerabilities typically associated with diverse IoT devices.

Table 7. *Cont.*

Work	Methodology	Key Findings
[161]	Introduces an UMA-based unified access control in a hybrid setup of IoT devices and intelligent agents.	Provides flexibility to regulate access control policies regardless of the individual characteristics of different entities. As a result, managing various permissions and roles during the decision-making process for negotiating agents becomes more straightforward.
[162]	Proposes a task and workflow-based framework extending the RBAC scheme called AW-TRBAC.	The dynamic access privilege assignments, SoD, and administration make AW-TRBAC not only expandable but also manageable to crucial risks in web applications while handling highly complicated requests. Imposes policies on data storage by generating task instances with designated events and actions to address the risk of inadequate logging and monitoring.
[163]	Leverages the concept of trust policies to design a novel authorization technique.	Provides both fine-grained and simplified access control management through centralized specification and enforcement of policies across diverse IoT devices and applications.

4.4. RQ4: What Are the Recent Trends of Access Control Models and Their IoT Application Domains?

In this subsection, we investigate the researchers' tendencies while developing access control framework for the IoT system. According to our study from RQ2, we find that the state-of-the-art models, especially blockchain-based and deep learning-based authorization schemes, are widely leveraged for IoT. Interestingly, the significance of the attribute-based traditional scheme, ABAC, has not faded yet. To observe the specific pattern of employing these techniques, we draw a plot in Figure 13. The figure demonstrates the number of publications (solid lines) as well as the trends (dashed lines) of these three access control models in the last few years. Though we see a linear increasing shift in all three cases, the rise of the blockchain's dashed line is much higher than that of deep learning and ABAC. In addition, it can be seen that blockchain technology has been utilized remarkably in the last two years (2023 and 2024). Moreover, we observe a tendency of preferring deep learning-based models over the conventional attribute-based models.

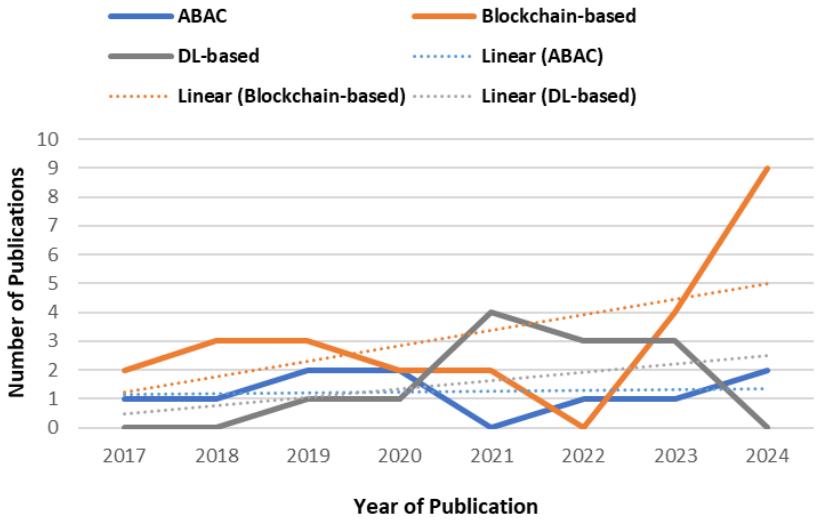

Figure 13. Year-wise publications and recent trends of the widely used ABAC, blockchain-based, and DL-based access control models in IoT.

We analyze the proportion of the existing authorization schemes considering various IoT application domains. Interestingly, we find that more than half of the access control models (almost 57.4%) are developed considering no specific IoT sector, which indicates the applicability and usability of these frameworks in all IoT fields. However, a notable number of existing works (18.3%) are focused on the IoT-enabled healthcare systems. Since the patients' private and sensitive information (also known as electronic healthcare records) is stored in the cloud, in most cases, the secure access and management of these data are extremely needed. Additionally, several research works aim to develop frameworks for the smart home and intelligent transportation systems. A list is shown in Table 8 regarding the access control models deployed in different applications of IoT. Another important findings is that smart home and healthcare-specific authorization schemes adopt conventional access control models, such as RBAC, ABAC, and CapBAC. On the contrary, blockchain-, machine learning-, and deep learning-based advanced schemes are not confined to any specific IoT domains. This finding discloses that the state-of-the-art models are more adaptable, flexible, and scalable for the dynamic IoT ecosystem.

Table 8. List of access control models based on different IoT application domains.

IoT Application Domains	Access Control Models	Ref.
Smart Home	RBAC, RBAC, CapBAC, ProBAC, HyBAC (RBAC+ABAC), HyBAC (RBAC+ABAC+CapBAC), others	[43,44,69,108,130,134,160]
Healthcare	RBAC, ABAC, ABAC, ABAC, ABAC, CapBAC, BC-based, BC-based, ProBAC, Risk-based, T&ST-based, HyBAC (ABAC+RBAC+Priority), DL-based, DL-based, DL-based, BC-based, ABAC, BC-based, BC-based, BC-based, ML-based	[46,47,51,53,57,59,65,78,80,97,98,101,102,109,121, 125,128,141,144–146]
Industry	RABC, ABAC, ML-based, BC-based	[45,56,99,139]
Intelligent Transportation System	ABAC, ABAC, HyBAC (RBAC+ABAC), HyBAC (ABAC+Proximity), DL-based, DL-based, BC-based	[54,55,103,129,131,147,152]
Smart city	BC-based, others	[88,163]
Agriculture	ABAC	[60]
Generalized	Almost all types of models	[17,41,42,50,52,58,61–64,66–68,72–77,79,81–87,89–96,100,104–107,110,111,113–118,120,122–124,126,127,132,133,135–138,148,150,151,153,155,156,159,161,164]

Further analysis is conducted on the application domains of widely used IoT access control models, especially blockchain-based, deep learning-based, and attribute-based ones. More specifically, in this part, we consider three IoT application domains which focus in IoT applicaion: the healthcare system, the intelligent transport system, and the generalized sector. One of the notable findings is that in most cases, blockchain-based models are applied to any IoT domain, irrespective of healthcare, smart home, industry, or any other field. However, some of these categories of schemes (25%) are still dedicated to the healthcare sector. On the other hand, while developing DL-based and attribute-based authorization models, healthcare and intelligent transport systems are also given similar importance with generalized application domains. Interestingly, the traditional ABAC schemes are notably employed in the healthcare system since around 45% of cases are found. The percentages of different IoT application sectors of these models are illustrated in Figure 14.

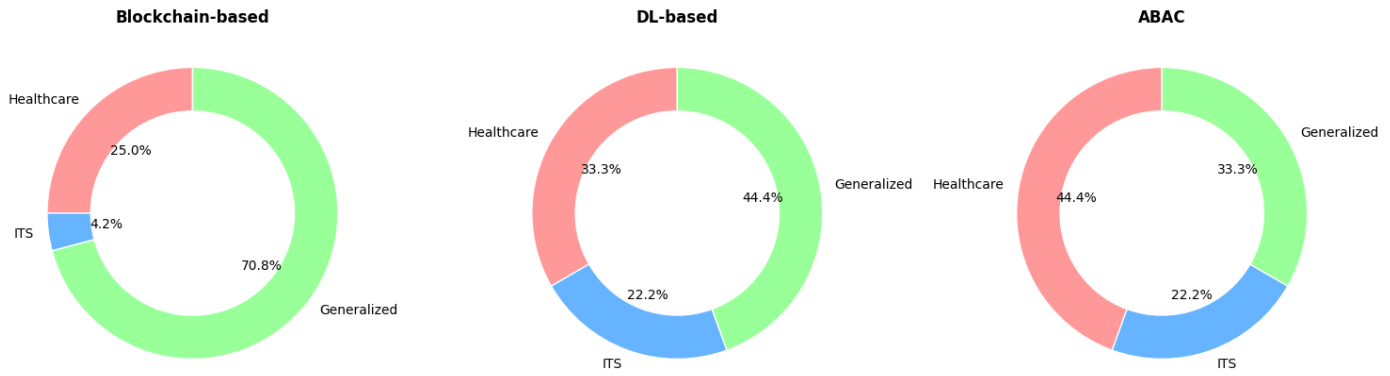

Figure 14. Analysis of blockchain-based, deep learning-based, and attribute-based (ABAC) different IoT application sectors.

