Complex & Intelligent Systems (2022) 8:3919–3941
https://doi.org/10.1007/s40747-022-00765-y

ORIGINAL ARTICLE

Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends

Abid Khan[1] · Awais Ahmad[2] · Mansoor Ahmed[3] · Jadran Sessa[4] · Marco Anisetti[4]

Received: 5 November 2021 / Accepted: 15 April 2022 / Published online: 19 May 2022

Abstract

Scalable and secure authorization of smart things is of the crucial essence for the successful deployment of the Internet of Things (IoT). Unauthorized access to smart things could exacerbate the security and privacy concern, which could, in turn, lead to the reduced adoption of the IoT, and ultimately to the emergence of severe threats. Even though there are a variety of IoT solutions for secure authorization, authorization schemes in highly dynamic distributed environments remain a daunting challenge. Access rights can dynamically change due to the heterogeneous nature of shared IoT devices and, thus, the identity and access control management are challenging. This survey provides a comprehensive comparative analysis of the current state-of-the-art IoT authorization schemes to highlight their strengths and weaknesses. Then, it defines the most important requirements and highlights the authorization threats and weaknesses impacting authorization in the IoT. Finally, the survey presents the ongoing open authorization challenges and provides recommendations for future research.

Keywords Access control · Security threat · Security attacks

Introduction

The exponential growth of connected devices (from tiny sensors to larger devices) will revolutionize the current distributed IT scenario and applications. Smart transportation, sustainable mobility, smart cities, e-health, smart vehicles, unmanned aerial vehicles (UAVs), and many more are just some examples of domains where the IoT is generating a paradigm shift promising positive impacts on everyday life. According to Intel,the IoT market value could reach 6.2 trillion dollars by 2025, and most of it will be in the health care and manufacturing sectors. The recent advancement in techniques related to IoT (e.g., Distributed storage, dynamic, and heterogeneity access) has enabled much easier device-to-device (D2D) communication over the Internet. However, the influx of IoT has introduced security and privacy concerns, thus reducing the radical growth of the emerging IoT. For adopting IoT, it is crucial to define standardized access controls for each system and adopt these controls on the final IoT deployment architecture as distributed or centralized. In IoT, it is difficult to manage D2D communication while ensuring secure authentication and authorization[1]. Unlike traditional access control mechanisms for centralized systems such as role-based access control (RBAC) [1] and attribute-based access control (ABAC) [2], the decentralized environment necessitates a new standard access control mechanism to cope with constrained physical devices and provide scalable and secure authorization accordingly. The IoT is specifically inter-networking of smart (often resource-constrained) devices that allow things to connect and exchange data; therefore, access control is mandatory. Access control can be viewed as how authorization is structured. Usually, authorization schemes are designed according to the organization structure using policies that are determining the appropriate

✉ Jadran Sessa
jadran.sessa@unimi.it

Abid Khan
abk15@aber.ac.uk

[1] Department of Computer Science, Aberystwyth University, Aberystwyth SY23 3DB, UK

[2] Computer Science Department, Air University, Islamabad, Pakistan

[3] Department of Computer Science, COMSATS University Islamabad, Park Road, Chak Shahzad, Islamabad, Pakistan

[4] Dipartimento di Informatica (DI), Università degli Studi di Milano, Via Celoria 18, Milan, Italy

[1] https://www.intel.com.au/content/www/au/en/internet-of-things/infographics/guide-to-iot-new.html.

allocation of access rights after successful authentication. Inadequate authorization may lead to some threats such as loss of data and control. Hackers or spammers may exploit access control weaknesses to alter, delete, or abuse sensitive data. This may raise several privacy concerns, especially in a critical environment. A third-party API may be used in IoT to enable D2D communication. Therefore, manufacturers should incorporate security mechanisms (authentication and authorization) with the third-party services. In healthcare systems, patients' devices (i.e., mobile phones) are used to store and visualize health records. These devices may face physical threats, since the handheld devices may be misplaced, stolen, or temporarily accessed by some other malicious third parties. Smart cards with two-factor authentications are vulnerable to smart card attacks.[2] Once a side-channel attack that observes the device operation succeeds, the attacker can gain the inside resource information easily. Even though IoT provides a large number of IoT solutions for secure authorization, authorization schemes in the highly distributed environment of IoT still present a formidable challenge. Since IoT is a shared infrastructure with heterogeneous devices, access rights may dynamically change. As a result, it is difficult to manage identity and access control. Nowadays, the adoption of IoT devices in specific application domains, such as health and industrial controls, is opening a new scenario, where IoT security is becoming strongly connected with safety. Security breaches in IoT could lead to privacy violations, safety and health consequences such as vehicle crashes, and failures in IoT medical devices such as pacemakers.

Our survey takes a different approach than the previous surveys on IoT, which normally considered IoT and the relative security aspects as a whole. In this survey, we focus on a specific aspect relative to the authorization mechanisms in IoT, which has been demonstrated to be one of the key blocking factors for the diffusion of IoT in a critical environment where trustworthiness is fundamental. [3] Our contributions can be summarized as follows:

1. Provided a comprehensive comparative analysis to show the strengths and weaknesses of the current authorization schemes in IoT,
2. Identified requirements for secure authorization in IoT,
3. Identified security leakages together with a comprehensive taxonomy of IoT threats and weaknesses,
4. Identified key challenges and future research trends.

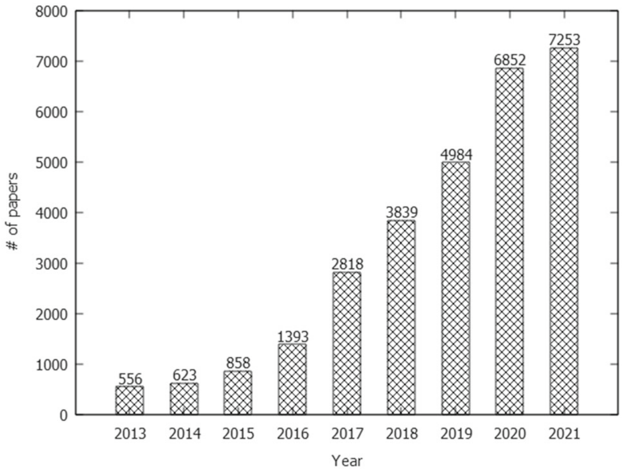

Fig. 1 Total amount of papers containing IoT and authorization keywords

The remainder of this survey is structured as follows. Section "Paper selection criteria" elucidates the paper selection criteria and provides a preview of the selected papers. Section "Comparison with the existing surveys" presents a comparison with the other existing surveys dealing with similar topics. In Section "The taxonomy", we propose a taxonomy for IoT authorization schemes and present a comparative analysis of the selected papers. Section "Non-functional requirements for authorization in IoT" presents the identification of requirements of the authorization schemes for IoT. In Section "Threats and weaknesses in IoT", authorization threats and weaknesses are elaborated. Finally, Sections "Challenges in authorization for IoT" and "Future trends" discuss the ongoing research challenges and future trends in IoT authorization, while Section "Conclusion" concludes the paper.

Paper selection criteria

In this section, we first present the paper selection criteria, and then we provide a short overview of the selected papers. We used the Explora journal discovery tool, provided by the Universitá degli Studi di Milano and complemented it with Google Scholar. To select from the available literature, we used the following selection criteria:

1. *Quality*, to select papers based on the quality. We privilege scientific and archival publications of well-recognized scientific publishers (e.g., IEEE, ACM, and Elsevier) and papers from international conferences and workshops.
2. *Coverage*, to be as inclusive as possible, considering even more generic papers that touch the aspects that we are interested in.
3. *Actionability*, to select papers based on their impact on concrete solutions and final products.

[2] Access Control Attacks and Monitoring, May-29-2012, https://access.itxlearning.com/data/cmdata/CISSP2012/Books/sbx_cissp_c02.pdf.

[3] OWASP Internet of Things Project:https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project.

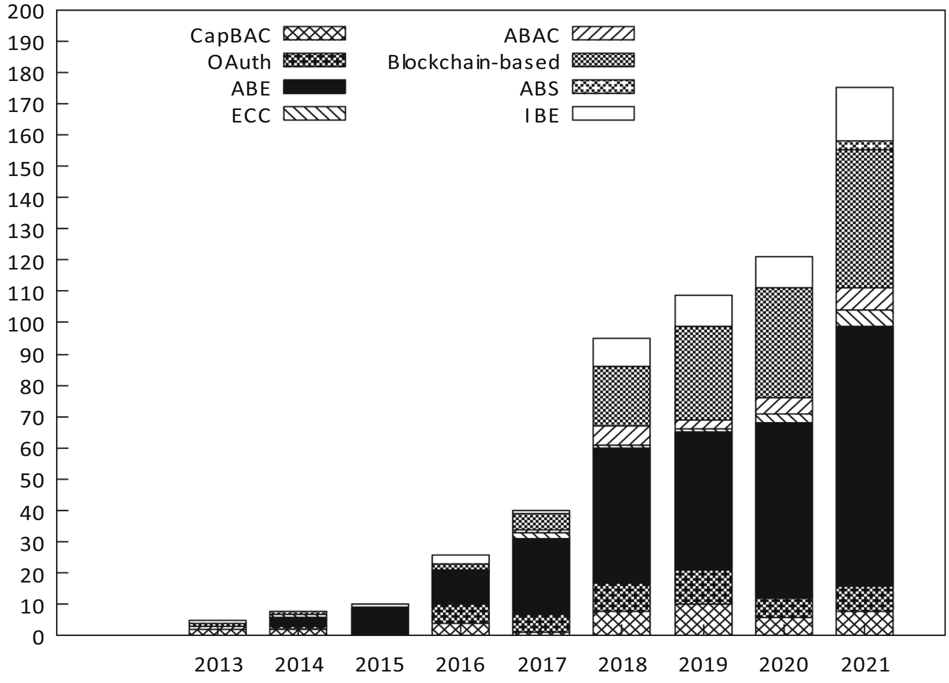

Fig. 2 Total number of papers based on the most popular authorization schemes

4. *Timeliness*, to facilitate the selection of the most recent papers where a better maturity of IoT has been reached even if the survey spans nearly a decade of research (2013–2022).

The paper selection process was based on a logic query definition compliant with the above criteria. First, we used the general keywords/queries such as ("IoT authorization") AND ("cybersecurity" OR "cyber security"). The initial number of returned papers containing these queries is shown in Fig. 1. Afterward, we further narrowed our search by including more specific keywords such as "Blockchain-based authorization" and "elliptic curve cryptography", to name but a few.

The shortlisted papers were then double checked by inspecting the abstract and searching for related terms in the paper. Due to the sheer number of published works during the considered period, we have prioritized the works having the largest number of citations in relation to the year of publication. On top of that, we have also set the exclusion criteria as follows:

1. Works in which IoT authorization was only mentioned briefly or as a part of use cases were excluded. Only those works in which authorization schemes for different aspects of IoT were the main topic of the research were included.
2. Regardless of their impact, works published by government institutions were not considered.
3. All of the works not written in English were excluded.

