IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 29 November 2023, accepted 18 December 2023, date of publication 26 December 2023,
date of current version 26 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3347495

RESEARCH ARTICLE

A Comprehensive Systematic Review of Access Control in IoT: Requirements, Technologies, and Evaluation Metrics

ZEINAB M. IQAL[1,2], ALI SELAMAT[1,2,3,4], (Member, IEEE), AND ONDREJ KREJCAR[3,4]

[1]Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, Malaysia
[2]MagicX (Media and Games Center of Excellence), Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, Malaysia
[3]Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, Kuala Lumpur 54100, Malaysia
[4]Faculty of Informatics and Management, University of Hradec Králové, 500 03 Hradec Kralove, Czech Republic

Corresponding authors: Zeinab M. Iqal (zeinabiqal@gmail.com) and Ali Selamat (aselamat@utm.my)

This work was supported in part by the Ministry of Higher Education (MOHE) through the Fundamental Research Grant Scheme (FRGS) under Grant FRGS/1/2022/ICT08/UTM/01/1, in part by the Universiti Teknologi Malaysia (UTM) Fundamental Research under Grant Vot Q.K130000.3843.23H46, and in part by the Faculty of Informatics and Management, University of Hradec Kralove, through the Specific Research Project (SPEV) under Grant 2102/2023.

ABSTRACT The Internet of Things (IoT) is an emerging technology with a high market growth rate. In the IoT, machines and users from different levels must collaborate to exchange data and share resources. The IoT opens the door for a vast improvement in all aspects of human life. However, the increasing adoption of the IoT in many sectors makes it difficult to control security risks. For this reason, there is a need for more effort in both research and industry to address the risks and find convenient solutions. This systematic literature review delves deeply into understanding the unique challenges and requirements posed by IoT environments. Through a detailed examination of 96 selected studies, this paper primarily addresses three research questions. The study concludes by summarizing key requirements, technologies, and metrics founded on our comprehensive analysis, aiming to steer further research in the domain. As IoT continues its expansion into various facets of our daily lives, there's a paramount need to integrate with emerging technologies and ensure scalability. Prioritizing real-world implementations is crucial for the next wave of innovations in access control systems.

INDEX TERMS Access control, Internet of Things, IoT, security, systematic review.

I. INTRODUCTION

The Internet of Things (IoT) is an emerging technology that enables communication, interaction, and data exchange between IoT devices. In IoT, data flows from different points and are collected for decision-making and analysis. The Development IoT applications faces many challenges, and security is a major one. The IoT promises to improve the quality of human life by providing advanced applications to support individuals' needs at all levels, including business, personal, and industry. IoT is built based on the available infrastructure of the Internet and combines both Internet infrastructure and emerging technologies. The result of this combination makes it easy to interconnect hundreds of billions of embedded systems and provide service management with less cost, and both scalability and flexibility changes [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

Access control works as a central support, ensuring strong information security. Recognizing the unique challenges presented by the IoT, access control not only serves to monitor and regulate resource access but also diligently restricts the needless spread of information [2]. Even as the IoT draws upon the legacy of traditional Internet technologies, it presents distinct characteristics absent in standard systems [3].

Access control sets the overarching framework governing who can access a resource and under which stipulations [4]. Authentication acts as a gatekeeper, verifying the identities of users, systems, or devices. Once this identity is authenticated, it is the domain of authorization to define the scope and nature of access permitted to the entity, ensuring precise adherence to the allowed parameters [5]. However, there is a conflict in understanding the difference between authentication and access control. Authentication asks "Who are you?" in general, whereas access control asks "Who is trusted?" [6].

Access control is responsible for ensuring security by preventing unauthorized access to data and resources.

As a result, IoT inherits the characteristics of the Internet and has unique features that are not present in traditional Internet technology. Therefore, technologies built for the conventional Internet can be used for IoT, but cannot perform in the best way. Access control is one such type of technology. Access control is a backbone technology that protects IoT resources by enforcing access restrictions on devices, objects, data, and services. Access control has many definitions, but in simple terms, it can be described as the mechanism for deciding access to resources.