4.5. RQ5: Which Requirements Are Fulfilled by the Existing Access Control Models?

In this section, we explore how our studied authorization models support access control requirements in general, without depending on specific solutions.

Granularity [12,13,36]: Refers to the capability to regulate data and resource access through the establishment of access control guidelines tailored to individual users or groups. Typically, these guidelines necessitate contextual details to enable precise control and are ideally articulated in a more detailed manner.

Context awareness [12]: The ability of a model to dynamically adjust access permissions based on changing contextual factors like time, location, and user actions within the environment. Context is very crucial for upholding privacy and security standards for all parties involved. They have to be carefully assessed when determining whether to authorize or restrict access to IoT devices or data.

Dynamicity [12,36]: This is defined as an access control framework's capability to adapt policies in real time and to decide based on the contextual information provided.

Interoperability [12,13,134]: This means the ability to effectively coordinate access control mechanisms in heterogeneous domains, which may have a wide variety of devices, protocols, networks, and platforms.

Delegation [12,13]: An entity with the authority over a resource or device can grant access rights (termed delegator) or temporarily delegate specific permissions to another entity (delegated) under predefined constraints. Given the ever-changing landscape of IoT, it is crucial for an access control framework to adapt smoothly to frequent users and resource additions to enable flexible delegation.

Automatic Revocation [12,36]: Revocation in plain terms refers to dynamically removing or invalidating access privileges from users or devices. Considering the constantly evolving nature of IoT environments in which devices frequently connect and disconnect from the network, an access control framework ought to automatically revoke access privileges upon meeting predefined conditions.

Scalability [12,13,36,134]: Scalability is the expandability of the network. To effectively handle the heterogeneity and continuously expanding nature of IoT devices, resources, and services, access control models in general need to be highly adaptable in both the scope and format of their policies.

Data trust [134]: By this, we mean establishing trust and confidence in the data generated, collected, shared, processed, and maintained within the IoT systems.

Continual control [134]: It is interpreted as ongoing and dynamic access control decisions, such as management and enforcement of access rights for users and devices in an IoT network.

Security [134]: An access control framework for IoT must prioritize safeguarding user privacy from various cyber threats considering the extensive range of connected devices from smart home gadgets to industrial sensors.

Integration support [134]: Since the IoT environment is extensively diverse, there may be a need to combine different mechanisms and approaches to manage access rights for users and devices.

User-driven [13]: It refers to the ability of the users to actively participate in defining, managing, and modifying access rules. Access control mechanisms ought to be driven by users since IoT applications necessitate direct user involvement in authorization, and users retain control over their data.

Apart from these major ones, there are a few more requirements, such as Ease of use [13,134], Distributed Nature [12,36], Availability [36], Efficiency [36], and Flexibility [13,36].

Table 9 presents a comparison of different access control frameworks based on their concern about satisfying several access control requirements using yes and no. This table shows the relative advantages and disadvantages of various proposals in terms of the considered aspects. The list of requirements is gathered from several works [12,13,36,134]. In fact, the existing surveys do not study access control requirements for all these models. Moreover, they analyze only a few requirements. In this paper, we explore 17 security requirements (the presence of which is considered an advantage and the absence considered a disadvantage) fulfilled by both the conventional and advanced access control models, thus contributing to the state-of-the-art literature.

Table 9. Comparing access control models based on specific requirements for IoT. Here, ✓ = Yes, and ✕ = No. Here, presence means advantage and absence means disadvantage of a model.

Requirement	Access Control Models														
	RBAC	ABAC	CapBAC	UCON	OrBAC	TBAC	BC-Based	ProBAC	ReBAC	Risk-Based	T&ST-Based	HyBAC	ML-Based	DL-Based	Others
Granularity	✕	✓	✕	✓	✕	✓	✕	✓	✓	✓	✓	✓	✓	✓	✕
Context-Awareness	✕	✓	✕	✓	✓	✓	✓	✕	✓	✓	✓	✓	✓	✓	✓
Dynamicity	✕	✓	✕	✓	✕	✓	✕	✓	✓	✓	✓	✓	✓	✓	✕
Interoperability	✕	✓	✓	✕	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕
Delegation	✕	✕	✓	✕	✓	✕	✓	✕	✓	✕	✕	✓	✓	✓	✕
Automatic Revocation	✕	✕	✓	✕	✕	✕	✓	✕	✓	✕	✕	✓	✓	✓	✕
Scalability	✕	✓	✓	✕	✕	✓	✕	✓	✓	✓	✕	✓	✓	✓	✕
Data trust	✕	✓	✓	✓	✕	✓	✓	✓	✓	✓	✕	✓	✓	✓	✕
Continual control	✕	✓	✓	✓	✕	✓	✓	✓	✓	✓	✕	✓	✓	✓	✕
Security	✓	✓	✓	✕	✓	✕	✓	✓	✓	✕	✓	✓	✓	✓	✕
Integration Support	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
User-driven	✓	✕	✓	✓	✕	✓	✓	✕	✓	✕	✕	✓	✓	✓	✕
Distributed Nature	✕	✕	✓	✕	✕	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕
Ease of use	✓	✕	✓	✓	✓	✕	✓	✓	✓	✕	✓	✓	✓	✓	✕
Availability	✕	✕	✕	✓	✕	✓	✓	✕	✓	✓	✓	✓	✓	✓	✕
Efficiency	✕	✓	✕	✕	✕	✓	✕	✓	✕	✓	✕	✓	✓	✓	✕
Flexibility	✕	✓	✕	✕	✕	✓	✕	✕	✓	✕	✕	✓	✓	✓	✕

5. Discussion and Future Challenges

This study extensively exhibits existing access control models in the IoT environment. Around 115 published works, including 77 journal papers and 38 conference papers, are discussed with essential technical findings. Though in the past, researchers tended to be more interested in conventional schemes, they eventually started focusing on advanced machine learning, deep learning, blockchain, and hybrid models. Although classical RBAC, ABAC, CapBAC, and TBAC frameworks offer complexity reduction and scalability, the incomparable characteristics of the advanced models such as high efficiency, accuracy, and dynamicity play a pivotal role in changing the researchers' attention. Further examination of the access control requirements satisfied by the models as depicted in Table 9 discloses that different models have different dimensions and priorities. However, the integration support aspect

is commonly required for all access control models while Automatic Revocation, Efficiency, and Flexibility are of relatively lower priority in most of the existing models.

Though the sophisticated state-of-the-art models show improved performances in policy formation and access regulation, there are still several issues that need to be considered while developing access control models for IoT systems in the future:

i. **Challenges of Combining Models**: A comprehensive exploration of hybrid authorization models reveals that researchers are confined to specific schemes such as RBAC and ABAC schemes to bring about new solutions. Another crucial issue to uncover is that all of the hybrid models combine only the conventional schemes, RBAC, ABAC, etc. Consequently, the existing hybrid schemes can only reduce complexities of the policy management, decrease extra overhead, and handle issues related to individual models. The adaption of complicated patterns and uncertain environments remains unresolved, which results in inefficiency and severe security and privacy issues. Hence, we need an appropriate framework for large-scale distributed IoT systems. Arguably, integrating diverse models is a difficult task since they have distinct dependencies, advantages, and drawbacks. A rigorous technical investigation is needed on the potential usability, viability, and applicability of integrating traditional and advanced schemes. However, intuitively, different conventional models leveraging roles, attributes, capabilities, trusts, risks, and relationships can be consolidated with machine learning- or blockchain-based models to not only increase efficiency and adaptability but also lessen complexities.