Figure 2 shows the distribution of the eight most popular authorization schemes in the period from 2013 until 2022. The considered schemes include:

- Elliptic Curve Cryptography (ECC), first introduced by Miller [53] in 1985, is a public-key cryptography approach based on the mathematical concept of elliptic curves over finite fields that implements the main capabilities of the asymmetric cryptosystems, including encryption, signatures, and key exchange.
- Attribute-based Access Control (ABAC) is a variation of the Role-based Access Control (RBAC) scheme, which was first coined by Ferraiolo and Kuhn in 1992 [1]. It is a logical access control approach that establishes authorization to carry out a sequence of operations.
- Identity-based Encryption (IBE), introduced in 2001 by Boneh and Franklin [54], is an encryption scheme based on Weil pairing that allows anyone within an organization to encrypt any text/information with another user's identity.
- Attribute-based Encryption (ABE), initially proposed in 2005 by Sahai and Waters [55] as fuzzy identity-based encryption, allows for multiple private keys to be used with a single public key, which is built from a list of attributes.
- Open Authorization (OAuth), created as a part of Twitter OpenID implementation in 2006 by Twitter, is an open protocol that provides secure authorization in a simple

and standard way from the web, mobile, and desktop applications.[4]

– Attribute-based Signature (ABS), proposed in 2010 by Maji et al. [56], allows a user to sign a message with fine-grained control over identifying information. The scheme reveals only that the user has attested the message with a certain set of attributes.
– Capability-based Access Control (CapBAC), first proposed by Gusmeroli et al. [4] in 2013, provides users with the capability to manage their access control processes while providing delegation and access control customization.
– Decentralized blockchain-based authorization schemes authorize users to the resources found on the underlying technology of cryptocurrencies, such as Bitcoin, first created in 2008 by an individual or group of people under the name Satoshi Nakamoto [57].

It can be noted that the research interest in the topic of ABE has been progressively increasing over the years, while the authorization schemes based on Blockchain technology have gained traction since 2017. Out of this pool, for this survey, we considered the final set consisting of 50 papers according to the previously specified criteria. Table 1 illustrates the set of selected papers according to the period they were published, as well as the scope of authorization/access control approaches they are based on.

Table 1 Evolution of authorization schemes

Period	Principal schemes
2013–2014	Policy-based access control with Extensible Access Control Markup Language (XACML) [3]
	Capability-based access control(CapBAC) [4,5]
	Identity Authentication and Capability-based Access Control (IACAC) [6]
	Distributed Capability-based Access Control (DCapBAC) [7,8]
	Fuzzy Trust Based Access Control (FTBAC) [9]
	Delegation-based authorization scheme [10]
	Host Identity Protocol (HIP) and Datagram Transport Layer Security (DTLS) based schemes [11]
	Attribute-based Signature (ABS) [12]
	Attribute-based Access Control (ABAC) [13]
	Attribute-role-based hybrid access control [14]
	Open Authorization (OAuth) [15]
	Federated Identity and Access Management (FIAM) OAuth2 with MQTT [16]
	Hierarchical Attribute-based access control [17]
	Advanced Encryption Standard (AES) [18]
2015–2017	Attribute-based access control (ABAC) [19]
	Smart gateways [20]
	DCapBAC [21,22]
	Attribute-based Encryption (ABE) [23,24]
	Multimedia files access control [25]
	OAuth [26]
	Identity-based Encryption (IBE) [27]
	Ontology based context-aware role-based access control [28]
	Certificateless signcryption scheme [29]
	Decentralized Blockchain-based approach [30,31]
2018–2022	Decentralized Blockchain-based approach [32–39]
	Elliptic Curve Cryptography (ECC) based inter-device authentication and authorization [40,41]
	Ciphertext-policy Attribute-based Encryption (CP-ABE) [42,43]
	Pseudonyms based scheme [44]
	IBE [45,46]
	Three-factor certificateless signcryption-based access control [47]
	Blockchain and ABE-based authorization [48]
	One-way cryptographic hash functions [49]
	CapBAC [50,51]
	OAuth2.0 [52]

Comparison with the existing surveys

In this section, we present the relevant surveys that focused on IoT security. To compare them to our study, we identified prominent contributions they may provide, including i) taxonomy of mechanisms (T), vulnerabilities or weaknesses (V), requirements addressed (R), and challenges and future trends (C). Table 2 provides the comparison of the related surveys according to the above contribution provided.

Ouaddah et al. [59] surveyed the access control issues in IoT. However, the paper lacks a discussion on the authorization vulnerabilities, threats, and resilience to attacks, as well as the thematic classification of the existing state-of-the-art schemes. Trnka et al. [61] provided a detailed taxonomy to study the authorization and authentication schemes for IoT. The authors argued that security context-awareness leads to a better user experience. The authors also discussed the suitability of the studied techniques for distributed and centralized architectures in IoT. Lone et al. [73] provided an overview of the literature based on the use of Blockchain smart contracts for providing security services in IoT, and

[4] https://oauth.net/about/introduction/.

Table 2 Comparison of the related surveys in the terms of taxonomy (T), Vulnerabilities (V), Challenges (C), and Requirements (R) where ✓indicates that topic was covered, ✗indicates that topic was not covered, and ∼ indicates that topic was partially covered

Reference	T	V	C	R	Y
Aleisa et al. [58]	✗	✓	∼	✗	2016
Ouaddah et al. [59]	✓	✗	✓	✓	2017
Yang et al. [60]	∼	∼	∼	✓	2017
Trnka et al. [61]	✓	✗	✓	∼	2018
Sfar et al. [62]	✓	✓	✓	✓	2018
Hou et al. [63]	∼	✓	✓	✓	2019
Verma et al. [64]	∼	✓	✓	∼	2019
Gonzalez-Manzano et al. [65]	✗	∼	✓	✗	2019
Celik et al. [66]	✗	✓	✓	✓	2019
Ferrag et al. [67]	✗	✓	✓	✗	2019
Sequeiros et al. [68]	✗	✓	∼	✓	2020
Qiu et al. [69]	∼	✗	✓	✓	2020
Sha et al. [70]	✗	✓	✓	∼	2020
Sengupta et al. [71]	∼	✓	∼	∼	2020
Hathaliya et al. [72]	✓	∼	✓	✓	2020
Lone et al. [72]	✓	✗	✗	∼	2021
Mohammad et al. [72]	∼	∼	✓	✓	2021
Sudarsan et al. [72]	✓	✗	✓	✓	2021

singled out access control and authentication as the most commonly mentioned factors for accomplishing this goal.

There are several surveys conducted on the security aspects of IoT [58,60,63,66,68]. Aleisa et al. [58] studied the privacy issues and threats along with their limitations from the IoT perspective. Yang et al. [60] organized the survey in segments covering limitations and classification of attacks with a special focus on mechanisms and architectures for authentication and access control. They also presented some security issues and solutions organized into the perception, network, transport, and application layers. Compared to our survey, they did not structure the security issues into threats, weaknesses, and attacks, but just listed them. Besides, they did not provide future trends and gaps analysis. Sfar et al. [62] focused on the roadmap for security in IoT. It provides a classification of different surveys based on security issues covered and systemic and cognitive approaches used for classifying the state-of-the-art of IoT security research activities and technological solutions. It also presents an extensive review of the main standardization activities related to IoT security. It uses a smart factory as a use case to show the application of the proposed systemic and cognitive approaches to IoT security. Hou et al. [63] presented a survey focused on IoT security from a data perspective. They focused on data life cycles, following different dimensions ranging from a data source on the device (i.e., the security of the source), to groups of IoT entities (i.e., security of the communication, authentication, and access control), until the final application (i.e., privacy, forensics, and legal challenges). However, the discussion on authentication and authorization is quite limited. Verma et al. [64] discussed the security challenges and countermeasures in the IoT context. Compared to our survey, it is generic to all the IoT aspects and only superficially touches on the issue of IoT authorization. Gonzalez-Manzano et al. [65] focused on continuous authentication aimed at ensuring user identity via user-related IoT devices. Celik et al. [66] studied program-analysis techniques for evaluating privacy and security issues in IoT with a specific emphasis on identifying attacks and countermeasures. Ferrag et al. [67] investigated the existing authorization and authentication techniques for mobile IoT devices using bio-features. The authors only focused on bio-features-based techniques and discussed the threat models and countermeasures. Sequeiros et al. [68] surveyed existing approaches, tools, and techniques for attack and system modeling applicable to IoT, Cloud computing, and Mobile Computing. In their work, Qiu et al. [69] reviewed the current state-of-the-art access control models and systems in the IoT environment, focusing on characteristics, technologies, challenges, and open research issues. They highlighted access control policy composition and access control policy sharing as two main categories of requirements for supporting future access control research. Finally, the survey discusses access control policy authorization from three aspects, including attribute discovery mechanism, policy mining, and policy authorization. Sha et al. [70] scrutinized existing edge-based IoT security solutions and research endeavors, from the perspective of security architecture designs, firewalls, intrusion detection systems, authentication and authorization protocols, and privacy-preserving mechanisms. Sengupta et al. [71] put limelight on IIoT problems and solutions. Furthermore, the authors provided object-based categorization of attacks in IoT based on vulnerabilities, after which they investigated the advantages and disadvantages of Blockchain-based solutions in addressing security challenges. However, the authors primarily focused their research only on one Blockchain-based solution, namely Tangle. Hathaliya et al. [72] overviewed a range of top-notch solutions for maintaining security and privacy in Healthcare 4.0, such as Blockchain-based solutions. They thoughtfully presented various taxonomies for exploring different security and privacy issues affecting Healthcare 4.0 and classified the advantages and weaknesses of the available techniques. Mohammad et al. [74] analysed the existing access control-based authorization schemes for smart homes and underlined the related requirements, design and implementation challenges, and characteristics based on the maturity level and access control model. The authors also identified multi-user management, resource constraints, dynamicity, flexibility, and machine-to-machine interaction as the open challenges to be solved for smart homes. Sudarsan et al. [75] suggested classification of the existing authorization techniques, based on the three pillars, namely access control models, subgranting models, and authorization governance. They also compared the advantages and shortcomings of governance strategies based on their organizational structure. However, unlike our study, the authors did not consider security threats covered by each of the investigated solutions. However, our survey is different from these studies in several ways. First, we provide an in-depth analysis of the existing IoT authorization schemes based on the cryptographic technique used by a scheme. The above surveys either ignored or partially discussed the cryptographic techniques used by the authorization mechanisms. Second, none of the previous surveys defined the requirements for IoT authorization nor presented a comparative analysis of the existing schemes based on these requirements. Third, the above surveys did not consider security threats on authorization schemes. In our survey, we consider threats and security weaknesses on various authorization techniques, and provide a complete overview of challenges and future trends.

The taxonomy

In this section, we propose a taxonomy of IoT authorization techniques based on the current state-of-the-art, as depicted in Fig. 3. According to our taxonomy, the authorization schemes in IoT can be broadly divided into two categories, namely *cryptographic schemes and non-cryptographic-based schemes*. In the following, we describe each of our taxonomy classes identifying the most relevant works among the ones we selected according to our criteria in Section “Paper selection criteria”. We also compare them in terms of strengths and weaknesses recouping their peculiarities in Tables 3, 4,5,6.

Cryptography-based authorization Schemes

Cryptographic authorization schemes can be further divided into symmetric and asymmetric schemes.

Symmetric-key cryptography (SKC)-based schemes:

Symmetric-key cryptography is an encryption scheme in which both the sender and receiver share the same secret key. The following works proposed IoT authorization schemes based on the symmetric-key cryptography.

In 2013, Seitz et al. [3] suggested a framework for enabling fine-grained and flexible access control for connected devices that have limited power. The authors utilized XACML for producing policy-based access control and symmetric keys for ensuring object protection. Alohali et al. [18] proposed a lightweight security scheme for smart homes that considers device types, as well as their capabilities, scalability, and energy efficiency. The proposed scheme is based on AES. To protect device interaction, Garcia-Morchon et al. [11] proposed two separate schemes, namely an HIP-based scheme and a DTLS-based scheme. They noted that the DTLS-based scheme allows for easier interaction and interoperability, while the overall performance of HIP is better. In 2014, Hummen et al. [10] proposed a delegation architecture for memory-constrained devices that forwards costly DTLS connection establishment to a delegation server. The proposed architecture also offers authorization while maintaining the role of the central server. To mitigate security risks coming from information sharing and gathering over public channels, in 2021, Alsahlani and Popa [49] proposed lightweight multi-factor authentication and authorization scheme for real-time data access in IoT. Their solution is based on one-way cryptographic hash functions and bitwise XOR operations, in addition to deploying a fuzzy extractor algorithm for verifying users’ biometric information.