Traditional access control techniques do not perform well in IoT environments. However, they cannot fully solve security challenges that are more complex than those encountered in traditional networks. Many known access control frameworks are based on policies including Role-Based Access Control (RBAC) [7], Attribute-based Access Control(ABAC) [4], and Usage Control [8]. These frameworks work implicitly, assuming that the systems have central authority. IoT is an environment that has both similar and different requirements to the traditional Internet.

The growth of IoT applications requires considerable efforts to support and secure IoT at all levels. This article aims to provide a general view of access control in the IoT environment. In this study, we present a systematic literature review of recently published papers on access control for the IoT environment to investigate access control models, technologies, challenges, and evaluation metrics, which is a step toward designing an improved access control model for IoT.

This review helps us to identify available research on access control in the context of IoT, and provide researchers to understand the access control requirement in IoT, the available used techniques for development, and the evaluation metrics. In this study, and based on the selected research plan, 96 articles were selected for final investigation. We discussed and analyzed the access control technologies, models, challenges, and evaluation metrics, to make this study as a first step of researchers during their journey on this topic.

Motivation: The IoT has transformed the structure of our digital society, we can see IoT devices everywhere, connecting everything from our homes to our hospitals. But with so many devices talking to each other, we need to be sure that they're sharing information safely. That's where access control comes in - it's like a gatekeeper for device interactions. The question of who gets access, when, and under which conditions isn't just technical - it's foundational. It determines the trustworthiness of the entire ecosystem. However, understanding how to best control this access is a big task, and there's a lot of scattered information out there. Yet, despite its significance, the domain of access control within IoT remains scattered across diverse studies, each exploring a sliver of the vast landscape. This problem calls for a synthesized, holistic exploration, setting the stage for our systematic review.

Contributions: In our comprehensive systematic review titled "A Comprehensive Systematic Review of Access Control in IoT: Requirements, Technologies, and Evaluation Metrics," we've made several significant contributions to the field. Firstly, we have gathered and meticulously analyzed the various requirements essential for an effective IoT access control system. Beyond just collating requirements, we've also conducted a thorough review of the myriad of technologies proposed and implemented in this sphere, presenting them in a comparative framework that facilitates side-by-side evaluation, filling a notable gap in existing literature. Additionally, our focus on evaluation metrics introduces a standardizing element, suggesting benchmarks that validate the effectiveness of these technologies not just theoretically, but in practical, real-world scenarios.

A crucial addition to our paper is the development of a taxonomy for access control technologies specific to IoT. This taxonomy categorizes and organizes these technologies, providing a clear and structured understanding of the field. This not only offers a comprehensive overview of the current landscape but also illuminates the way forward, identifying existing knowledge gaps and suggesting promising areas for future research and innovation.

II. RELATED WORK

The existing studies covered access control in the IoT in different ways. In recent years, various research studies have profoundly enriched the discourse on access control within the Internet of Things (IoT) environment, each offering nuanced perspectives on the challenges and potential solutions. Qiu et al. embarked on an exhaustive journey through the domain of access control specific to IoT search environments. Their survey underscored the necessity of effective access control mechanisms to regulate the ever-growing volume of IoT data, especially when such data is of a sensitive nature, encompassing personal health, location details, and more. They aptly identify challenges like node heterogeneity, open environments, and the complexities of multiparty resource sharing. Of particular note is their emphasis on the unresolved research issue of policy conflicts arising from diverse authorizations and multiparty dynamics [9].

Shruti et al., on the other hand, turned their gaze towards the world of attribute-based encryption (ABE) within the IoT paradigm. With the IoT realm now intertwined with cloud and fog computing, the need for robust security measures is paramount. Through their research, the criticality of ABE emerges, a mechanism offering granular control coupled with flexibility. They provided valuable insights into various ABE schemes, drawing attention to the fact that while some ABE solutions might shine in certain performance aspects, no single model is the gold standard across every performance indicator. This lends weight to the importance of contextual selection of ABE schemes based on the precise needs of specific IoT applications [10].