ii. **Dependency on High Computational Resources**: The experimental results of the existing models demonstrate that though the blockchain-, machine learning-, and deep learning-based frameworks offer high accuracy, enhanced security, and better performance, these models require excessive computational power like high-performance GPUs (Graphics Processing Units), a large volume of storages for generating, executing, and managing large datasets during training and testing phases. Undoubtedly, deep learning algorithms can seamlessly handle enormous datasets and offer fast processing, but they require significant time to achieve minor precision improvements. Moreover, parameter-tuning is another unavoidable critical issue since adjusting the number of layers with the expected accuracy is entirely correlated [165]. In this regard, heuristics and metaheuristics, especially evolutionary algorithms (EAs) adapted from nature, can be utilized to obtain optimized solutions in a short time.

iii. **Scalability and Latency Issues of Blockchain**: According to the existing studies, the mining processes of consensus algorithms in the blockchain, such as Proof of Work (PoW), Proof of Stake (PoS), and Proof of Existence (PoE), are proven to incur high electricity and energy, which surpass the capabilities of resource-constrained IoT devices [166]. In addition, the unavoidable scalability issues in IoT become more extreme while blockchain-based models are leveraged since the transactions per second in blockchain are comparatively much higher [167]. Numerically, the average throughputs of different blockchain protocols, for example, Bitcoin and Ethereum, are 7 and 20 transactions per second, respectively. Likewise, other systems integrating blockchain technology such as PayPal and Visa exhibit 200 and 2000 transactions per second, respectively [168]. Moreover, the excessively high latency of blockchain transactions adds to the inefficiency of IoT access control models. Latency refers to the total time between initiating a transaction and confirming its validation at the receiver's end. In blockchain, transactions are kept in a queue for verification through consensus, which increases the delay (or latency) as the number of nodes increases [169].

iv. **Issues of Cloud-enabled IoT AC Models**: The integration of cloud computing resolves the resource-constrained and power-constrained limitations of IoT devices to

a large extent. Thus, a new structure called Cloud-IoT architecture is formed, where continuously generated huge amounts of diverse and dynamic IoT data are shared and transferred to the cloud for storing, managing, and analyzing. In addition, different entities like physical devices, gateways, and service providers are involved in IoT data management in the cloud. Consequently, these data become more susceptible to security breaches since the attack surface significantly enlarges. Specifically, three major concerns including security, ownership, and privacy while sharing IoT data are mentioned in [170]. To address these issues, it is essential to design formal procedures for specifying data possession. Simultaneously, to monitor and control data flows and ensure security and data trust, researchers need to concentrate more on developing sophisticated architectures considering CE-IoT (Cloud-enabled IoT).

In addition to the issues and challenges mentioned above, edge-cloud collaboration is one of the most trending topics nowadays. Numerous studies in the literature have been conducted on this computing technology-based network while performing different tasks, such as object detection [171], resource allocation [172], anomaly detection [173], exception handling in production [174], etc. Recently, Wang et al. [175] leveraged a matchmaking attribute-based encryption technique to develop a trustworthy access control, especially in the cloud-edge-device data-sharing paradigm. Specifically, they restricted malicious behaviors of data owners by evaluating and sanitizing trust values (quality) of data. Therefore, it is recommended that new access control schemes be developed considering the edge-cloud-driven IoT network.

As this is a survey paper, we opt not to comment on specific technical performance issues without appropriate study in that direction. Combining various models and testing their performance or optimization is out of the scope of this work. Future research efforts can be exerted to test the performance of various combined models and their applicability in different IoT scenarios.

6. Conclusions

While the promises offered by IoT are catchy, the access control model would either make it or break it for real-life implementations. In this paper, we studied some crucial aspects of authorization for IoT, specifically emphasizing access control models. We contributed to the literature by exploring almost all existing significant works, considering the crucial period of research in this area, which has captured both the conventional and advanced schemes. Simultaneously, we analyzed the trade-offs of adopting advanced models like blockchain, machine learning, and hybrid models. Moreover, we elaborated on a few well-established advanced and revolutionary works by presenting their substantial architectural designs. Furthermore, we analyzed the major outcomes of all the studies included in this survey, prioritizing their strengths. This in-depth analysis will facilitate the decision-making process on which access control model is the most appropriate one, depending on the specific real-world IoT applications. Apart from these, a large-scale visualized taxonomy of access control models in the IoT environment was drawn, the recent trends and various specialized schemes considering specific IoT application domains were analyzed, and the requirements achieved by these authorization solutions were figured out.

In the end, we depicted several technical challenges of designing sophisticated access control models for IoT and then mentioned some insightful possible directions, such as combining conventional schemes with machine learning, adopting heuristics and metaheuristics techniques with deep learning, and developing scalable blockchain solutions for resource-constrained IoT devices. We hope that both the general readers and expert researchers actively working in this area are able to use this study as a useful resource material.

Author Contributions: Conceptualization, M.S.A. and A.-S.K.P.; investigation, M.S.A.; resources, M.S.A. and A.-S.K.P.; writing—original draft preparation, M.S.A.; writing—review and editing, M.S.A. and A.-S.K.P.; visualization, M.S.A. and A.-S.K.P.; supervision, A.-S.K.P.; project administration, M.S.A. and A.-S.K.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

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

Abbreviations

The following abbreviations are used in this manuscript:

ABAC	Attribute-based Access Control	ACC	Access Control Contract
ACL	Access Control List	ANN	Artificial Neural Network
AoT	Authentication of Things	BBAC	Billing-based Access Control
CapBAC	Capability-based Access Control	CE-IoT	Cloud-enabled IoT
CNN	Convolutional Neural Network	COI	Conflict of Interest
CRL	Capability Revocation List	DAC	Discretionary Access Control
DL	Deep Learning	DMS	Domain Management Server
DRM	Digital Rights Management	DT	Decision Tree
EHS	Electronic Healthcare System	ELM	Extreme Learning Machine
FDL	Federated Deep Learning	GAN	Generative Adversarial Network
GCP	Google Cloud Platform	HyBAC	Hybrid Access Control
IBAC	Identity-based Access Control	IIoT	Industrial Internet of Things
IoT	Internet of Things	IoV	Internet of Vehicles
ITS	Intelligent Transport System	KNN	k-Nearest Neighbor
LR	Logistic Regression	LSTM	Long Short-Term Memory
MAC	Mandatory Access Control	MEC	Multi-Access Edge Computing
MIoT	Manufacturing Internet of Things	ML	Machine Learning
MQTT	Message Queuing Telemetry Transport	OrBAC	Organizational-based Access Control
PBAC	Privilege-based Access Control	PE	Policy Evaluation
PG	Policy Generalization	PoE	Proof of Existence
PoS	Proof of Stake	PoW	Proof of Work
ProBAC	Protocol-based Access Control	RBAC	Role-based Access Control
ReBAC	Relationship-based Access Control	RL	Reinforcement Learning
SCADA	Supervisory Control and Data Acquisition	SL	Supervised Learning
SoD	Segregation of Duties	SVM	Support Vector Machine
TACO	Trusted Access Control Object	TBAC	Trust-based Access Control
TCC	Trust Calculation Contract	TEE	Trusted Execution Environment
TRS	Trust and Reputation System	UCON	Usage Control model
UMA	User-Managed Access	XACML	Extensible Access Control Markup Language

References

1. Singh, A.K.; Anand, A.; Lv, Z.; Ko, H.; Mohan, A. A survey on healthcare data: A security perspective. *ACM Trans. Multimid. Comput. Commun. Appl.* **2021**, *17*, 1–26. [CrossRef]
2. Shukla, S.; Patel, S.J. A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing. *Computing* **2022**, *104*, 1173–1202. [CrossRef]
3. Madakam, S.; Ramaswamy, R.; Tripathi, S. Internet of Things (IoT): A literature review. *J. Comput. Commun.* **2015**, *3*, 164–173. [CrossRef]
4. Wang, W.; Yang, S.; Zhang, X.; Xia, X. Research on the Smart Broad Bean Harvesting System and the Self-Adaptive Control Method Based on CPS Technologies. *Agronomy* **2024**, *14*, 1405. [CrossRef]
5. Khattab, A.; Habib, S.E.; Ismail, H.; Zayan, S.; Fahmy, Y.; Khairy, M.M. An IoT-based cognitive monitoring system for early plant disease forecast. *Comput. Electron. Agric.* **2019**, *166*, 105028. [CrossRef]
6. Yang, C.; Shen, W.; Wang, X. Applications of Internet of Things in manufacturing. In Proceedings of the 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanchang, China, 4–6 May 2016 ; IEEE: New York, NY, USA, 2016; pp. 670–675.
7. Ben-Daya, M.; Hassini, E.; Bahroun, Z. Internet of things and supply chain management: A literature review. *Int. J. Prod. Res.* **2019**, *57*, 4719–4742. [CrossRef]