Asymmetric cryptography (PKC)-based schemes

Asymmetric cryptography is a type of cryptography in which the public key is distributed freely to anyone, while the private key must be kept secret.

Asymmetric schemes are further divided into non-homomorphic schemes and homomorphic schemes:

Homomorphic encryption-based schemes: In homomorphic encryption, computations are carried out directly on encrypted data without requiring access to a secret key. Such type of encryption generates results in an encrypted form, which matches the result of the operations made on the plaintext when decrypted. In the time period from 2013 to 2014, the major area of research focused on capabilities and contextualization challenges in IoT. Mahalle et al. [6] introduced the concept of capabilities in the context of IoT. This approach suggested Identity Authentication and Capability-based Access Control (IACAC) grant access to the local network. However, the scheme does not apply to a WAN environment. In 2013, Gusmeroli et al. [4] affirmed that several authorization frameworks, such as RBAC do not offer effective, scalable, and manageable mechanisms to support the dynamic and distributed nature of IoT. Such frameworks cannot provide the least privileges. For this, delegation-based authentication and attribute-based access control using symmetric-key-based datagram transport layer security (DTLS) protocol (CapBAC) were proposed. However, this approach is not compatible with multi-cast traffic and lacks contextualization. A distributed capability-based access control model (DCapBAC) is presented in the work of Skarmeta et al. [7]. This is based on Elliptic Curve Digi-

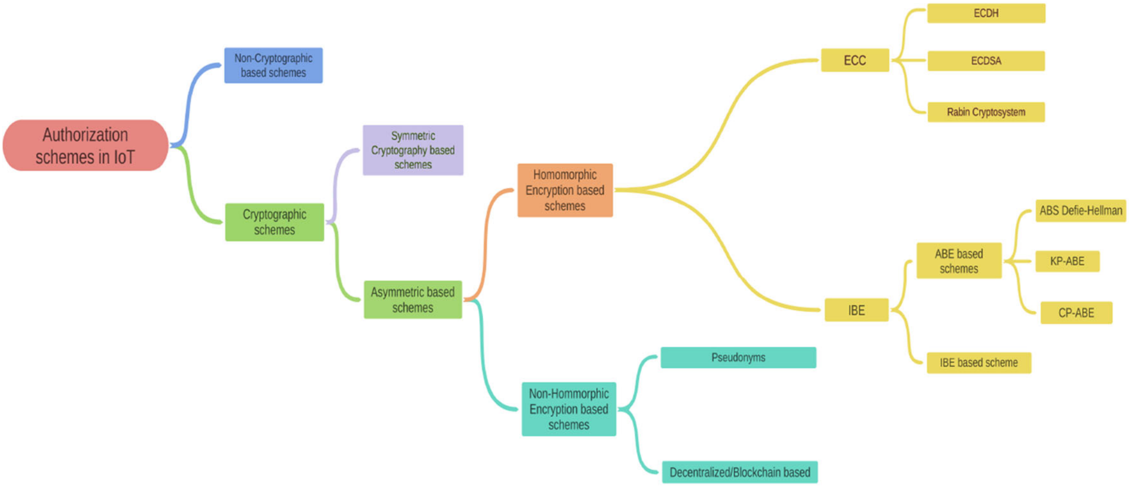
Authorization schemes in IoT
Non-Cryptographic based schemes
Cryptographic schemes
Symmetric Cryptography based schemes
Asymmetric based schemes
Homomorphic Encryption based schemes
Non-Hommorphic Encryption based schemes
ECC
ECDH
ECDSA
Rabin Cryptosystem
IBE
ABE based schemes
ABS Defie-Hellman
KP-ABE
CP-ABE
IBE based scheme
Pseudonyms
Decentralized/Blockchain based

Fig. 3 Taxonomy for authorization schemes in IoT

tal Signature Algorithm (ECDSA), where smart objects are enabled with access control logic for IoT devices. Similarly, in 2014, Hernández-Ramos et al. [8] proposed an efficient and scalable DCapBAC scheme for certification and authorization, which also supports a trust mechanism. Vucinic et al. [5] established an efficient Object-based Security Architecture (OSCAR) that provides End-to-End (E2E) security. Furthermore, the proposed system can offer the validity of trust domains and access control, while it achieves authentication using DTLS for key distribution. This scheme utilizes CapBAC for ensuring communication confidentiality and safeguarding nodes from replay attacks. Ye et al. [13] defined ABAC policies to resolve contextualization issues. It provides a lightweight ciphering and trust relationship in distributed environments using ECC. Kaiwen and Lihua [14] used an attribute-based hybrid model for defining access control in IoT. The proposed scheme has defined a policy language of attribute rules and a mechanism to overcome policy conflicts and redundancy. The authors used an example of the WeChat social networking application and provide a comparison with traditional ABAC. Ning et al. [17] suggested an aggregated-proof-based hierarchical authentication (APHA) mechanism to provide hierarchical attribute-based access control. This proposed scheme used the homomorphism function for Chebyshev chaotic maps [17], and directed path descriptors to achieve data integrity and data confidentiality. APHA assumed that the path descriptor is fresh and a trusted third party has authority on the entitled values. In their work, Su et al. [12] proposed an attribute-based signature approach using tree attributes, where policies are expressed by defining AND/OR gates thresholds. Signature forging is not possible as the signature guarantee that the user with appropriate attributes satisfies the policy. Mahalle et al. [9] introduced a scalable and energy-efficient fuzzy trust-based access control model for calculating trust. Attribute-based encryption (ABE) is used for achieving data storage, sharing, and transformation security in IoT. In the work by Yao et al. [23], lightweight key policy-based ABE with ECC was used to address privacy and security issues in IoT. Thatmann and Zickau [24] extended this approach using ciphertext policy-based ABE, which incorporates a fast and robust MQTT resource. Hernández-Ramos et al. [21] proposed a lightweight authentication and authorization mechanism based on DCapBAC. Moreover, to initiate the security bootstrapping process, a light-weighted authentication protocol over LAN (EAPOL) was associated with constrained devices. On the other hand, to achieve end-to-end secure authorization, XACML (Extensible Access Control Markup Language) was used for attaining lightweight access tokens. The year after, the same authors presented a flexible and lightweight DCapBAC using ECC that is based on policy decision point (PDP) [22]. To cope with the pervasive nature of heterogeneous devices' ecosystems, Bernabe et al. [19] proposed a flexible and efficient trust-aware distributed capability-based access control (DCapBAC) approach. This approach provides a flexible, efficient, and end-to-end security access control approach, but lacks privacy-aware features. Li et al. [27] used heterogeneous signcryption (HSC) scheme based on identity-based encryption (IBE). The proposed scheme aims to tackle identity issues of wireless sensor networks (WSN) in the context of IoT. In their work, Hosseinzadeh et al. [28] proposed a hybrid context-aware role-based access control for evaluation of the response time for regulating an access request. In 2017, Li et al. [29] designed an access control using a certificateless signcryption scheme for industrial IoT. Their scheme managed to achieve public verifiability, ciphertext authenticity, and insider security. Yang et al. [25] introduced a notion of multimedia protection into the role-based access control scheme. On top of that, the authors adopted the method of encrypted files for storage for ensuring multimedia data security and utilized digital signatures for verifying senders' identities during the reception phase. In 2018, Chifor et al. [42] proposed an authorization stack for IoT devices specifically installed in smart homes. Based on the Fast Identity Online (FIDO) protocol, users are allowed to authenticate their corresponding IoT devices. Moreover, this scheme has also analyzed the integration aspect, which makes it applicable to the existing solutions. To reduce computation overhead, Ding et al. [43] proposed a simple scalar multiplication pairing-free access control scheme based on CP-ABE. Moreover, for boosting the expressiveness of the access policy, they deployed a linear secret sharing scheme access structure (LSSS). The proposed scheme is also able to directly revoke a user or an attribute without the need of updating other users' keys. Xu et al. [50] proposed a Blockchain-enabled decentralized capability-based access control (BlendCAC) scheme for large-scale IoT systems. The authors suggested an identity-based capability token management strategy ensuring propagation and revocation of the access authorization. Moreover, the proposed scheme can efficiently impose authorization and validation in distributed and trustless IoT networks. In 2019, Lohachab [40] proposed an inter-device authentication and authorization scheme based on ECC and Message Queuing Telemetry Transport (MQTT). MQTT is an inexpensive M2M and IoT application protocol based on publish-subscribe architecture, designed specifically for resource-constrained devices. Zemmoudj et al. [44] proposed a context-aware pseudonymization and authorization model for a smart hospital. The proposed scheme uses the context information to generate a set of rules, which are used to generate a value for the trust threshold. The scheme also supports a dynamic delegation to better manage patient health between different entities. Kumar et al. [46] proposed JEDI, which is a many-to-many end-to-end encryption and key delegation for IoT systems. The authors have used a pairing-based scheme called wildcard key derivated identity-based encryption (WKD-IBE) as a building block for their proposed scheme. In 2020, Mandal et al. [47] proposed a three-factor certificateless-signcryption-based user access control for the IoT environment (CSUAC-IoT), where user password, personal biometrics, and mobile device are as authentication factors. In their scheme, the user and smart device authorize and authenticate mutually via the trusted gateway. Su et al. [45] used a proxy re-encryption-based authentication mechanism to provide a trusted authorization mechanism for nodes in CloudIoT. The authors provided the concept of dividing the cloud servers into servers based on downloading and uploading behavior. Shin and Kwon [41] proposed an ECC-based privacy-preserving authentication, authorization, and key agreement scheme for WSNs in 5 G-based IoT. Besides providing anonymity, untraceability, session key agreement, forward and backward secrecy, the proposed scheme offers protection against a wide variety of attacks, including replay, user-collusion, desynchronization, impersonation, and privilege insider attacks. In 2021, Bakir et al. [51] presented a capability authorization mechanism named CAPLets that can be efficiently used by the least capable IoT devices for supporting granular access control. Moreover, the proposed solution bolsters token capabilities by utilizing static and dynamic constraints for permitting a growing number of policies through and safeguarding the metadata channel and utilizes strong cryptography for defining a secure key exchange protocol.

[5] [6] **Non-homomorphic encryption-based schemes:** In 2013, Fremantle et al. [16] used OAuth2 with MQTT protocol to support user-directed decisions over access in a federated IoT environment. In 2014, Cirani et al. [15] presented an architecture based on the OAuth protocol and using a non-homomorphic encryption scheme that allows access tokens to third-party clients through an authorization server. This access control scheme lowers the processing load, while at the same time providing fine-grained and flexible access control policies. However, this architecture lacks end-to-end security integration between IoT and the Internet, thus allowing a single point of security compromise. This architecture does not support single sign-on (SSO). In 2016, Niruntasukrat et al. [26] designed and implemented an OAuth 1.0a-based authorization mechanism for MQTT-based IoT. During the design process, the authors carefully considered certain aspects, including node resources and user interface limitations, and key/secret distribution and management. Afterward, they showcased the robustness of the proposed scheme against eavesdropping, replay, node capturing, and man-in-the-middle attacks. Starting from 2017, an increasing focus of research has been placed on authorization schemes based on Blockchain technology. One of the first significant Blockchain-based schemes for managing and revoking delegation for granting access control, called FairAccces was proposed by Ouaddah et al. [30] In their work, Pinno et al. [31] presented a decentralized, scalable, interoperable, fault-tolerant, transparent, and user-friendly scheme for IoT access authorization called ControlChain. The proposed scheme can form relationships between users and devices, thus allowing attributes' allocation for their use for authorization. The number and popularity of decentralized Blockchain-based authorization schemes continued growing in the period from 2018 until the time of writing of this work. Tapas et al. [32] proposed a Blockchain-based IoT-Cloud authorization and delegation mechanism. Moreover, the authors have used Ethereum-based smart contracts for the implementation of the scheme. The scheme is decentralized and allows the client to audit the authorization of operations. Fayad et al. [33] proposed an adaptive

[5] We note that this scheme is also based on ECC.