Shifting the focus broader still, Ragothaman et al. offer an extensive survey on designing access control solutions for

the IoT. With the IoT characterized by its diverse range of devices, resource constraints, and heterogeneity, it's evident that a one-size-fits-all approach is far from viable. Their paper makes a compelling argument for the importance of dynamic policy specifications and presents an intricate tapestry of access control requirements critical for the IoT's security. They underscore that while a multitude of access control models for the IoT have been postulated, the search for a universally applicable model remains ongoing [11].

At the intersection of blockchain and IoT, Butun and Österberg present an analysis of the potential of blockchain systems to bolster the security layers of IoT networks. The decentralized nature of blockchain introduces a new set of challenges for traditional access control systems. Their paper emphasizes the importance of scalability and interoperability within blockchain-based IoT applications, pushing the narrative towards the need for lightweight consensus algorithms and a comprehensive understanding of system behavior from a cybersecurity vantage. They strongly advocate for permissioned Blockchain Systems (BCSs) for IoT platforms due to data volume considerations, emphasizing the necessity of a hybridized access control system [12].

Collectively, these studies illuminate the multifaceted world of access control within the IoT ecosystem. While each offers unique insights, the overarching narrative underscores the importance of tailored access control models to navigate the complexities of the IoT landscape.

Building upon this extensive body of work, we present a review titled ''A Comprehensive Systematic Review of Access Control in IoT: Requirements, Technologies, and Evaluation Metrics'' that aims to synthesize the diverse streams of research into a coherent narrative. While preceding studies have presented insights into particular dimensions of access control within the IoT environment, this evaluation sticks out in its comprehensive technique to the issue. By integrating the numerous perspectives, it offers a panoramic view of the requirements, the present-day technologies presently employed, and the metrics used for assessment. Furthermore, this article addresses gaps identified in previous literature and proposes a more holistic framework for understanding access control in the IoT realm. The systematic methodology employed ensures that the review captures a wide spectrum of research, making it an invaluable resource for researchers, industry experts, and policymakers eager to navigate the intricate world of IoT access control.

III. METHODOLOGY

A systematic literature review (SLR) is a protocol in which researchers conduct a review of specific studies using a systematic process. The process begins with predefined research questions and keywords, followed by a search strategy, selection of studies, and analysis of the selected studies to evaluate the impact of the research. The objective of this systematic literature review is to examine and assess the current research on access control technologies for IoT systems. The review follows the guidelines for systematic literature reviews in software engineering areas as set and described in [13].

SLR is a methodology that provides the reader with a complete description of the review's steps. The methodology starts by defining the research questions to determine a specific target before proceeding to the next step. Inclusion and exclusion criteria are then determined as filters for the initial search results. The selection process for the relevant articles is discussed in detail. This methodology provides the reader with a comprehensive understanding of the research process, including information on the final selected articles. Figure 1 illustrates the steps involved in the review.

A. RESEARCH QUESTION

The following are the research questions (RQs) definitions for the proposed review:

RQ1. What are the distinct requirements for access control in IoT environments compared to traditional systems, and how have these needs evolved with the growth and diversification of IoT applications?

RQ2. Which technologies and methodologies have been proposed or adopted for access control in IoT, and what are their advantages, limitations, and applicability in various IoT scenarios?

RQ3. How are the effectiveness and robustness of access control mechanisms in IoT evaluated in the literature, and what are the commonly accepted metrics and benchmarks?

B. SEARCH AND SELECTION PROCESS

The search process is conducted rigorously and accurately to ensure all relevant papers are found, and no potentially helpful study is missed. The most well-known libraries are Scopus and Web of Science (WOS). We built the search query by defining the main keywords using Boolean operators. The final search query is:

("Internet of Things" OR IoT) AND ("access control") AND (requirements OR challenges OR comparison OR "technologies" OR methodologies OR methods OR solutions OR model OR framework OR evaluation OR estimation OR metrics OR "performance measurement" OR "evaluation criteria" OR effectiveness OR robustness)

C. INCLUSION AND EXCLUSION CRITERIA

Inclusion and exclusion criteria were set to achieve this review's goals: i) to answer research questions, and ii) to ensure an efficient review as a result.

Inclusion Criteria: Studies written in the English language, relevant to the research questions, scientific, peer-reviewed, and published between 2019 and 2023.

Exclusion Criteria: Studies focusing solely on protocols, architecture, or device access control, and articles that are not fully accessible to researchers.