8. Alquhali, A.H.; Roslee, M.; Alias, M.Y.; Mohamed, K.S. Iot based real-time vehicle tracking system. In Proceedings of the 2019 IEEE Conference on Sustainable Utilization and Development in Engineering and Technologies (CSUDET), Penang, Malaysia, 7–9 November 2019; IEEE: New York, NY, USA, 2019; pp. 265–270.
9. Kim, T.h.; Ramos, C.; Mohammed, S. Smart city and IoT. *Future Gener. Comput. Syst.* 2017, *76*, 159–162. [CrossRef]
10. Gharibi, M.; Boutaba, R.; Waslander, S.L. Internet of drones. *IEEE Access* **2016**, *4*, 1148–1162. [CrossRef]
11. Ahsan, M.S.; Islam, M.S.; Hossain, M.S.; Das, A. Detecting Smart Home Device Activities Using Packet-Level Signatures from Encrypted Traffic. *IEEE Trans. Dependable Secur. Comput.* **2024**, 1–12. [CrossRef]
12. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access control for IoT: A survey of existing research, dynamic policies and future directions. *Sensors* **2023**, *23*, 1805. [CrossRef]
13. Malik, A.K.; Emmanuel, N.; Zafar, S.; Khattak, H.A.; Raza, B.; Khan, S.; Al-Bayatti, A.H.; Alassafi, M.O.; Alfakeeh, A.S.; Alqarni, M.A. From conventional to state-of-the-art IoT access control models. *Electronics* **2020**, *9*, 1693. [CrossRef]
14. Ouaddah, A.; Mousannif, H.; Abou Elkalam, A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. *Comput. Netw.* **2017**, *112*, 237–262. [CrossRef]
15. Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. *J. Netw. Comput. Appl.* **2019**, *144*, 79–101. [CrossRef]
16. Bertin, E.; Hussein, D.; Sengul, C.; Frey, V. Access control in the Internet of Things: A survey of existing approaches and open research questions. *Ann. Telecommun.* **2019**, *74*, 375–388. [CrossRef]
17. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. *IEEE Internet Things J.* **2020**, *7*, 4682–4696. [CrossRef]
18. Istiaque Ahmed, K.; Tahir, M.; Hadi Habaebi, M.; Lun Lau, S.; Ahad, A. Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction. *Sensors* **2021**, *21*, 5122. [CrossRef]
19. Pal, S.; Jadidi, Z. Protocol-based and hybrid access control for the iot: Approaches and research opportunities. *Sensors* **2021**, *21*, 6832. [CrossRef]
20. Namane, S.; Ben Dhaou, I. Blockchain-based access control techniques for IoT applications. *Electronics* **2022**, *11*, 2225. [CrossRef]
21. Iqal, Z.M.; Selamat, A.; Krejcar, O. A Comprehensive Systematic Review of Access Control in IoT: Requirements, Technologies, and Evaluation Metrics. *IEEE Access* **2023**, *12*, 12636–12654. [CrossRef]
22. Pal, S.; Dorri, A.; Jurdak, R. Blockchain for IoT access control: Recent trends and future research directions. *J. Netw. Comput. Appl.* **2022**, *203*, 103371. [CrossRef]
23. Aldowah, H.; Ul Rehman, S.; Umar, I. Security in internet of things: Issues, challenges and solutions. In *Recent Trends in Data Science and Soft Computing, Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018), Kuala Lumpur, Malaysia, 23–24 June 2018*; Springer: Cham, Switzerland, 2019; pp. 396–405.
24. Polat, G.; Sodah, F. Security issues in iot: Challenges and countermeasures. *ISACA J.* **2019**, *1*, 1–7.
25. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
26. Aydos, M.; Vural, Y.; Tekerek, A. Assessing risks and threats with layered approach to Internet of Things security. *Meas. Control* **2019**, *52*, 338–353. [CrossRef]
27. Agazzi, A.E. Smart home, security concerns of IoT. *arXiv* **2020**, arXiv:2007.02628.
28. Henze, M.; Hermerschmidt, L.; Kerpen, D.; Häußling, R.; Rumpe, B.; Wehrle, K. A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Gener. Comput. Syst.* **2016**, *56*, 701–718. [CrossRef]
29. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [CrossRef]
30. Liranzo, J.; Hayajneh, T. Security and privacy issues affecting cloud-based IP camera. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; IEEE: New York, NY, USA, 2017; pp. 458–465.
31. Seralathan, Y.; Oh, T.T.; Jadhav, S.; Myers, J.; Jeong, J.P.; Kim, Y.H.; Kim, J.N. IoT security vulnerability: A case study of a Web camera. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Republic of Korea, 11–14 February 2018; IEEE: New York, NY, USA, 2018; pp. 172–177.
32. Costin, A. Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, Vienna, Austria, 28 October 2016; pp. 45–54.
33. Pathan, A.S.K. Editorial article: On the boundaries of trust and security in computing and communications systems. *Int. J. Trust. Manag. Comput. Commun.* **2014**, *2*, 1–6. [CrossRef]
34. Huang, C.; Liu, S. Securing the future of industrial operations: A blockchain-enhanced trust mechanism for digital twins in the industrial Internet of Things. *Int. J. Comput. Appl.* **2024**, *46*, 338–347. [CrossRef]