[6] We note that this scheme is also based on Blockchain.

Table 3 Strengths and weaknesses of ECC-based cryptographic schemes

Reference	Strengths (⊕) and Weaknesses (⊖)
Hernández-Ramos et al. [21]	⊕ Enabling a secure Thing-to-Thing communication ⊕ Integrity and confidentiality ⊖ No trust management ⊖Lack of availability, reliability and principle of least privileges
Gusmeroli et al. [4]	⊕ Scalable, manageable, flexible, granular ⊖ Lack of confidentiality, integrity, availability and reliability
Hosseinzadeh et al. [28]	⊕ Support heterogeneous environment ⊖ Low response time ⊖ Lack of confidentiality and robustness
Hernández-Ramos et al. [22]	⊕ Access to CoAP resources ⊕ Feasibility, non-repudiation, scalability, interoperability ⊖ Lack of flexibility
Skarmeta et al. [7]	⊕ Lightweight, flexible, scalable, interoperable and providing E2E security ⊖ Authorization decisions externalized ⊖ DCapBAC does not provide trust mechanism
Ye et al. [13]	⊕ Flexible and scalable ⊖ Lack of confidentiality
Mahalle et al. [6]	⊕ Data integrity, scalability ⊕ Protection from DoS, replay, and MIN attacks ⊖ Not suitable if a set of resources is large and changes a lot ⊖ Not fully suitable for WAN ⊖ Lack of integration and usability
Vucinic et al. [5]	⊕ Protection from replay and DoS attacks ⊖ Lack of availability and anonymity
Kaiwen and Lihua [14]	⊕ Policy management and permission assignment ⊖ Limited applicability
Ning et al. [17]	⊕ Data confidentiality, data integrity, and trust ⊖ TTP is involved ⊖ The trusted entity has authority on the entitled values, so any malicious activity can cause the loss of user's data
Yanget al. [25]	⊕ Resistant to tampering, replay, MITM and password guessing attacks ⊖ Lack of scalability
Zemmoudj et al. [44]	⊕ A dynamic delegation mechanism ⊖ Public-key certificate not supported ⊖ Storage and computation overhead
Lohachab [40]	⊕ Lightweight ⊖ Strong authentication ⊖ Cannot handle the dynamic nature of devices
Hernández-Ramoset al. [8]	⊕ Scalable and interoperable ⊖ Lack of privacy
Xu et al. [50]	⊕ Scalable and lighweight ⊖ More work required for real-world apps
Shin and Kwon [41]	⊕ Resistance against a wide variety of attacks ⊖ Lack of scalability
Bakiret al. [51]	⊕ High efficiency on the least-capable devices ⊖ Lack of non-repudiation and scalability ⊖ Certain memory constraints

and lightweight Blockchain-based authentication and authorization scheme for different IoT use cases. The proposed scheme meets security requirements such as heterogeneity and robustness against cryptanalysis attacks while maintaining the low cost of implementation. In 2019, Ding et al. [35] suggested an attribute-based access control mechanism for simplifying access management. To avoid a single point of failure and data tampering, the authors used a Blockchain, which stores the record of the distribution of attributes. In 2020, Siris et al. [36] proposed decentralized authorization models for constrained IoT devices based on smart contracts and interledger mechanisms. Proposed models exploit principal advantages of smart contracts and multiple Blockchains, involving immutably recording hashes of authorization information and policies, resilience through the execution of smart contract code on all Blockchain nodes, and cryptographically linking transactions and IoT events recorded on the different Blockchains using hash-lock and time-lock mechanisms. Ali et al. [34] proposed a decentralized Blockchain-based permission delegation and access control framework for IoT

Table 4 Strengths and weaknesses of the other homomorphic-based cryptographic schemes

Reference	Strengths (⊕) and Weaknesses (⊖)
Li et al. [27]	⊕ Confidentiality, integrity, authentication, and non-repudiation ⊕ Message and ciphertext attack ⊖ TTP, also called the key generating center (KGC) is involved ⊖ As KGC generates a partial private key by using user identity and the master key, the user identity is at risk if KGC is curious
Su et al. [12]	⊕ Unforgeability, reduced computational cost ⊖ Lack of confidentiality, integrity, availability, reliability, and non-repudiation
Bernabe et al. [19]	⊕ Light-weighted, flexible, heterogeneous, context-aware, interoperable, E2E security QoS, reputation and social relationship ⊖ Lack of anonymous access token
Ferraiolo et al. [76]	⊕ Flexibility, integrity ⊖ Access control decisions can be determined by the roles individual users ⊖ Lack of scalability
Yao et al. [23]	⊕ Lowcommunication overhead ⊖ Poor generality in application scope ⊖ Lack of flexibility and scalability
Thatmann and Zickau [24]	⊕ Forward/backward secrecy supported ⊖ Intrusion can remain undetected
Suet al. [45]	⊕ Scalable and flexible ⊖ High cost of encryption/decryption by using PRE in IoT ⊖ The permission revocation is a serious problem
Li et al. [29]	⊕ Low computational cost ⊖ Lack of scalability
Kumar et al. [46]	⊕ Encryption with URIs and Expiry ⊕ Integrity, anonymity ⊖ Relies on an application-layer gateway ⊖ Lack of reliability and flexibility
Chifor et al. [42]	⊕ Lightweight ⊖ Overhead in network packet loss injection ⊖ Lack of software security stack for multiple platforms
Dinget al. [43]	⊕ Data security, forward security and backward collision resistance ⊖ High computation cost
Mandalet al. [47]	⊕ High resilience against the variety of attacks ⊖ High computational cost
Renet al. [48]	⊕ Relatively low complexity and overhead ⊕ Resilience against some common attacks ⊖ Access delay in token decryption ⊖ Lack of availability and confidentiality

called xDBAuth. The proposed solution preserves users' privacy by utilizing the Proof-of-Authenticity/Integrity mechanism for finding/retrieving user/IoT device platform hashes in the Blockchain. Blockchain in this scheme also enables user transparency and prevents potential adversaries and legitimate users from exploiting delegated permissions. Khalid et al. [37] proposed a decentralized authentication and access control mechanism for lightweight IoT devices that is based on fog computing and public Blockchain. In 2021, Putra et al. [38] proposed a decentralized IoT access control scheme based on ABAC with a supplementary Trust and Reputation System (TRS), which separates sensitive data from the public TRS data. Furthermore, their approach quantifies Service Consumer (SC) and Service Provider (SP) behavior, while utilizing recursion for streamlining the trust and reputation score computation. Ren et al. [48] proposed ABE and Blockchain-based access control mechanism for applications in SDN-IoT networks. Besides supporting authorization in heterogeneous and untrusted SDN-IoT control domains, their solution also enables the recording of all interactions between applications and the IoT network. The authors designed dedicated token encapsulation, distribution, validation, and update schemes to satisfy the decentralization requirements, whereas they utilized ABE for reducing complexity and overhead. Similarly, Wickstrom et al. [39] proposed a protocol that utilizes smart contracts on the

Table 5 Strengths (⊕) and weaknesses (⊖) of the other cryptographic and non-cryptographic schemes

Symmetric-based cryptographic schemes Reference	Strengths (⊕) and Weaknesses (⊖)
Hummen et al. [10]	⊕ E2E connections, reduced computation, memory overhead and network transmission to some extent ⊕ Remote authorization ⊖ Incompatibility with multi-cast traffic ⊖ Lack of contextualization
Mahalle et al. [9]	⊕ Low energy consumption ⊖ No real-world implementation
Garcia-Morchon et al. [11]	⊕ Flexible key management, secure communication ⊕ Interoperable and scalable ⊖ Lack of availability and scalability
Seitz et al. [3]	⊕ Fine grained and flexible access control ⊖ Meta-data can easily be compromised ⊖ Lack of reliability and non-repudiation
Alohali et al. [18]	⊕ Backward and forward secrecy ⊕ Resilience to replication and MITM attacks ⊖ Lack of scalability
Alsahlani and Popa [49]	⊕ High scalability ⊕ Low computation costs ⊖ Lack of reliability and non-repudiation
Non-cryptographic schemes	
Reference	Strengths (⊕) and Weaknesses (⊖)
Moosavi et al. [20]	⊕ Low overhead ⊖ Limited usability

Ethereum Blockchain for enforcing secure deployment, communication, management, and maintenance of IoT devices, in addition to providing authorization and authentication. in the same year, Julku et al. [52] attempted to integrate Device Identity Composition Engine (DICE)-based device attestation with the IAM system and explained how this proposed solution can augment the OAuth 2.0 framework and provide a scalable way for managing trustworthiness in distributed environments which have a significant amount of sensitive network resources. Furthermore, the authors proposed a proof-of-concept implementation of device attestation-enhanced identity management for a microcontroller class device.

Non-cryptographic-based schemes

[7]Cryptographic schemes are often computationally intensive, which is not always feasible in the context of IoT. Hence, Moosavi et al. [20] proposed a secure and efficient authentication and authorization scheme for IoT-based healthcare that relies on smart e-health gateways for taking away some weight from medical sensor nodes that are used for secure communication. In addition, their architecture depends on the certificate-based DTLS handshake protocol, and utilizes a secure key management scheme between sensor nodes and the smart gateway to accomplish security.

Non-functional requirements for authorization in IoT

In this section, we present a set of requirements that are fundamental for authorization in IoT, including:

R1 **Authentication:** Identification and authentication play a critical role in IoT security and privacy management. The authorization process strongly relies on the success and trustworthiness of the authentication process.

R2 **Access control:** Access control is used to restrict the access of available resources against undesired access. Different from traditional systems, IoT mainly focuses on more ubiquitous services being accessed on top of a heterogeneous network architecture for people, things, devices, services, etc. Therefore, who gets access to which resource is essential in IoT. Paramount characteristics of the access control can be summarized as follows:

(a) The principle of Least Privileges (PoLP): Access control is critical, so that the least privileges must be assigned to assure that during maintenance, and the maintainer cannot use all authorized rights. In IoT, PoLP provides the lowest level of things rights.

(b) Granularity (Gr): The level of access control must be fine-grained to satisfy the principle of least privileges.

(c) Separation of duties (SoD): Separation of duties is a significant part of internal controls. The objective of SoD is to distribute the tasks and subordinate privileges among multiple things (i.e., devices or users).

[7] We note that this scheme is also based on ABAC.