TABLE 1. List of retrieved studies with their type and year of publication.

Paper ID	Citation	Publication Type	Year of publication	Cited by	Paper ID	Citation	Publication Type	Year of publication	Cited by
1	[14]	Article	2021	11	49	[15]	Conference	2019	3
2	[16]	Article	2021	9	50	[17]	Conference	2019	21
3	[18]	Article	2021	9	51	[19]	Conference	2019	15
4	[20]	Article	2021	8	52	[21]	Conference	2019	10
5	[22]	Article	2021	9	53	[23]	Article	2019	26
6	[24]	Article	2021	-	54	[25]	Article	2019	29
7	[26]	Article	2021	41	55	[27]	Article	2019	289
8	[28]	Article	2021	10	56	[29]	Article	2022	4
9	[30]	Article	2021	11	57	[31]	Article	2021	4
10	[32]	Article	2021	13	58	[33]	Article	2021	91
11	[34]	Article	2021	46	59	[35]	Article	2022	27
12	[36]	Conference	2021	3	60	[37]	Article	2023	-
13	[38]	Article	2021	3	61	[39]	Article	2022	1
14	[40]	Article	2021	19	62	[41]	Conference	2019	1
15	[42]	Article	2021	7	63	[43]	Article	2020	22
16	[44]	Article	2021	25	64	[45]	Conference	2020	1
17	[46]	Article	2021	10	65	[47]	Article	2022	
18	[48]	Article	2020	18	66	[49]	Article	2022	-
19	[50]	Conference	2020	4	67	[51]	Conference	2020	-
20	[52]	Conference	2020	3	68	[53]	Article	2022	4
21	[54]	Conference	2020	40	69	[55]	Article	2023	20
22	[56]	Conference	2020	1	70	[57]	Article	2022	1
23	[58]	Conference	2020	15	71	[59]	Article	2019	7
24	[60]	Conference	2020	16	72	[61]	Article	2022	13
25	[62]	Conference	2020	-	73	[63]	Conference	2022	-
26	[64]	Conference	2020	13	74	[65]	Article	2019	35
27	[66]	Conference	2020	38	75	[67]	Article	2022	6
28	[68]	Conference	2020	1	76	[69]	Article	2023	3
29	[70]	Conference	2020	5	77	[71]	Article	2023	-
30	[72]	Conference	2020	53	78	[73]	Article	2023	4
31	[74]	Conference	2020	46	79	[75]	Article	2023	13
32	[76]	Conference	2020	7	80	[77]	Conference	2022	-
33	[78]	Article	2020	45	81	[79]	Article	2020	14
34	[80]	Article	2020	6	82	[81]	Article	2021	13
35	[82]	Conference	2020	7	83	[83]	Conference	2020	1
36	[84]	Article	2020	30	84	[85]	Article	2021	9
37	[86]	Article	2020	7	85	[87]	Conference	2022	-
38	[88]	Article	2020	2	86	[89]	Conference	2020	17
39	[90]	Conference	2019	29	87	[91]	Article	2020	10
40	[92]	Conference	2019	4	88	[93]	Conference	2019	1
41	[94]	Conference	2019	63	89	[95]	Article	2019	29
42	[96]	Article	2019	52	90	[97]	Article	2021	20
43	[98]	Article	2019	28	91	[99]	Article	2020	13
44	[100]	Conference	2019	3	92	[101]	Article	2020	7
45	[102]	Conference	2019	6	93	[103]	Conference	2021	2
46	[104]	Article	2019	33	94	[105]	Article	2022	-
47	[106]	Conference	2019	9	95	[107]	Article	2023	-
48	[108]	Article	2023	3	96	[109]	Article	2023	3

D. ANALYSIS OF RESULTS

Figure 2 illustrates the number of annual publications and citations related to IoT Access Control from 2015 to 2023 (data sourced from Scopus and WoS as of 15/9/2023), highlighting the growing interest and importance of this research area. The selected studies equal to 96 studies 58 are journal articles and 36 are conference publication, Figure 3 shows the types of the selected studies. Where Table 1 showing the list of selected studies, including years published, type article or conference, and the times each study is cited.