35. Chaqfeh, M.A.; Mohamed, N. Challenges in middleware solutions for the internet of things. In Proceedings of the 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, USA, 21–25 May 2012; IEEE: New York, NY, USA, 2012; pp. 21–26.
36. Alnefaie, S.; Alshehri, S.; Cherif, A. A survey on access control in IoT: Models, architectures and research opportunities. *Int. J. Secur. Netw.* **2021**, *16*, 60–76. [CrossRef]
37. Bertino, E.; Jajodiat, S.; Samarati, P. Enforcing mandatory access control in object bases. In Proceedings of the Security for Object-Oriented Systems: Proceedings of the OOPSLA-93 Conference Workshop on Security for Object-Oriented Systems, Washington, DC, USA, 26 September 1993; Springer: Berlin/Heidelberg, Germany, 1994; pp. 96–116.
38. Downs, D.D.; Rub, J.R.; Kung, K.C.; Jordan, C.S. Issues in discretionary access control. In Proceedings of the 1985 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 22–24 April 1985; IEEE: New York, NY, USA, 1985; p. 208.
39. Sandhu, R.S. Role-based access control. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 1998; Volume 46, pp. 237–286.
40. Ferraiolo, D.F.; Sandhu, R.; Gavrila, S.; Kuhn, D.R.; Chandramouli, R. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2001**, *4*, 224–274. [CrossRef]
41. Liu, J.; Xiao, Y.; Chen, C.P. Internet of things' authentication and access control. *Int. J. Secur. Netw.* **2012**, *7*, 228–241. [CrossRef]
42. Ameer, S.; Benson, J.; Sandhu, R. The EGRBAC model for smart home IoT. In Proceedings of the 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), Las Vegas, NV, USA, 11–13 August 2020; IEEE: New York, NY, USA, 2020; pp. 457–462.
43. Ameer, S.; Sandhu, R. The HABAC model for smart home IoT and comparison to EGRBAC. In Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Virtual, 28 April 2021; pp. 39–48.
44. Liu, Q.; Zhang, H.; Wan, J.; Chen, X. An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things. *IEEE Access* **2017**, *5*, 7001–7011. [CrossRef]
45. Yavari, A.; Panah, A.S.; Georgakopoulos, D.; Jayaraman, P.P.; van Schyndel, R. Scalable role-based data disclosure control for the internet of things. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; IEEE: New York, NY, USA, 2017; pp. 2226–2233.
46. Rashid, M.; Parah, S.A.; Wani, A.R.; Gupta, S.K. Securing E-Health IoT data on cloud systems using novel extended role based access control model. In *Internet of Things (IoT) Concepts and Applications*; Springer: Cham, Switzerland, 2020; pp. 473–489.
47. 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. Guide to attribute based access control (abac) definition and considerations (draft). *NIST Spec. Publ.* **2013**, *800*, 1–54.
48. Servos, D.; Osborn, S.L. Current research and open problems in attribute-based access control. *ACM Comput. Surv. (CSUR)* **2017**, *49*, 1–45. [CrossRef]
49. Hemdi, M.; Deters, R. Using REST based protocol to enable ABAC within IoT systems. In Proceedings of the 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, USA, 13–15 October 2016; IEEE: New York, NY, USA, 2016; pp. 1–7.
50. Das, S.; Namasudra, S. Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure. *IEEE Trans. Ind. Inform.* **2022**, *19*, 821–829. [CrossRef]
51. Arfaoui, A.; Cherkaoui, S.; Kribeche, A.; Senouci, S.M.; Hamdi, M. Context-aware adaptive authentication and authorization in internet of things. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.
52. Ray, I.; Alangot, B.; Nair, S.; Achuthan, K. Using attribute-based access control for remote healthcare monitoring. In Proceedings of the 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 8–11 May 2017; IEEE: New York, NY, USA, 2017; pp. 137–142.
53. Salonikias, S.; Mavridis, I.; Gritzalis, D. Access control issues in utilizing fog computing for transport infrastructure. In *Critical Information Infrastructures Security, Proceedings of the 10th International Conference, CRITIS 2015, Berlin, Germany, 5–7 October 2015*; Revised Selected Papers 10; Springer: Berlin/Heidelberg, Germany, 2016; pp. 15–26.
54. Gupta, M.; Awaysheh, F.M.; Benson, J.; Alazab, M.; Patwa, F.; Sandhu, R. An attribute-based access control for cloud enabled industrial smart vehicles. *IEEE Trans. Ind. Inform.* **2020**, *17*, 4288–4297. [CrossRef]
55. Salonikias, S.; Gouglidis, A.; Mavridis, I.; Gritzalis, D. Access control in the industrial internet of things. In *Security and Privacy Trends in the Industrial Internet of Things*; Springer: Cham, Switzerland, 2019; pp. 95–114.
56. Alnefaie, S.; Cherif, A.; Alshehri, S. Towards a distributed access control model for IoT in healthcare. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, UK, 1–3 May 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.
57. Bhatt, S.; Sandhu, R. Abac-cc: Attribute-based access control and communication control for internet of things. In Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, Barcelona, Spain, 10–12 June 2020; pp. 203–212.

58. Aghili, S.F.; Sedaghat, M.; Singelée, D.; Gupta, M. MLS-ABAC: Efficient multi-level security attribute-based access control scheme. *Future Gener. Comput. Syst.* **2022**, *131*, 75–90. [CrossRef]
59. Patil, R.Y. A secure privacy preserving and access control scheme for medical internet of things (MIoT) using attribute-based signcryption. *Int. J. Inf. Technol.* **2024**, *16*, 181–191. [CrossRef]
60. Mahalingam, N.; Sharma, P. Secure monitoring model for smart agriculture using an optimized attribute-based access control centralized authority system. *Multimed. Tools Appl.* **2024**, *83*, 44781–44798. [CrossRef]
61. Mahalle, P.N.; Anggorojati, B.; Prasad, N.R.; Prasad, R. Identity authentication and capability based access control (iacac) for the internet of things. *J. Cyber Secur. Mobil.* **2013**, *1*, 309–348. [CrossRef]
62. Anggorojati, B.; Mahalle, P.N.; Prasad, N.R.; Prasad, R. Capability-based access control delegation model on the federated IoT network. In Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, 24–27 September 2012; IEEE: New York, NY, USA, 2012; pp. 604–608.
63. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. A federated capability-based access control mechanism for internet of things (iots). In Proceedings of the Sensors and Systems for Space Applications XI, Orlando, FL, USA, 5–19 April 2018; SPIE: Bellingham, WA, USA, 2018; Volume 10641, pp. 291–307.
64. Ahamed, J.; Khan, F. An enhanced context-aware capability-based access control model for the internet of things in healthcare. In Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 20–21 November 2019; IEEE: New York, NY, USA, 2019; pp. 126–131.
65. Hussein, D.; Bertin, E.; Frey, V. A community-driven access control approach in distributed IoT environments. *IEEE Commun. Mag.* **2017**, *55*, 146–153. [CrossRef]
66. Nakamura, S.; Enokido, T.; Takizawa, M. Information flow control based on the CapBAC (capability-based access control) model in the IoT. *Int. J. Mob. Comput. Multimed. Commun. (IJMCMC)* **2019**, *10*, 13–25. [CrossRef]
67. Hernández-Ramos, J.L.; Jara, A.J.; Marin, L.; Skarmeta, A.F. Distributed capability-based access control for the internet of things. *J. Internet Serv. Inf. Secur. (JISIS)* **2013**, *3*, 1–16.
68. Gusmeroli, S.; Piccione, S.; Rotondi, D. A capability-based security approach to manage access control in the internet of things. *Math. Comput. Model.* **2013**, *58*, 1189–1205. [CrossRef]
69. Hernández-Ramos, J.L.; Jara, A.J.; Marín, L.; Skarmeta Gómez, A.F. DCapBAC: Embedding authorization logic into smart things through ECC optimizations. *Int. J. Comput. Math.* **2016**, *93*, 345–366. [CrossRef]
70. Park, J.; Sandhu, R. Towards usage control models: Beyond traditional access control. In Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, Monterey, CA, USA, 3–4 June 2002; pp. 57–64.
71. Zhang, G.; Gong, W. The research of access control based on UCON in the internet of things. *J. Softw.* **2011**, *6*, 724–731.
72. Hariri, A.; Ibrahim, A.; Alangot, B.; Bandopadhyay, S.; La Marra, A.; Rosetti, A.; Joumaa, H.; Dimitrakos, T. UCON+: Comprehensive Model, Architecture and Implementation for Usage Control and Continuous Authorization. In *Collaborative Approaches for Cyber Security in Cyber-Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 209–226.
73. Kalam, A.A.E.; Baida, R.E.; Balbiani, P.; Benferhat, S.; Cuppens, F.; Deswarte, Y.; Miege, A.; Saurel, C.; Trouessin, G. Organization based access control. In *Proceedings POLICY 2003, Proceedings of the IEEE 4th International Workshop on Policies for Distributed Systems and Networks, Lake Como, Italy, 4–6 June 2003*; IEEE: New York, NY, USA, 2003; pp. 120–131.
74. Bouij-Pasquier, I.; Ouahman, A.A.; Abou El Kalam, A.; de Montfort, M.O. SmartOrBAC security and privacy in the Internet of Things. In Proceedings of the 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, Morocco, 17–20 November 2015; IEEE: New York, NY, USA, 2015; pp. 1–8.
75. Mahalle, P.N.; Thakre, P.A.; Prasad, N.R.; Prasad, R. A fuzzy approach to trust based access control in internet of things. In Proceedings of the Wireless VITAE 2013, Atlantic City, NJ, USA, 24–27 June 2013; IEEE: New York, NY, USA, 2013; pp. 1–5.
76. Bernal Bernabe, J.; Hernandez Ramos, J.L.; Skarmeta Gomez, A.F. TACIoT: Multidimensional trust-aware access control system for the Internet of Things. *Soft Comput.* **2016**, *20*, 1763–1779. [CrossRef]
77. Butt, A.U.R.; Mahmood, T.; Saba, T.; Bahaj, S.O.; Alamri, F.S.; Iqbal, M.W.; Khan, A.R. An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment. *IEEE Access* **2023**, *11*, 138813–138826. [CrossRef]
78. Shi, N.; Tan, L.; Yang, C.; He, C.; Xu, J.; Lu, Y.; Xu, H. BacS: A blockchain-based access control scheme in distributed internet of things. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2585–2599. [CrossRef]
79. Abushmmala, F.F.; AbuSamra, A.A. Blockchain-Based Secure Smart Health IoT solution Using RBAC Architecture. *J. Eng. Res. Technol.* **2023**, *10*, 40–48.
80. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access* **2019**, *7*, 38431–38441. [CrossRef]
81. Zaidi, S.Y.A.; Shah, M.A.; Khattak, H.A.; Maple, C.; Rauf, H.T.; El-Sherbeeny, A.M.; El-Meligy, M.A. An attribute-based access control for IoT using blockchain and smart contracts. *Sustainability* **2021**, *13*, 10556. [CrossRef]
82. Chen, H.; Wan, W.; Xia, J.; Zhang, S.; Zhang, J.; Peng, X.; Fan, X. Task-Attribute-Based Access Control Scheme for IoT via Blockchain. *Comput. Mater. Contin.* **2020**, *65*. [CrossRef]