Table 6 Strengths and weaknesses of non-homomorphic-based cryptographic schemes

Reference	Strengths (⊕) and Weaknesses (⊖)
Cirani et al. [15]	⊕ Flexible, configurable, easy to integrate, customized fine-grained access policies ⊕ Low processing load ⊖ Single point of security compromise ⊖ No E2E security integration, SSO not addressed
Niruntasukrat et al. [26]	⊕ Protection against a wide variety of attacks ⊖ Lack of confidentiality ⊖ Poor application-level data encryption
Ouaddah et al. [30]	⊕ Transparency and granularity ⊖ Blockchain bloat ⊖ Multiple real-time confirmations required
Tapaset al. [32]	⊕ Blockchain as a technological building block scheme and Smart contracts ⊖ Weak session key management ⊖ Lack of scalability
Fremantleet al. [16]	⊕ Token size of OAuth is minimized ⊖ Prone to DoS attacks
Pinno et al. [31]	⊕ User friendly, transparent and scalable ⊕ High compatibility and scalability ⊖ Lack of revocation and delegation
Xu et al. [50]	⊕ Scalable and lighweight ⊖ More work required for real-world apps
Fayad et al. [33]	⊕ Robustness against cryptanalysis attacks ⊕ Scalable and lightweight ⊖ Still incomplete
Dinget al. [35]	⊕ Low overhead ⊖ Lack of flexibility, scalability and robustness
Khalidet al. [37]	⊕ Resilience to spoofing, Sybil, message replay and substitution attacks ⊖ High energy consumption
Ali et al. [34]	⊕ Lightweight ⊕ High throughput ⊖ No formal verification
Siriset al. [36]	⊕Reduces the amount of data that needs to be sent to the constrained IoT devices ⊖ High execution cost in certain scenarios
Julku et al. [52]	⊕ Simplicity of service implementation and scalability ⊖ Limited usability ⊖ High performance overhead
Putra et al. [38]	⊕ Scalable and reliable ⊕ Access control, reputation,and network protocol attacks resilience ⊖ High latency ⊖ Bootstrapping problem
Wickstrom et al. [39]	⊕ Autonomous device management ⊖Lack of scalability, and non-repudiation

- Static separation of duties (SSoD): The separation of duties that is enforced in the administrative environment is called static separation of duties.
- Dynamic separation of duties (DSoD): The separation of duties that is enforced only at the runtime is called dynamic separation of duties.

(d) Revocation (Re): In revocation, the access rights are taken back.

(e) Delegation (De): Assigning access rights to someone else to do parts of someone else’s job.

(f) Semantics (Se): Semantics provide meanings to things. Semantic requires supporting contextualization, heterogeneous, and interoperable environment.

- Contextualization (Con): Contextualization means to provide a meaning within which an action is taken in the constrained environment.
- Interoperability (Int): Interoperability denotes the exchange of useful information from unambiguous, shared resources. In IoT compatibility is still one of the most important hurdles.
- Heterogeneity (Het): Access control is one of the security parameters in a heterogeneous environment. IoT aims to connect several heterogeneous devices to improve the quality of life. However, only authorized users have the privileges to access the given resource.

R3 Confidentiality: In IoT, data confidentiality means that the user’s and application’s data must be kept private and only authorized entities should have access to view or modify it. Privacy-enhancing technologies (PETs) represent a set of techniques, which are used to achieve confidentiality. Due to the recent general data protection regulations (GDPR), the confidentiality of data has been recently gaining a lot of attention.

R4 **Availability:** Availability means that the services and data must be accessible. Before the services and IoT data can be made accessible, the access has to be authorized.

R5 **Non-repudiation**: Non-repudiation guarantees that things cannot deny their actions. The fact that a particular object has accessed a certain resource or performed a certain action cannot be denied. Authorization plays a fundamental role in this context. Denial of activity in the IoT environment is also a serious concern. However, it can be countered by measures carried out for non-repudiation threats.

R6 **Data Integrity:** Authorization framework in the heterogeneous IoT environment requires having end-to-end data integrity in the storage system. This means that the data cannot be modified by unauthorized entities and only the legitimate authorized entities should have the ability to do it.

R7 **Flexibility:** In IoT, access rights are dynamically changed. Therefore, it is required to have a flexible access control mechanism. For example, the security framework should be easy to update and dynamic policy rules should be customizable at runtime.

R8 **Accountability:** Accountability is defined as an obligation or responsibility. It ensures that all the actions of entities are traceable. Generally, security logs are used to keep track of the activities with only authorized entities having access to these logs.

R9 **Trust:** In IoT, there is a need for a reliable access control mechanism. In IoT, lack of trust leads to consumers' hesitation to the new technologies, while a trustworthy authorization mechanism improves the user's experience and reputation.

R10 **Privacy:** Privacy determines what type of data is shared with the third parties. This entails the privacy of the data collected and processed at various nodes in the IoT ecosystem.

R11 **Scalability:** In the context of IoT, scalability is defined as the capability of things to control a growing amount of work and its ability to accommodate this growth. It also denotes how the authorization technique will work if the number of devices is increased for the IoT ecosystem.

Table 7 shows a comparison of the selected papers in terms of the satisfaction of the requirements.

Threats and weaknesses in IoT

IoT is characterized by a large-scale distributed architecture of objects that are heterogeneous in functionalities and platform/communication protocols. They cope with different legislation/regulations, but can be deployed in places where the legislation is different. The IoT objects may need to show high automation, since they can be unsupervised, with a limited user interface, and deployed in a potentially unknown environment. They are becoming increasingly integrated with the physical world, which leads to a rising number of safety concerns (e.g., in the case of UAVs and autonomous cars). Given this scenario, IoT comes with tremendous security challenges. The peculiarity of IoT devices, which can be deployed fast, globally, and without a controlled lifespan, does not find a counterpart in cybersecurity strategies, which are still not permeating the industries. In the early stages of IoT deployment, the Vtech data breach on toys, Mirai botnet, and more recently the Silex malware attack showed how a threat to IoT can be catastrophic. Device/IoT systems can benefit from a security by design approach due to their manufactured nature.

The concepts of vulnerabilities and weaknesses have been largely used to characterize security issues, and sometimes over-defined in literature, generating colliding definitions. In this survey, we reconcile the Mitre and ENISA (European Union Agency for Cybersecurity) definitions as follows. A *threat* represents the potential for an attacker to exploit one or more system *weaknesses* through a concrete *vulnerability*. The *attack* is the action generated from this exploitation. We note that vulnerabilities are system-specific, whereas threats and weaknesses are generic and thus more suitable for a survey. The concept of weaknesses and vulnerabilities has been materialized in *Common Weakness Enumeration* that represents high-level weaknesses as *Common Vulnerabilities Exposures* .[8] The concept of threats has been percolated in a number of taxonomies in literature. In this survey, we refer to the one released by ENISA[9] contextualizing it for IoT.

In the following, we focus on authorization in IoT. We first identify the main threats and then describe the principal security weaknesses.

IoT authorization threats

In the following, we define a set of threat groups, taking inspiration from the generic ENISA threat taxonomy, but focusing on IoT authentication/authorization. We describe

[8] CWE Common Weakness Enumeration, https://cwe.mitre.org/data/definitions/699.html

[9] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy.

Table 7 Comparison of authorization requirements in IoT, ✓means that a particular requirement is fulfilled by the scheme, whereas ✗means that this requirement is not provided by the scheme

Reference	R1	R2									R3	R4	R5	R6	R7	R8	R9	R10	R11
		PoLP	Gr	SoD		Re	De	Se											
				SSoD	DSoD			Con	Int	Het									
Li et al. [27]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓	✗
Hernández-Ramos et al. [21]	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓
Kaiwen et al. [14]	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓
Mahalle et al. [9]	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓
Ning et al. [17]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗
Cirani et al. [15]	✓	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓
Bernabe et al. [19]	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓
Hernández-Ramos et al. [22]	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✓
Vucinic et al. [5]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓
Hummen et al. [10]	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓
Skarmeta et al. [7]	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓
Ye et al. [13]	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✓
Su et al. [12]	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗
Mahalle et al. [6]	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓
Yao et al. [23]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✓	✓	✗
Gusmeroli et al. [4]	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓
Garcia-Morchon et al. [11]	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓
Seitz et al. [3]	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗
Hosseinzadeh et al. [28]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✗
Thatmann and Zickau [24]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✓
Moosavi et al. [20]	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✓
Ouaddah et al. [30]	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Niruntasukrat et al. [26]	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗
Li et al. [29]	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	✓	✗
Pinno et al. [31]	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	✗	✓	✓
Chifor et al. [42]	✓	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓
Lohachab et al. [40]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗
Zemmoudj et al. [44]	✓	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
Su et al. [45]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓
Kumar et al. [46]	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓

Table 7 continued

Reference	R1	R2									R3	R4	R5	R6	R7	R8	R9	R10	R11
		PoLP	Gr	SoD		Re	De	Se											
				SSoD	DSoD			Con	Int	Het									
Ding et al. [35]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓
Tapas et al. [32]	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
Hernández-Ramos et al. [8]	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓
Fremantle et al. [16]	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Yang et al. [25]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗
Alohali et al. [18]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗
Fayad et al. [33]	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓
Ding et al. [43]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓
Khalid et al. [37]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗
Siris et al. [36]	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓
Ali et al. [34]	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓
Shin and Kwon [41]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗
Mandal et al. [47]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗
Putra et al. [38]	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓
Ren et al. [48]	✓	✗	✓	✓	✗	✓	✓	✗	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✓
Wickstrom et al. [39]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✓	✗
Alsahlani and Popa [49]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓
Xu et al. [50]	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓
Bakir [51]	✓	✓	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗
Julku et al. [52]	✓	✗	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓

why they are relevant and present a list of corresponding threats.

G1 deliberate physical attack: IoT devices are more exposed to physical attacks than other traditional devices due to their pervasive nature. This in conjunction with the resource-constrained nature of these devices causes several risks that depend on the weaknesses of the authorization procedure introduced by the physical access to the device (e.g., via unprotected dedicated management port).

- **Device cloning and substitution:** The absence of strong authentication of the devices in the IoT ecosystem allows cloning and substitutions [77]. The device can be substituted with a compromised one, rendering the rest of the IoT ecosystem incapable of identifying this substitution. Even simple cloning can be used to block the legitimate device, in turn causing a sort of DoS. During the bootstrapping procedure, a device can be also cloned and deployed in a malicious environment to extract information such as credentials.
- **Device tampering:** The physical access allows reverse engineering of firmware that can bypass any authorization and replace the firmware with malicious code [25]. For instance, the direct access to firmware replacement procedures and authorization weaknesses for such physical procedures (e.g., hardware reset without authorizations) may cause a number of attacks, such as camouflage, and malicious device/node injection, just to name a few.
- **Extraction of private information:** Physical access may lead to the evasion of access control or authorization, and extraction of sensitive information, such as hard-coded credentials, from the device memory.

G2 Unintentional damage/loss of information: Human errors are among the most critical threats in today's complex environment. These errors cause accidental threats, usually resulting from misconfiguration, clerical errors, misapplication of valid rules, and knowledge-based mistakes. In IoT, an authorization may need a non-trivial human intervention, since things usually do not have apriori knowledge about their ecosystem or completely automatic mechanisms to differentiate legitimate and illegitimate devices.

- **Inadequate design and adaptation:** It refers to inadequate design of the authorization mechanisms or the absence of accountability [21]. IoT devices rely on software that might contain severe bugs due to wrong design choices and the absence of a reliable adaptation/update strategy to fix such bugs. This makes the devices persistently vulnerable to many different types of attacks that can exploit access control leakages.
- **Over-privileged services:** It refers to misconfiguration due to a human error that leads to granting more privileges than required for services that can be used by an attacker to compromise the IoT system.
- **Conflict of interest of confidential data:** It refers to human error that allows an unauthorized user to access confidential data, including access credentials [6,27]. In many cases, it refers to the back-end IoT-Cloud infrastructure.

G3 interception and unauthorized acquisition: In an IoT network, not all communication channels are protected adequately. For instance, keying material, security parameters, or configuration settings can be exchanged with weak or unsuitable cryptographic algorithms. In IoT, it is usually assumed that no third parties can eavesdrop during the execution of key materials exchange protocol. However, this assumption may lead to the introduction of the following weaknesses:

- **Interception of information:** Interception of information refers to the threat of intercepting improperly secured information in transmission [6,27]. An attacker with low privileges can misuse transitional flaws in the authorization mechanisms to gain more privileged access to the device.
- **Communication protocol hijacking:** It refers to taking control of an existing communication session between two elements of the network. IoT communication protocol hijacking takes advantage of the possibility to sniff the traffic, and then uses aggressive strategies such as disconnection forcing.

G4 Nefarious activity/abuse: Deliberate malicious activities focused on gaining control or advantage. This threat group contains some of the most widespread IoT threats related to authentication/authorization weaknesses.