IV. DISCUSSION

Access control in the IoT is one of the hottest topics facing many challenges as an essential issue in IoT security. This paper can be a starting point for understanding and exploring research ideas about access control in the Internet of Things. This section will discuss the selected publications from the research question's point of view.

RQ1: What are the distinct requirements for access control in IoT environments compared to traditional systems, and how have these needs evolved with the growth and diversification of IoT applications?

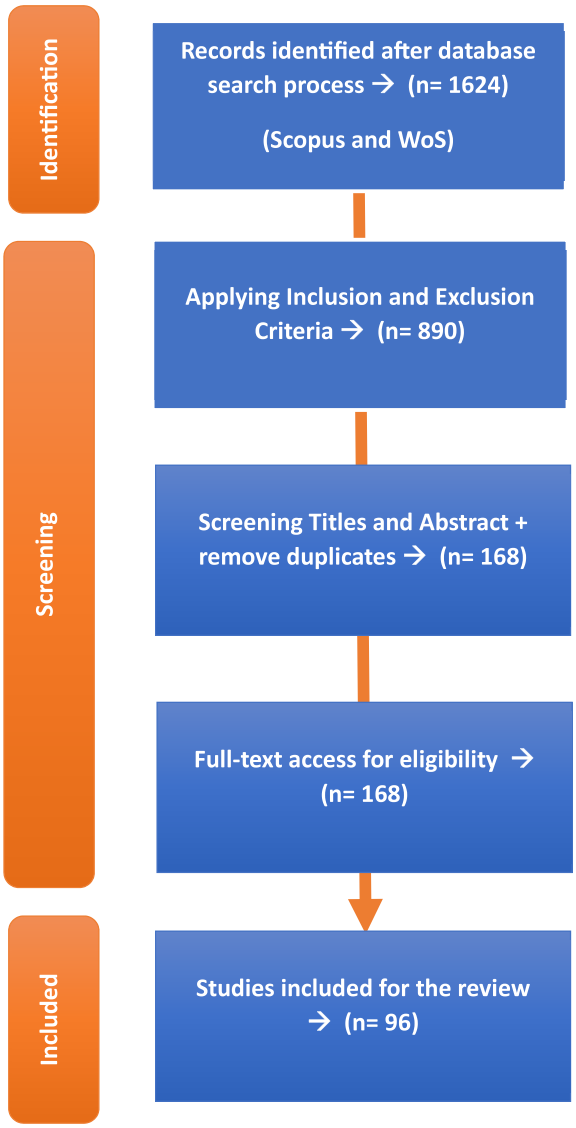

FIGURE 1. The steps involved in the review.

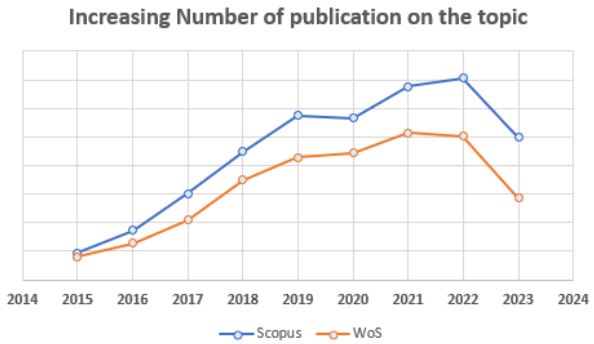

FIGURE 2. The number of annual publications and citations.

Exploring and testing the selected studies based on the requirements is the first step to achieving the best access control solution in any system. There are many ways to list the important requirements. In our case, we have chosen

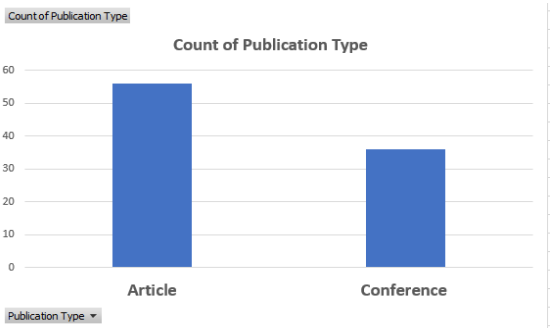

FIGURE 3. Selected studies types (Article or Conference).

to base our requirements on the survey in [110], where the leading access control requirements were elicited based on the IoT requirements and IoT application requirements. In this study, we will use the listed access control requirements to identify whether the available access control models satisfy the requirements or not.