83. Chen, Y.; Tao, L.; Liang, B.; Sun, L.; Li, Y.; Xing, B.; Chen, L. Capability and Blockchain-Based Fine-Grained and Flexible Access Control Model. *IEEE Netw.* **2023**, *37*, 197–205. [CrossRef]
84. Liu, C.; Xu, M.; Guo, H.; Cheng, X.; Xiao, Y.; Yu, D.; Gong, B.; Yerukhimovich, A.; Wang, S.; Lyu, W. Tbac: A tokoin-based accountable access control scheme for the internet of things. *IEEE Trans. Mob. Comput.* **2023**, *24*, 6133–6148. [CrossRef]
85. Pathak, A.; Al-Anbagi, I.; Hamilton, H.J. TABI: Trust-based ABAC mechanism for edge-IoT using blockchain technology. *IEEE Access* **2023**, *11*, 36379–36398. [CrossRef]
86. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust management in decentralized iot access control system. In Proceedings of the 2020 IEEE international conference on blockchain and cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; IEEE: New York, NY, USA, 2020; pp. 1–9.
87. Sabrina, F. Blockchain and structural relationship based access control for IoT: A smart city use case. In Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrück, Germany, 14–17 October 2019; IEEE: New York, NY, USA, 2019; pp. 137–140.
88. Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
89. Di Francesco Maesa, D.; Mori, P.; Ricci, L. Blockchain based access control. In *Distributed Applications and Interoperable Systems: 17th IFIP WG 6.1 International Conference, DAIS 2017, Proceedings of the 12th International Federated Conference on Distributed Computing Techniques, DisCoTec 2017, Neuchâtel, Switzerland, 19–22 June 2017*; Proceedings 17; Springer: Berlin/Heidelberg, Germany, 2017; pp. 206–220.
90. Zhang, Y. Smart Contract-Based Access Control for the Internet of Things. *arXiv* **2018**, arXiv:1802.04410. [CrossRef]
91. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers* **2018**, *7*, 39. [CrossRef]
92. Liu, H.; Han, D.; Li, D. Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access* **2020**, *8*, 18207–18218. [CrossRef]
93. Dukkipati, C.; Zhang, Y.; Cheng, L.C. Decentralized, blockchain based access control framework for the heterogeneous internet of things. In Proceedings of the Third ACM Workshop on Attribute-Based Access Control, Tempe, AZ, USA, 21 March 2018; pp. 61–69.
94. Pinno, O.J.A.; Gregio, A.R.A.; De Bona, L.C. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In Proceedings of the GLOBECOM 2017–2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; IEEE: New York, NY, USA, 2017; pp. 1–6.
95. Zhonghua, C.; Goyal, S.; Rajawat, A.S. Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing. *J. Supercomput.* **2024**, *80*, 1396–1425.
96. Tian, J.; Tian, J.; Du, R. MSLShard: An efficient sharding-based trust management framework for blockchain-empowered IoT access control. *J. Parallel Distrib. Comput.* **2024**, *185*, 104795. [CrossRef]
97. Abid, A.; Cheikhrouhou, S.; Kallel, S.; Tari, Z.; Jmaiel, M. A smart contract-based access control framework for smart healthcare systems. *Comput. J.* **2024**, *67*, 407–422. [CrossRef]
98. Raj, A.; Prakash, S. An Efficient Blockchain-Based Access Control Framework for IoT-Healthcare System. *Wirel. Pers. Commun.* **2024**, *136*, 1017–1045. [CrossRef]
99. Usman, M.; Sarfraz, M.S.; Aftab, M.U.; Habib, U.; Javed, S. A Blockchain based Scalable Domain Access Control Framework for Industrial Internet of Things. *IEEE Access* **2024**, *12*, 56554–56570. [CrossRef]
100. Tian, H.; Tian, J. A Blockchain-Based Access Control Scheme for Reputation Value Attributes of the Internet of Things. *Comput. Mater. Contin.* **2024**, *78*, 1297–1310. [CrossRef]
101. Velmurugan, S.; Prakash, M.; Neelakandan, S.; Martinson, E.O. An efficient secure sharing of electronic health records using IoT-based hyperledger blockchain. *Int. J. Intell. Syst.* **2024**, *2024*, 6995202.
102. Idrissi, H.; Palmieri, P. Agent-based blockchain model for robust authentication and authorization in IoT-based healthcare systems. *J. Supercomput.* **2024**, *80*, 6622–6660. [CrossRef]
103. Hussain, S.; Tahir, S.; Masood, A.; Tahir, H. Blockchain-enabled Secure Communication Framework for Enhancing Trust and Access Control in the Internet of Vehicles (IoV). *IEEE Access* **2024**, *12*, 110992–111006. [CrossRef]
104. Pereira, P.P.; Eliasson, J.; Delsing, J. An authentication and access control framework for CoAP-based Internet of Things. In Proceedings of the IECON 2014—40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, USA, 29 October–1 November 2014; IEEE: New York, NY, USA, 2014; pp. 5293–5299.
105. Neto, A.L.M.; Souza, A.L.; Cunha, I.; Nogueira, M.; Nunes, I.O.; Cotta, L.; Gentille, N.; Loureiro, A.A.; Aranha, D.F.; Patil, H.K.; et al. Aot: Authentication and access control for the entire iot device life-cycle. In Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM, Stanford, CA, USA, 14–16 November 2016; pp. 1–15.
106. Sciancalepore, S.; Piro, G.; Caldarola, D.; Boggia, G.; Bianchi, G. OAuth-IoT: An access control framework for the Internet of Things based on open standards. In Proceedings of the 2017 IEEE symposium on computers and communications (ISCC), Heraklion, Greece, 3–6 July 2017; IEEE: New York, NY, USA, 2017; pp. 676–681.