- **Identity fraud:** It refers to both weak user/admin credentials and authentication, and identity spoofing, which involves authentication protocol leakages at device bootstrapping time [4,6]. Identity fraud in IoT can occur as a result of spoofing identity provisioning protocols. This links back to the G3 group.
- **Poor credential management:** Poor credential management, including weak password choices and lack of multi-factor user authentication and administrative interfaces of devices, gateways, or back-ends, is a common vulnerability in many information systems. It is even more exacerbated in IoT due to the limitations at the device side [4,6].

- **Denial of Service:** DoS is among the main threats for IoT in which devices are resource-constrained [3]. It aims to threaten components' availability by exhausting their resources, causing performance decrease, loss of data, service outages, on one side, and also potential safety issues on the other side.
- **Unauthorized activities:** It refers to activities that often lead to malicious code injection (malware, worms, trojans, etc.). This is strongly related to weak authentication and authorization mechanisms that allow the injection without suitable access credentials verification.
- **Malicious trusted third-party APIs:** It refers to the use of third-party API for authorization, which is quite diffuse in IoT given the limited capabilities of the devices [27].

IoT authorization weaknesses

We first present the generic source of leakages that affect IoT and then refine them into a set of more authorization-specific weakness groups.

- **Software bugs**: All softwares are affected by bugs. In IoT, software bugs are often more frequent than in other ICT systems due to a small budget and strict time for dealing with software/firmware-related constraints, e.g., web interface-level constraints.
- **Design mistakes**: Nowadays, security-by-design is becoming an essential recommendation in ICT. IoT devices can benefit a lot from a security-by-design approach, since they are traditionally designed to meet budget constraints and provide as many functionalities as possible. Wrong security design/planning affects most of the ICT systems, but it is much more severe in IoT, since it is quite complex to patch a device posteriori, especially when the patches have to deal with wrong design decisions. For instance, despite frequent patches, the risk of vulnerabilities at the OS level is often high. Real-time operating systems (RTOS) such as RIoT used for IoT use a high level of abstraction. Thus, they provide less control over access control fine details [78]. Once the hacker can create an authenticated session with the operating system, he/she can easily escalate privileges.
- **Security policy errors:** Security policy-related vulnerabilities are common in IoT due to the nature of the IoT device which is often simple in terms of onboard software solutions. In addition, the security in IoT is still not well addressed by the producers, who usually neglect security policies and technologies that support the security features in heterogeneous and untrusted environments. It is quite frequent to have unwritten or poorly written security policies [79]. In addition, when available, levels of Access policies are usually not fine-grained and thus not able to achieve the principle of least privileges.
- **Miss-configurations:** Generally, IoT devices have limited configuration capabilities. A full configuration interface for addressing issues, such as security policies or features updates is rarely provided after deployment. The difficulties in IoT device software updating are the principal reasons for the high number of unpatched devices. In general, the security of the IoT also depends on the security of the involved third parties, which inherently have weak default configurations. Consequently, such configurations have an initialization stage that can be easily bypassed or re-executed, which can in turn allow an attacker to insert backdoors and gain elevation of privileges.

Inspired by Mitre Common Weakness Enumeration (CWE) taxonomy [8], Fig. 4 shows specific authorization weakness groups and the most relevant sub-weaknesses. In the following, we describe the peculiarities of each weakness group describing the link to principal leakages and threats groups.

- **Authentication weaknesses:** It encompasses all the weaknesses that refer to the process of authentication and the credentials. It encompasses all the weaknesses that refer to the process of authentication and the credentials. More specifically, it refers to IoT authentication credential weaknesses, such as (i) the widely diffuse adoption of hard-coded credentials, (ii) lack of protection of those credentials, (iii) weakness of the password requirements, and iv) weaknesses related to the recovery of forgotten passwords. It also refers to the generic weaknesses in proving the correctness of a given identity and the possibility to bypass authentication procedures. Another critical weakness is the absence of limitations on the number of allowed authentications attempts. This weakness can lead to brute force attacks. This group is mainly affected by *software bugs* and *design mistakes* leakages. For instance, it relates to threat group (G2) in case of human error in treating credentials and to threat group (G3) in the case of leakages at the protocol level. Besides brute force attacks, weak or insufficient authentication can also open the door for password, dictionary, ciphertext, and replay attacks [80].
- **Protection weaknesses:** It encompasses all the weaknesses related to the protection of sensitive information at rest and in transit, cleartext storage, unprotected transport of credentials, generic miss encryption, and insufficient control at the networking level. This group is mainly affected by *software bugs* and *miss-configurations* leakages. It relates to the following threat groups:

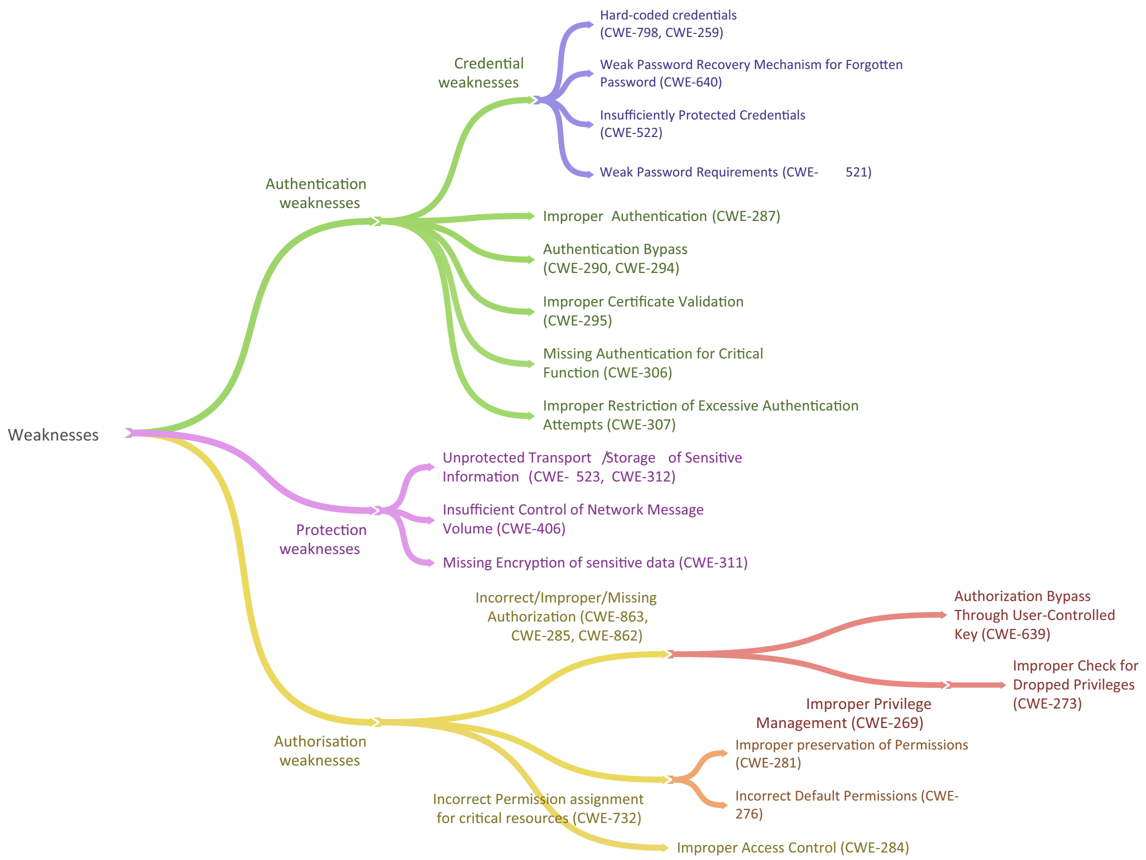
Weaknesses
Authentication weaknesses
Credential weaknesses
Hard-coded credentials (CWE-798, CWE-259)
Weak Password Recovery Mechanism for Forgotten Password (CWE-640)
Insufficiently Protected Credentials (CWE-522)
Weak Password Requirements (CWE- 521)
Improper Authentication (CWE-287)
Authentication Bypass (CWE-290, CWE-294)
Improper Certificate Validation (CWE-295)
Missing Authentication for Critical Function (CWE-306)
Improper Restriction of Excessive Authentication Attempts (CWE-307)
Protection weaknesses
Unprotected Transport /Storage of Sensitive Information (CWE- 523, CWE-312)
Insufficient Control of Network Message Volume (CWE-406)
Missing Encryption of sensitive data (CWE-311)
Authorisation weaknesses
Incorrect/Improper/Missing Authorization (CWE-863, CWE-285, CWE-862)
Authorization Bypass Through User-Controlled Key (CWE-639)
Improper Check for Dropped Privileges (CWE-273)
Improper Privilege Management (CWE-269)
Improper preservation of Permissions (CWE-281)
Incorrect Default Permissions (CWE-276)
Incorrect Permission assignment for critical resources (CWE-732)
Improper Access Control (CWE-284)

Fig. 4 IoT authorization and authentication weaknesses with the relative CWE ids

- (G1), due to the possibility of physically capturing, modifying, substituting, or cloning the device,
- (G3), due to the possibility of intercepting information in transit and hijacking protocol
- (G4), due to the exposure to identity fraud and DoS. Moreover, the attacks related to weak protection on the in-transit channel and at the device level include distributed denial of services (DDoS), man-in-the-middle attack (MITM), eavesdropping, node capture, side channel, and tampering.
- **Authorization weaknesses:** IIt encompasses weaknesses that refer to the authorization process, including incorrect, improper, or missing authorization, bypassed or improperly checked privilege, and incorrect permission assignment using the default, or improperly preserved definition of privileges. This group is mainly affected by *security policy errors*, *design mistakes*, and *miss-configurations* leakages. It relates to the threat group (G2) mainly due to human errors, over-privileged assignments, and adaptation in handling access control and threat group (G4) for the exposure to unauthorized activities. The most common attacks that can occur as a result of weak authorization and impact privacy include removal reapplication, access aggregation, and internal attacks.

We note that from the pool of the analyzed research works, 88% at least partially fill in protection weaknesses, while two-thirds satisfy authentication weaknesses. However, only 28% at least partially fill the identified authorization weaknesses, indicating that there is still space for improvement in future research.

Challenges in authorization for IoT

Several issues and challenges related to security and privacy in IoT are discussed in [62,81–84]. In the following, we underline the challenges in the context of Access controls and authorization in IoT.

C1 **Provision of new services:** The advent of IoT has been continuously bringing new services, such as smart cities. Such services can be a significant source of revenue for the governments and private sectors alike.

C2 **Building trust:** Building trust in the IoT environment is a key challenge. Therefore, enhancing trust using flexible revocation and delegation methods will pave the way for the adoption of IoT technologies.

C3 **Distributed versus centralized authorization:** The recent diffusion of IoT networks and devices has made centralized architecture a centerpiece for addressing the protection of smart object services and resources. In such environments, back-end servers are responsible for authentication and authorization tasks. Using traditional access control mechanisms prevents E2E security [85]. Consequently, centralized architecture cannot provide scalability for smart objects in IoT. To deal with the distributed nature of IoT and to support the least privileges of requirements, a deep revision and adaptation are required [83].

C4 **Standardization:** In general, standards are defined as beliefs of conventionality with legal requirements. However, in IoT, standards can be described in the aspect of the easy-to-use user interface, application design, and security and privacy tools.

C5 **Data confidentiality:** In the IoT scenario, data confidentiality represents a major concern [6]. Data confidentiality indicates that unauthorized entities are not allowed to access and modify the data. In a heterogeneous IoT environment, both users and authorized smart objects may access data. Thus, there is a need to address the two most important aspects, namely defining an object authentication method (Identity management Models) [86] and deploying a proper access control framework for the federated IoT environment. Some existing solutions for ensuring data confidentiality are not directly applicable in the context of IoT because of the following major limitations:

- **Scalability:** A scalable system can increase its efficiency and performance when tested in a constrained environment.
- **Flexible access control:** In the dynamic and heterogeneous environment of IoT, there is a need for a flexible access control mechanism.