As mentioned in [110], three main categories were specified:

A. POLICY SPECIFICATIONS

1) FINE-GRAINED ACCESS CONTROL

In the intricate landscape of IoT, the granularity of access control plays a pivotal role. Fine-grained access control revolves around detailed and specific rules or conditions that determine how resources within an IoT environment are accessed. It offers a high level of precision and specificity in setting access parameters, ensuring only authorized entities, under specific conditions, can interact with an IoT device or its data. The study [64] introduces 'Bloccess,' a reliable fine-grained access control mechanism rooted in blockchain technology, designed to instill trust in inherently distrusted environments. The architecture of Bloccess, with its user-centric focus, can be effortlessly incorporated into existing systems. Bloccess supports adaptable fine-grained access control implementation, which can be defined without restrictions. Another study, [56], proposes a solution based on fine-grained requirements – a layered IoT-based secure access control model. This model facilitates: i) Fine-grained control over patient health data, allowing role-specific users to access cloud-stored health data based on their access permissions. ii) Mapping of health device nodes into virtual objects in the cloud. Users can remotely control the statuses of these virtualized devices based on their rights. The scheme has proven to be effective, secure, and efficient through theoretical analysis and experiments. Researchers in [16] explained that traditional solutions tend to offer blanket access, or they are overly reliant on cloud backends, which affects granular access, scalability, and robustness. This research introduces ''Heracles'', an IoT access control system designed to provide fine-grained, scalable access control. It is built on a 3-tier structure that balances centralized policy with decentralized execution. The study

[51] introduces the use of SDN technology in the IoT realm to enable network control and forwarding separation, making it easier to handle access controls in this dynamic environment. The authors have designed a method to facilitate granular access control in IoT devices using SDN. The approach allows detailed specifications regarding which devices can access what, under what conditions, and when. A testing platform is constructed, combining Mininet simulation with an industrial wireless system. The results highlight that the designed access control can effectively filter unauthorized accesses based on several parameters like device source, action requests, and access timing.

2) CONTEXT-AWARE ACCESS CONTROL

Equally crucial is the system's ability to be context-aware. Access control decisions that are context-aware adjust based on the surrounding environment or the state of a user or device. Such a system takes into account factors like location, time, device status, and even environmental conditions, which enables dynamic and relevant security measures. This ensures that access controls aren't just static rules but can adapt in real-time to provide appropriate **security** based on the situation. The study [93] proposes implementing an access control policy for each node in the IoT network using context awareness, ensuring that only genuine nodes have access to network resources. The access control policy is set for each node in the IoT network using context awareness, ensuring only genuine nodes have access to network resources. In contrast, [92] proposed Enhanced context-aware capability-based access control model. This model integrates context-based authentication and access control, aiming to achieve scalability and flexibility in a distributed environment like IoT. The model employs Elliptic Curve Cryptography (ECC) for authentication, which provides a secure way to ensure the identity of entities within the IoT network.

B. POLICY ADMINISTRATION

1) HANDLING IoT DYNAMICITY

IoT ecosystems are inherently dynamic, with devices frequently joining or leaving the network or changing states. An access control system needs to effectively handle this dynamicity to maintain optimal security. It should be capable of adapting to these changes without compromising security or functionality, thus ensuring that as the IoT ecosystem evolves, security measures remain robust. The study [68] addresses the challenge in existing communication systems that require a robust trust mechanism. Establishing security and thwarting potential malicious activities, especially by users with high-risk behaviors, are prime concerns. The researchers proposed a technique that aims to curtail malevolent activities by closely observing user behavior through smart contracts. The foundation of this approach is blockchain technology, which ensures trust and verification of user possessions. The solution's infrastructure is primarily divided into two sections: the smart contract itself and an authentication system protocol. The paper highlights the importance of blockchain technology and smart contracts in establishing trust and security. The immutable nature of blockchain ensures that once a transaction is recorded, it cannot be altered. This provides a layer of trust and transparency. Simultaneously, smart contracts automate and enforce the contract's terms, ensuring that users adhere to the stipulated behavior or face repercussions.