107. Cirani, S.; Picone, M.; Gonizzi, P.; Veltri, L.; Ferrari, G. Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. *IEEE Sens. J.* **2014**, *15*, 1224–1234. [CrossRef]
108. Wu, X.; Steinfeld, R.; Liu, J.; Rudolph, C. An implementation of access-control protocol for IoT home scenario. In Proceedings of the 2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), Wuhan, China, 24–26 May 2017; IEEE: New York, NY, USA, 2017; pp. 31–37.
109. Kumar, P.M.; Gandhi, U.D. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. *J. Supercomput.* **2020**, *76*, 3963–3983. [CrossRef]
110. Cruz-Piris, L.; Rivera, D.; Marsa-Maestre, I.; De La Hoz, E.; Velasco, J.R. Access control mechanism for IoT environments based on modelling communication procedures as resources. *Sensors* **2018**, *18*, 917. [CrossRef]
111. Colombo, P.; Ferrari, E. Access control enforcement within mqtt-based internet of things ecosystems. In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 13–15 June 2018; pp. 223–234.
112. Hardy, N.W. The Internet of Things Ecosystem: Survey of the Current Landscape, Identity Relationship Management, Multifactor Authentication Mechanisms, and Underlying Protocols. *Int. J. Comput. Inf. Eng.* **2016**, *10*, 1202–1206.
113. Arora, C.; Rizvi, S.Z.R.; Fong, P.W. Higher-order relationship-based access control: A temporal instantiation with iot applications. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, New York, NY, USA, 8–10 June 2022; pp. 223–234.
114. Praharaj, L.; Ameer, S.; Gupta, M.; Sandhu, R. Attributes aware relationship-based access control for smart IoT systems. In Proceedings of the 2022 IEEE 8th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 14–16 December 2022; IEEE: New York, NY, USA, 2022; pp. 72–81.
115. dos Santos, D.R.; Westphall, C.M.; Westphall, C.B. Risk-based dynamic access control for a highly scalable cloud federation. In Proceedings of the Seventh International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2013), Barcelona, Spain, 25–31 August 2013; pp. 8–13.
116. Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B.; Daniel, J. Developing an adaptive Risk-based access control model for the Internet of Things. In Proceedings of the 2017 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), Exeter, UK, 21–23 June 2017; IEEE: New York, NY, USA, 2017; pp. 655–661.
117. Atlam, H.F.; Alenezi, A.; Hussein, R.K.; Wills, G.B. Validation of an adaptive risk-based access control model for the internet of things. *Int. J. Comput. Netw. Inf. Secur.* **2018**, *14*, 26. [CrossRef]
118. Atlam, H.F.; Wills, G.B. An efficient security risk estimation technique for Risk-based access control model for IoT. *Internet Things* **2019**, *6*, 100052. [CrossRef]
119. Atlam, H.F.; Azad, M.A.; Alassafi, M.O.; Alshdadi, A.A.; Alenezi, A. Risk-based access control model: A systematic literature review. *Future Internet* **2020**, *12*, 103. [CrossRef]
120. Atlam, H.F.; Azad, M.A.; Fadhel, N.F. Efficient NFS model for risk estimation in a risk-based access control model. *Sensors* **2022**, *22*, 2005. [CrossRef]
121. Jiang, R.; Chen, X.; Yu, Y.; Zhang, Y.; Ding, W. Risk and UCON-based access control model for healthcare big data. *J. Big Data* **2023**, *10*, 104. [CrossRef]
122. Guo, F.; Shen, G.; Huang, Z.; Yang, Y.; Cai, M.; Wei, L. Dabac: Smart contract-based spatio-temporal domain access control for the internet of things. *IEEE Access* **2023**, *11*, 36452–36463. [CrossRef]
123. Guo, Y.; Yin, L.; Li, C.; Qian, J. Spatiotemporal access model based on reputation for the sensing layer of the IoT. *Sci. World J.* **2014**, *2014*, 671038. [CrossRef]
124. Lee, C.; Guo, Y.; Yin, L. A Location Temporal based Access Control Model for IoTs. *AASRI Procedia* **2013**, *5*, 15–20. [CrossRef]
125. Abdunabi, R.; Basnet, R.; Al Amin, M. Secure Access Control for Healthcare Information Systems: A Body Area Network Perspective. In Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–11 March 2023; IEEE: New York, NY, USA, 2023; pp. 1036–1045.
126. Attia, H.B.; Kahloul, L.; Benharzallah, S. A new hybrid access control model for security policies in multimodal applications environments. *J. Univ. Comput. Sci* **2018**, *24*, 392–416.
127. El Bouanani, S.; El Kiram, M.A.; Achbarou, O.; Outchakoucht, A. Pervasive-based access control model for IoT environments. *IEEE Access* **2019**, *7*, 54575–54585. [CrossRef]
128. Thakare, A.; Lee, E.; Kumar, A.; Nikam, V.B.; Kim, Y.G. PARBAC: Priority-attribute-based RBAC model for azure IoT cloud. *IEEE Internet Things J.* **2020**, *7*, 2890–2900. [CrossRef]
129. Aftab, M.U.; Munir, Y.; Oluwasanmi, A.; Qin, Z.; Aziz, M.H.; Zakria; Son, N.T.; Tran, V.D. A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles. *IEEE Access* **2020**, *8*, 24196–24208. [CrossRef]
130. Ameer, S.; Benson, J.; Sandhu, R. Hybrid approaches (ABAC and RBAC) toward secure access control in smart home IoT. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 4032–4051. [CrossRef]

131. Lang, U.; Schreiner, R. Proximity-based access control (pbac) using model-driven security. In Proceedings of the ISSE 2015: Highlights of the Information Security Solutions Europe 2015 Conference, Berlin, Germany, 1–2 November 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 157–170.
132. Kaiwen, S.; Lihua, Y. Attribute-role-based hybrid access control in the internet of things. In Proceedings of the Web Technologies and Applications: APWeb 2014 Workshops, SNA, NIS, and IoTS, Changsha, China, 5 September 2014; Proceedings 16; Springer: Berlin/Heidelberg, Germany, 2014; pp. 333–343.
133. Wang, J.; Wang, H.; Zhang, H.; Cao, N. Trust and attribute-based dynamic access control model for Internet of Things. In Proceedings of the 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, China, 12–14 October 2017; IEEE: New York, NY, USA, 2017; pp. 342–345.
134. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. Policy-based access control for constrained healthcare resources in the context of the Internet of Things. *J. Netw. Comput. Appl.* **2019**, *139*, 57–74. [CrossRef]
135. Outchakoucht, A.; Abou El Kalam, A.; Es-Samaali, H.; Benhadou, S. Machine learning based access control framework for the Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 331–340 [CrossRef]
136. Outchakoucht, A.; Hamza, E.S.; Leroy, J.P. Dynamic access control policy based on blockchain and machine learning for the internet of things. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 417–424. [CrossRef]
137. Zhao, Y.; Su, M.; Wan, J.; Hou, J.; Mei, D. Access control policy maintenance in IoT based on machine learning. *J. Circuits, Syst. Comput.* **2021**, *30*, 2150189. [CrossRef]
138. Liu, A.; Du, X.; Wang, N. Efficient access control permission decision engine based on machine learning. *Secur. Commun. Netw.* **2021**, *2021*, 3970485. [CrossRef]
139. Usman, M.; Sarfraz, M.S.; Habib, U.; Aftab, M.U.; Javed, S. Automatic hybrid access control in scada-enabled iiot networks using machine learning. *Sensors* **2023**, *23*, 3931. [CrossRef] [PubMed]
140. Zhou, L.; Su, C.; Li, Z.; Liu, Z.; Hancke, G.P. Automatic fine-grained access control in SCADA by machine learning. *Future Gener. Comput. Syst.* **2019**, *93*, 548–559. [CrossRef]
141. Bhansali, P.K.; Hiran, D.; Kothari, H.; Gulati, K. Cloud-based secure data storage and access control for internet of medical things using federated learning. *Int. J. Pervasive Comput. Commun.* **2024**, *20*, 228–239. [CrossRef]
142. Nobi, M.N.; Krishnan, R.; Huang, Y.; Shakarami, M.; Sandhu, R. Toward deep learning based access control. In Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy, Baltimore, MD, USA, 24–27 April 2022; pp. 143–154.
143. Cappelletti, L.; Valtolina, S.; Valentini, G.; Mesiti, M.; Bertino, E. On the quality of classification models for inferring ABAC policies from access logs. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; IEEE: New York, NY, USA, 2019; pp. 4000–4007.
144. Thilagam, K.; Beno, A.; Lakshmi, M.V.; Wilfred, C.B.; George, S.M.; Karthikeyan, M.; Peroumal, V.; Ramesh, C.; Karunakaran, P. Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System. *J. Nanomater.* **2022**, *2022*, 2638613. [CrossRef]
145. Lin, H.; Kaur, K.; Wang, X.; Kaddoum, G.; Hu, J.; Hassan, M.M. Privacy-aware access control in IoT-enabled healthcare: A federated deep learning approach. *IEEE Internet Things J.* **2021**, *10*, 2893–2902. [CrossRef]
146. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]
147. Zhou, Z.; Gaurav, A.; Gupta, B.B.; Lytras, M.D.; Razzak, I. A fine-grained access control and security approach for intelligent vehicular transport in 6G communication system. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 9726–9735. [CrossRef]
148. Yu, Z.; Chen, W.; Wang, J.; Ye, K. Deep Reinforcement Learning Based Access Control Strategy for Edge Computing in IoT System. In Proceedings of the 2021 IEEE International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI), Fuzhou, China, 24–26 September 2021; IEEE: New York, NY, USA, 2021; pp. 699–702.
149. Akbarfam, A.J.; Barazandeh, S.; Maleki, H.; Gupta, D. Dlacb: Deep learning based access control using blockchain. *arXiv* **2023**, arXiv:2303.14758.
150. Xu, L.; Qin, M.; Yang, Q.; Kwak, K.S. Learning-aided dynamic access control in MEC-enabled green IoT networks: A convolutional reinforcement learning approach. *IEEE Trans. Veh. Technol.* **2021**, *71*, 2098–2109. [CrossRef]
151. Rahman, M.; Chen, L.; Loo, J.; Jie, W. Towards Deep Learning Based Access Control using Hyperledger-Fabric Blockchain for the Internet of Things. In Proceedings of the 2023 IEEE 6th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), Marrakech, Morocco, 21–23 November 2023; IEEE: New York, NY, USA, 2023; pp. 1–8.
152. Liu, Y.; Xiao, M.; Zhou, Y.; Zhang, D.; Zhang, J.; Gacanin, H.; Pan, J. An access control mechanism based on risk prediction for the IoV. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; IEEE: New York, NY, USA, 2020; pp. 1–5.
153. Chu, M.; Li, H.; Liao, X.; Cui, S. Reinforcement learning-based multiaccess control and battery prediction with energy harvesting in IoT systems. *IEEE Internet Things J.* **2018**, *6*, 2009–2020. [CrossRef]