To ensure data confidentiality based on the above-discussed issues, several extended access control methods are proposed, including RBAC, ABAC, Cap-RBAC, context-aware access control, and OAuth.

C6 **Data integrity:** Data integrity refers to combining heterogeneous data sources and providing an easy-to-use single query interface to end-users. The integration of data with different access attributes and roles is a fundamental research problem in IoT. Thus, there is a need to ensure fine-grained easily accessible access control policies.

C7 **Standard security services adoption:** Standard security services adoption denotes the process of evaluating each IoT manufacturer's implementation and selecting appropriate vendors, that obey and follow the best applicable industry standards (i.e., OWASP and Build it Securely).

C8 **Sharing of IoT-related information with device manufacturers:** To provide support and monitor devices' health, device manufacturers continuously collect and analyze the data from devices. Therefore, to ensure that the authorized model is properly implemented at the back-end of the data warehouses, the least privileged access to the third parties and manufacturers has to be enabled.

C9 **Implementation of the AAA server for defining access control preferences:** AAA server (Authentication, Authorization, and Accountability) handles user requests for access. It is often difficult to ensure what type of access privileges are permitted, to whom, under what circumstances, and under which location and time. At the same time, in some other cases, there is a need to integrate the AAA server with the third party.

C10 **Integration of Identity management with Physical access control systems (PACS):** Physical access control systems are the key challenge for ensuring additional security in IoT devices. One of the solutions for this challenge is selective provisioning, which can provide improved physical security [77].

C11 **Ensuring physical availability of the devices:** Small-size IoT devices (i.e., RFID) embedded pervasively in the IoT have limited resources and are often physically connected to malicious third parties. To identify tampering in such devices, one of the solutions is to utilize trust-aware and context-aware access control mechanisms.

C12 **Access control attacks and threats:** Inappropriate security controls lead to malicious attacks and threats against IoT systems and devices. The challenge is to identify appropriate controls for the final architecture of IoT (distributed or centralized). To prevent such attacks, "Access control attacks and monitoring" whitepaper[2] suggests solutions in which:

(a) Control Physical access is a key solution to prevent Physical access control attacks.
(b) Encrypted password files or password masking can be used to prevent illegal access.
(c) Multi-factor authentication with the least privileges must be deployed.
(d) Multiple audits can be very effective for access controls as they keep track of the actual usage of data.

Nevertheless, malicious attacks may still increase the risk of unauthorized access to resources in IoT[2].

C13 **Spreading IoT awareness:** IoT awareness and campaigns are necessary for consumers, who should take security seriously and respond accordingly [87].

Future trends

The presented survey not only provides an insight into the work which has to be done in the IoT authorization but also opens up the following questions:

- What type of access privileges are permitted to whom in which context?
- Who can be trusted?
- Do authorization mechanisms and policies provide full security?

In ABAC, attribute-based rules are used to grant access. Thus, it is difficult to determine which permission is available for a specific user. To address this, multiple rules have to be executed. This ultimately leads to rule explosion (similar to role explosion) in IoT. It is noteworthy mentioning that both RBAC and ABAC have overlapping qualities. A hybrid approach between ABAC and RBAC can be used for supporting the dynamic nature of IoT. However, defining a state line between individual and entity roles can prove to be effective. Other questions open to researchers include:

- How the authorization procedure is provided and what are the adoption methods in IoT?
- What information should be accessed, when should it be accessed, and who should be allowed to access it?
- Which interoperable semantic standards and policies are adopted within an organization and across the organization?
- What are the proper theories of authorization management in IoT?

In context-aware access control, rules adaptation and decisions can be performed on the fly. It is worthwhile to use context-aware access control to achieve dynamic access requests. Effective semantic techniques are helpful for context-aware access control, assembling, and finding conflicts in shared policies. However, contextualization is not enough for secure authorization. The use of authentication, which includes POLP by default, holds fine-grained dynamic access rights with separation of duties, delegation rights, and auditability. However, in such access controls, single sign-on security is compromised. Hence, it is necessary to deploy a multi-factor authentication with the principle of least privileges and incorporate accountability to keep track of all user data usage. The timeline of access control in Table 1 shows that CapBAC can be assumed as the representative approach in IoT in recent years, since it offers the principle of least authorization (POLA) with a high degree of flexibility and fine-grained access control. Moreover, to deal with machine interoperability and trust, it is advisable to incorporate lightweight and reusable semantic techniques with CapBAC. Furthermore, more research efforts are needed for privacy enhancement using anonymous capability-based access control techniques. On the other hand, issuing capabilities to all subjects is the major drawback of CapBAC. It is necessary to standardize the structure of CapBAC services, tokens, and protocols [4]. In the last couple of years, Blockchain technology has been becoming increasingly popular as one of the most promising solutions for IoT authorization. Blockchain comes with several perks, including decentralization, transparency, scalability, and immutability. As one of the defining Blockchain features, immutability refers to the ability of the Blockchain ledger to maintain its transaction history permanent, indelible, and unalterable. Consequently, authorization schemes based on decentralized Blockchain technologies have the potential of providing additional data integrity and trust, while at the same time having a lower cost. However, despite its undeniable potential in the field of IoT authorization, Blockchain technology brings certain shortcomings that still have to be addressed. One such shortcoming is the ever-growing size of an entire Blockchain, which in some cases presents an issue for the resource-constrained devices. Another similar issue is that resource-constrained devices might not be able to keep up with the speed and volume of the new registers [31]. We can expect to see an even larger number of Blockchain-based authorization solutions in the upcoming years, as well as their further advancements from both security and technical viewpoints. In the following list, we present the recommendations for enabling secure authorization in IoT, as well as the challenges identified in Section "Future trends" that can be potentially resolved with each of the provided recommendations.

- Implement unified user identity and access management with single sign-on. **Related challenges:** C4, C7
- Use multi-factor authentication with POLP by default [88]. **Related challenges:** C8
- Use cryptographic approaches to ensure the security of sensitive data. **Related challenges:** C5, C6
- Deploy fine-grained access rights with multiple audits. **Related challenges:** C1, C7
- Include accountability measures within secure IoT devices. **Related challenges:** C10, C11
- Have AAA server with the third-party services [89]. **Related challenges:** C1, C9
- Bind laws to establish trust. **Related challenges:** C1, C2
- Deploy lightweight attack-resistant solutions. **Related challenges:** C1, C5, C6, C12
- Shift focus to decentralized solutions. **Related challenges:** C3
- Raise awareness of IoT security requirements. **Related challenges:** C13.

Conclusion

Authorization is an important concern and a formidable challenge in IoT. While extended access control mechanisms are proposed to tackle these problems, IoT is still facing several issues and challenges related to the application of access control frameworks and authorization schemes. This survey presents a comprehensive overview and a comparative analysis of the existing authorization schemes. On top of that, we propose a thematic taxonomy of the existing IoT authorization techniques based on the current state-of-the-art. Afterward, we classify authorization threats, weaknesses, and loopholes, as well as their related subgroups. Finally, we identify IoT authorization challenges, analyze current trends, and provide recommendations for addressing the identified challenges in the future.

Acknowledgements This work has received funding from European Union's Horizon 2020 research and innovation programme under Grant Agreement No 830927, under the Marie Sklodowska-Curie Grant Agreement No. 801522, by Science Foundation Ireland and co-funded by the European Regional Development Fund through the ADAPT Centre for Digital Content Technology Grant Number 13/RC/2106_P2. It has also co-funded by Università degli Studi di Milano under the program "Piano sostegno alla ricerca".

Declarations

Conflict of interest There is no conflict of interest.

Availability of data and materials Not applicable.

Code availability Not applicable.

References

1. Ferraiolo D, Kuhn DR, Chandramouli R (2003) Role-based access control, Artech House,
2. Yuan E, Tong J (2005) Attributed based access control (abac) for web services, in: IEEE International Conference on Web Services (ICWS'05), IEEE
3. Seitz L, Selander G, Gehrmann C (2013) Authorization framework for the internet-of-things, in, IEEE 14th International Symposium on A World of Wireless, Mobile and Multimedia Networks(WoWMoM). IEEE 2013:1–6
4. Gusmeroli S, Piccione S, Rotondi D (2013) A capability-based security approach to manage access control in the internet of things. Math Comput Model 58(5–6):1189–1205
5. Vučinić M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R (2014) Oscar: Object security architecture for the internet of things. In: Proceeding of IEEE international symposium on a world of wireless, mobile and multimedia networks 2014, IEEE, pp. 1–10
6. Mahalle PN, Anggorojati B, Prasad NR, Prasad R (2013) Identity authentication and capability based access control (iacac) for the internet of things. J Cyber Secur Mob 1(4):309–348
7. Skarmeta AF, Hernandez-Ramos JL, Moreno MV (2014) A decentralized approach for security and privacy challenges in the internet of things. In: IEEE world forum on Internet of Things (WF-IoT). IEEE, 67–72
8. Hernández-Ramos JL, Jara AJ, Marin L, Skarmeta AF (2013) Distributed capability-based access control for the internet of things. J Int Serv Inf Secur (JISIS) 3(3/4):1–16
9. Mahalle PN, Thakre PA, Prasad NR, Prasad R (2013) A fuzzy approach to trust based access control in internet of things. In: Wireless VITAE 2013, IEEE, pp 1–5
10. Hummen R, Shafagh H, Raza S, Voig T, Wehrle K (2014) Delegation-based authentication and authorization for the ip-based internet of things. In: eleventh annual IEEE international conference on Sensing, Communication, and Networking (SECON). Ieee, pp 284–292
11. Garcia-Morchon O, Keoh SL, Kumar S, Moreno-Sanchez P, Vidal-Meca F, Ziegeldorf JH (2013) Securing the ip-based internet of things with hip and dtls. In: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, pp 119–124
12. Su J, Cao D, Zhao B, Wang X, You I (2014) epass: an expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things. Fut Gen Comput Syst 33:11–18
13. Ye N, Zhu Y, Wang R-c, Malekian R, Lin Q-M, An efficient authentication and access control scheme for perception layer of internet of things
14. Kaiwen S, Lihua Y (2014) Attribute-role-based hybrid access control in the internet of things. In: Asia-Pacific Web Conference, Springer, New York, pp 333–343
15. Cirani S, Picone M, Gonizzi P, Veltri L, Ferrari G (2014) Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. IEEE Sens J 15(2):1224–1234
16. Fremantle P, Aziz B, Kopeckỳ J, Scott P (2014) Federated identity and access management for the internet of things. In: International Workshop on Secure Internet of Things. IEEE 2014:10–17
17. Ning H, Liu H, Yang LT (2014) Aggregated-proof based hierarchical authentication scheme for the internet of things. IEEE Trans Parallel Distrib Syst 26(3):657–667
18. Alohali B, Merabti M, Kifayat K (2014) A secure scheme for a smart house based on cloud of things (cot). In: 6th Computer science and electronic engineering conference (CEEC), IEEE 2014:115–120
19. Bernabe JB, Ramos JLH, Gomez AFS (2016) Taciot: multidimensional trust-aware access control system for the internet of things. Soft Comput 20(5):1763–1779
20. Moosavi SR, Gia TN, Rahmani A-M, Nigussie E, Virtanen S, Isoaho J, Tenhunen H (2015) Sea: a secure and efficient authentication and authorization architecture for iot-based healthcare using smart gateways. Procedia Comput Sci 52:452–459
21. Hernandez-Ramos JL, Pawlowski MP, Jara AJ, Skarmeta AF, Ladid L (2015) Toward a lightweight authentication and autho-