154. Heaps, J.; Krishnan, R.; Huang, Y.; Niu, J.; Sandhu, R. Access control policy generation from user stories using machine learning. In Proceedings of the Data and Applications Security and Privacy XXXV: 35th Annual IFIP WG 11.3 Conference, DBSec 2021, Calgary, AB, Canada, 19–20 July 2021; Proceedings 35; Springer: Berlin/Heidelberg, Germany, 2021; pp. 171–188.
155. Gupta, D.; Bhatt, S.; Gupta, M.; Kayode, O.; Tosun, A.S. Access control model for google cloud iot. In Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 25–27 May 2020; IEEE: New York, NY, USA, 2020; pp. 198–208.
156. Tandon, L.; Fong, P.W.; Safavi-Naini, R. HCAP: A history-based capability system for IoT devices. In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 13–15 June 2018; pp. 247–258.
157. Gong, L. A Secure Identity-Based Capability System. In Proceedings of the S&P, Oakland, CA, USA, 1–3 May 1989; pp. 56–63.
158. Tsiatsis, V.; Gluhak, A.; Bauge, T.; Montagut, F.; Bernat, J.; Bauer, M.; Villalonga, C.; Barnaghi, P.; Krco, S. The SENSEI real world Internet architecture. In *Towards the Future Internet*; IoS Press: Amsterdam, The Netherlands, 2010; pp. 247–256.
159. Karimibiuki, M.; Aggarwal, E.; Pattabiraman, K.; Ivanov, A. Dynpolac: Dynamic policy-based access control for iot systems. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–7 December 2018; IEEE: New York, NY, USA, 2018; pp. 161–170.
160. Kim, J.E.; Boulos, G.; Yackovich, J.; Barth, T.; Beckel, C.; Mosse, D. Seamless integration of heterogeneous devices and access control in smart homes. In Proceedings of the 2012 Eighth International Conference on Intelligent Environments, Guanajuato, Mexico, 26–29 June 2012; IEEE: New York, NY, USA, 2012; pp. 206–213.
161. Rivera, D.; Cruz-Piris, L.; Lopez-Civera, G.; de la Hoz, E.; Marsa-Maestre, I. Applying an unified access control for IoT-based intelligent agent systems. In Proceedings of the 2015 IEEE 8th International Conference on Service-Oriented Computing and Applications (SOCA), Rome, Italy, 19–21 October 2015; IEEE: New York, NY, USA, 2015; pp. 247–251.
162. Uddin, M.; Islam, S.; Al-Nemrat, A. A dynamic access control model using authorising workflow and task-role-based access control. *IEEE Access* **2019**, *7*, 166676–166689. [CrossRef]
163. Omolola, O.; More, S.; Fasllija, E.; Wagner, G.; Alber, L. Policy-based access control for the IoT and Smart Cities. In Proceedings of the Open Identity Summit 2019, Garmisch-Partenkirchen, Germany, 28–29 March 2019; pp. 157–163.
164. Karnatak, V.; Mishra, A.K.; Tripathi, N.; Wazid, M.; Singh, J.; Das, A.K. A secure signature-based access control and key management scheme for fog computing-based IoT-enabled big data applications. *Secur. Priv.* **2024**, *7*, e353. [CrossRef]
165. Bharati, S.; Podder, P. Machine and deep learning for iot security and privacy: Applications, challenges, and future directions. *Secur. Commun. Netw.* **2022**, *2022*, 8951961. [CrossRef]
166. Kamal, R.; Hemdan, E.E.D.; El-Fishway, N. A review study on blockchain-based IoT security and forensics. *Multimed. Tools Appl.* **2021**, *80*, 36183–36214. [CrossRef]
167. Benrebbouh, C.; Mansouri, H.; Cherbal, S.; Pathan, A.S.K. Enhanced secure and efficient mutual authentication protocol in iot-based energy internet using blockchain. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 68–88. [CrossRef]
168. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A survey on the scalability of blockchain systems. *IEEE Netw.* **2019**, *33*, 166–173. [CrossRef]
169. Khan, D.; Jung, L.T.; Hashmani, M.A. Systematic literature review of challenges in blockchain scalability. *Appl. Sci.* **2021**, *11*, 9372. [CrossRef]
170. Bhatt, S.; Lo'ai, A.T.; Chhetri, P.; Bhatt, P. Authorizations in cloud-based internet of things: Current trends and use cases. In Proceedings of the 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 10–13 June 2019; IEEE: New York, NY, USA, 2019; pp. 241–246.
171. Guo, J.; Song, B.; Chen, S.; Yu, F.R.; Du, X.; Guizani, M. Context-aware object detection for vehicular networks based on edge-cloud cooperation. *IEEE Internet Things J.* **2019**, *7*, 5783–5791. [CrossRef]
172. Fan, W.; Zhao, L.; Liu, X.; Su, Y.; Li, S.; Wu, F.; Liu, Y. Collaborative service placement, task scheduling, and resource allocation for task offloading with edge-cloud cooperation. *IEEE Trans. Mob. Comput.* **2022**, *23*, 238–256. [CrossRef]
173. Jiang, B.; He, Q.; Zhai, Z.; Su, H. Anomaly Detection and Access Control for Cloud-Edge Collaboration Networks. *Intell. Autom. Soft Comput.* **2023**, *37*, 2335. [CrossRef]
174. Wang, W.; Hu, T.; Gu, J. Edge-cloud cooperation driven self-adaptive exception control method for the smart factory. *Adv. Eng. Inform.* **2022**, *51*, 101493. [CrossRef]
175. Wang, Z.; Fu, Y.; Lin, X. Attribute-Based Bilateral Access Control with Sanitization and Trust Management for IIoT. *IEEE Internet Things J.* **2024**. [CrossRef]