rization framework for smart objects. IEEE J Sel Areas Commun 33(4):690–702
22. Hernández-Ramos JL, Jara AJ, Marín L, Skarmeta Gómez AF (2016) Dcapbac: embedding authorization logic into smart things through ecc optimizations. Int J Comput Math 93(2) 345–366
23. Yao X, Chen Z, Tian Y (2015) A lightweight attribute-based encryption scheme for the internet of things. Fut Gen Comput Syst 49:104–112
24. Thatmann D, Zickau S, Förster A, Küpper A (2015) Applying attribute-based encryption on publish subscribe messaging patterns for the internet of things. In: 2015 IEEE International Conference on Data Science and Data Intensive Systems, IEEE, pp 556–563
25. Yang J, He S, Lin Y, Lv Z (2017) Multimedia cloud transmission and storage system based on internet of things. Multimed Tools Appl 76(17):17735–17750
26. Niruntasukrat A, Issariyapat C, Pongpaibool P, Meesublak K, Aiumsupucgul P, Panya A (2016) Authorization mechanism for mqtt-based internet of things. In: 2016 IEEE International Conference on Communications Workshops (ICC), IEEE, pp 290–295
27. Li F, Han Y, Jin C (2016) Practical access control for sensor networks in the context of the internet of things. Comput Commun 89:154–164
28. Hosseinzadeh S, Virtanen S, Díaz-Rodríguez N, Lilius J (2016) A semantic security framework and context-aware role-based access control ontology for smart spaces. In: Proceedings of the International Workshop on Semantic Big Data, pp 1–6
29. Li F, Hong J, Omala AA (2017) Efficient certificateless access control for industrial internet of things. Futur Gen Comput Syst 76:285–292
30. Ouaddah A, Abou Elkalam A, Ait Ouahman A (2016) Fairaccess: a new blockchain-based access control framework for the internet of things. Secur Commun Netw 9(18):5943–5964
31. Pinno OJA, Gregio ARA, De Bona LCE (2017) Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp. 1–6.https://doi.org/10.1109/GLOCOM.2017.8254521
32. Tapas N, Merlino G, Longo F (2018) Blockchain-based iot-cloud authorization and delegation. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), IEEE, pp 411–416
33. Fayad A, Hammi B, Khatoun R (2018) An adaptive authentication and authorization scheme for iot's gateways: a blockchain based approach. In: 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), IEEE, pp 1–7
34. Ali G, Ahmad N, Cao Y, Khan S, Cruickshank H, Qazi EA, Ali A (2020) xdbauth: Blockchain based cross domain authentication and authorization framework for internet of things. IEEE Access 8:58800–58816
35. Ding S, Cao J, Li C, Fan K, Li H (2019) A novel attribute-based access control scheme using blockchain for iot. IEEE Access 7:38431–38441
36. Siris VA, Dimopoulos D, Fotiou N, Voulgaris S, Polyzos GC (2020) Decentralized authorization in constrained iot environments exploiting interledger mechanisms. Comput Commun 152:243–251
37. Khalid U, Asim M, Baker T, Hung PC, Tariq MA, Rafferty L (2020) A decentralized lightweight blockchain-based authentication mechanism for iot systems, Cluster Computing 1–21
38. Putra GD, Dedeoglu V, Kanhere SS, Jurdak R, Ignjatovic A (2021) Trust-based blockchain authorization for iot. IEEE Trans Netw Serv Manag 18(2):1646–1658
39. Wickström J, Westerlund M, Pulkkis G (2021) Smart contract based distributed iot security: A protocol for autonomous device management. In: IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE 2021:776–781
40. Lohachab A et al (2019) Ecc based inter-device authentication and authorization scheme using mqtt for iot networks. J Inf Secur Appl 46:1–12
41. Shin S, Kwon T (2020) A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5g-integrated internet of things. IEEE Access 8:67555–67571. https://doi.org/10.1109/ACCESS.2020.2985719
42. Chifor B-C, Bica I, Patriciu V-V, Pop F (2018) A security authorization scheme for smart home internet of things devices. Fut Gen Comput Syst 86:740–749
43. Ding S, Li C, Li H (2018) A novel efficient pairing-free cp-abe based on elliptic curve cryptography for iot. IEEE Access 6:27336–27345. https://doi.org/10.1109/ACCESS.2018.2836350
44. Zemmoudj S, Bermad N, Omar M (2019) Context-aware pseudonymization and authorization model for iot-based smart hospitals. J Ambient Intell Hum Comput 10(11):4473–4490
45. Su M, Zhou B, Fu A, Yu Y, Zhang G (2020) Prta: A proxy re-encryption based trusted authorization scheme for nodes on cloudiot. Inf Sci 527:533–547
46. Kumar S, Hu Y, Andersen MP, Popa RA, Culler DE (2019) {JEDI}: Many-to-many end-to-end encryption and key delegation for iot. In: 28th {USENIX} Security Symposium ({USENIX} Security 19), pp 1519–1536
47. Mandal S, Bera B, Sutrala AK, Das AK, Choo K-KR, Park Y (2020) Certificateless-signcryption-based three-factor user access control scheme for iot environment. IEEE Internet Things J 7(4):3184–3197
48. Ren W, Sun Y, Luo H, Guizani M (2021) Siledger: A blockchain and abe-based access control for applications in sdn-iot networks. IEEE Trans Netw Serv Manag 18(4):4406–4419
49. Alsahlani AYF, Popa A (2021) Lmaas-iot: Lightweight multi-factor authentication and authorization scheme for real-time data access in iot cloud-based environment. J Netw Comput Appl 192:103177
50. Xu R, Chen Y, Blasch E, Chen G (2018) Blendcac: A blockchain-enabled decentralized capability-based access control for iots, In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE pp 1027–1034
51. Bakir F, Wolski R, Krintz C (2021) Caplets: Resource aware capability-based access control for iot. In: 2021 IEEE/ACM Symposium on Edge Computing (SEC), IEEE
52. Julku J, Suomalainen J, Kylänpää M (2021) Delegated device attestation for iot. In: 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, pp. 1–8
53. Miller VS (1985) Use of elliptic curves in cryptography, in: Conference on the theory and application of cryptographic techniques, Springer, pp. 417–426
54. Boneh D, Franklin M (2001) Identity-based encryption from the weil pairing, In: Annual international cryptology conference, Springer, pp. 213–229
55. Sahai A, Waters B (2005) Fuzzy identity-based encryption, In: Annual international conference on the theory and applications of cryptographic techniques, Springer, pp. 457–473
56. Maji HK, Prabhakaran M, Rosulek M (2011) Attribute-based signatures, In: Cryptographers' track at the RSA conference, Springer, pp. 376–392
57. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system, Decentralized Business Review 21260
58. Aleisa N, Renaud K Privacy of the internet of things: a systematic literature review (extended discussion), arXiv preprint arXiv:1611.03340

59. Ouaddah A, Mousannif H, Abou Elkalam A, Ouahman AA (2017) Access control in the internet of things: Big challenges and new opportunities. Comput Netw 112:237–262
60. Yang Y, Wu L, Yin G, Li L, Zhao H (2017) A survey on security and privacy issues in internet-of-things. IEEE Internet Things J 4(5):1250–1258
61. Trnka M, Cerny T, Stickney N (2018) Survey of authentication and authorization for the internet of things, Security and Communication Networks
62. Sfar AR, Natalizio E, Challal Y, Chtourou Z (2018) A roadmap for security challenges in the internet of things. Digital Communications and Networks 4(2):118–137
63. Hou J, Qu L, Shi W (2019) A survey on internet of things security from data perspectives. Comput Netw 148:295–306
64. Verma N, Sangwan S, Sangwan S, Parsad D Iot security challenges and counters measures, International Journal of Recent Technology and Engineering (IJRTE) ISSN 2277–3878
65. Gonzalez-Manzano L, Fuentes JMD, Ribagorda A (2019) Leveraging user-related internet of things for continuous authentication: A survey. ACM Computing Surveys (CSUR) 52(3):1–38
66. Celik ZB, Fernandes E, Pauley E, Tan G, McDaniel P (2019) Program analysis of commodity iot applications for security and privacy: Challenges and opportunities. ACM Computing Surveys (CSUR) 52(4):1–30
67. Ferrag MA, Maglaras L, Derhab A (2019) Authentication and authorization for mobile iot devices using biofeatures: Recent advances and future trends, Security and Communication Networks
68. Sequeiros JB, Chimuco FT, Samaila MG, Freire MM, Inácio PR (2020) Attack and system modeling applied to iot, cloud, and mobile ecosystems: embedding security by design. ACM Computing Surveys (CSUR) 53(2):1–32
69. Qiu J, Tian Z, Du C, Zuo Q, Su S, Fang B (2020) A survey on access control in the age of internet of things. IEEE Internet Things J 7(6):4682–4696
70. Sha K, Yang TA, Wei W, Davari S (2020) A survey of edge computing-based designs for iot security. Digital Communications and Networks 6(2):195–202
71. Sengupta J, Ruj S, Bit SD (2020) A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. J Netw Comput Appl 149:102481
72. Hathaliya JJ, Tanwar S (2020) An exhaustive survey on security and privacy issues in healthcare 4.0. Comput Commun 153:311–335
73. Lone AH, Naaz R (2021) Applicability of blockchain smart contracts in securing internet and iot: a systematic literature review. Computer Science Review 39:100360
74. Mohammad ZN, Farha F, Abuassba AO, Yang S, Zhou F (2021) Access control and authorization in smart homes: A survey. Tsinghua Science and Technology 26(6):906–917
75. Sudarsan SV, Schelén O, Bodin U Survey on delegated and self-contained authorization techniques in cps and iot, IEEE Access
76. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R (2001) Proposed nist standard for role-based access control. ACM Transactions on Information and System Security (TISSEC) 4(3):224–274
77. Cirani S, Ferrari G, Veltri L (2013) Enforcing security mechanisms in the ip-based internet of things: An algorithmic overview. Algorithms 6(2):197–226
78. Alamri A, Bertok P, Thom JA, Fahad A (2016) The mediator authorization-security model for heterogeneous semantic knowledge bases. Futur Gener Comput Syst 55:227–237
79. Suhail S, Hussain R, Abdellatif M, Pandey SR, Khan A, Hong CS (2020) Provenance-enabled packet path tracing in the rpl-based internet of things. Comput Netw 173:107189
80. Babar S, Mahalle P, Stango A, Prasad N, Prasad R (2010) Proposed security model and threat taxonomy for the internet of things (iot), in: International Conference on Network Security and Applications, Springer, pp. 420–429
81. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (iot): A vision, architectural elements, and future directions. Futur Gener Comput Syst 29(7):1645–1660
82. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: Vision, applications and research challenges. Ad Hoc Netw 10(7):1497–1516
83. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Comput Netw 57(10):2266–2279
84. Díaz M, Martín C, Rubio B (2016) State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. J Netw Comput Appl 67:99–117
85. Alcaraz C, Roman R, Najera P, Lopez J (2013) Security of industrial sensor network-based remote substations in the context of the internet of things. Ad Hoc Netw 11(3):1091–1104
86. Chen J, Liu Y, Chai Y (2015) An identity management framework for internet of things, in: 2015 IEEE 12th International Conference on e-Business Engineering, IEEE, pp. 360–364
87. Guo B, Zhang D, Wang Z, Yu Z, Zhou X (2013) Opportunistic iot: Exploring the harmonious interaction between human and the internet of things. J Netw Comput Appl 36(6):1531–1539
88. Gupta U Application of multi factor authentication in internet of things domain, arXiv preprint arXiv:1506.03753
89. Rose K, Eldridge S, Chapin L (2015) The internet of things: An overview. The internet society (ISOC) 80:1–50

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.