2) USABILITY

While security is paramount, the ease of use for end-users and administrators cannot be ignored. The usability of an access control mechanism denotes how user-friendly and intuitive it is. Balancing security with ease of use ensures that while the environment remains secure, stakeholders can effectively manage and interact with access controls without facing undue complexities. Usability is an urgent need in some IoT applications, such as smart homes, as demonstrated in [52]. While the paper introduces a fine-grained and highly secure model, it also acknowledges potential challenges related to usability, especially for home IoT users who might find such detailed access controls overwhelming. The paper introduces a compelling extension to the ABAC model, considering the unique challenges posed by the IoT environment. By integrating authentication scores and advocating for functionality-based access controls, the study presents a robust solution to some of the most pressing security concerns in IoT. However, its real-world application, especially in terms of usability and integration with platforms like Azure IoT, remains an area for future exploration. The study sets a promising direction for further research in refining and implementing these models in actual IoT environments. In contrast, the study [30] focuses specifically on usability. It introduces a trust management scheme that leverages the Markov chain, acknowledging the evolving nature of IoT devices.''. This is particularly crucial in countering the security challenges arising due to the potential vulnerabilities of IoT devices. The prototype system, deployed on Ethereum for testing purposes, indicated that the scheme can efficiently provide secure, high-throughput, and adaptable access control for IoT. It is adept at resisting network misbehaviors and attacks. The system ensures detailed authorization by evaluating a broad spectrum of factors, thus improving usability by catering to specific device and environment needs. The usability is further enhanced by integrating access policies with smart contracts, ensuring both flexibility and security. To counteract the challenges posed by the ever-changing attributes of IoT devices, the trust management scheme is incorporated. This not only enhances security but also ensures that devices can be trusted and accessed without continuous re-evaluation, thus improving usability.

3) POLICY MANAGEMENT

Central to policy administration is the systematic control of who can do what. Policy management offers tools and processes that allow for the definition, deployment, and updating of access control policies across IoT devices. This

centralization ensures consistent security enforcement across all devices, regardless of their roles or functions within the network. The study [75] provides a detailed insight into the multiple challenges associated with IoT management and access control, emphasizing the need for enhanced security protocols. It provides a detailed insight into the multiple challenges associated with IoT management and access control, emphasizing the need for enhanced security protocols. The proposed approach to integrating both SDN and blockchain offers a comprehensive solution to a majority of the challenges associated with IoT access control and management.

4) AUTOMATED DECISIONS

With the scale of IoT networks, manual oversight for each access request is impractical. The capability for automated decision-making, where the system can autonomously grant or deny access based on predefined rules, speeds up access processes and minimizes human errors. This efficiency ensures that devices and users receive timely access permissions as needed. Almost all studies addressed this requirement, underscoring its particular importance in the context of IoT. The paper [73] introduces the crypto-currency-based access control model (CcBAC), which utilizes blockchain technology and is supported by the Trusted Execution Environment (TEE). This model seeks to resolve existing challenges by providing fine-grained access, strong auditability, and efficient access procedure control. By incorporating blockchain technology, the CcBAC model leverages the inherent benefits of decentralization and tamper resistance. This decentralized ledger ensures that access control policies are transparent and cannot be altered without detection. Instead of relying on centralized decision-making mechanisms, CcBAC uses smart contracts on the blockchain to automate policy decisions. This makes the decision process and its outcomes both transparent and verifiable.

5) REDUCING OVERHEAD ON IoT CONSTRAINED DEVICES

Many IoT devices operate with limited computational and memory resources. As such, it's crucial to design access controls that are lightweight and don't exert undue strain on these devices. By reducing overhead, these devices can operate efficiently without compromising on security. One of the studies that covers this requirement is [54], the article introduces an innovative trust-aware continuous authorization architecture specifically designed for the consumer Internet of Things (IoT) sector, such as Smart Homes. At its core, the architecture is built to tackle the overhead challenges frequently encountered in constrained IoT devices. The system seamlessly integrates trust-level assessments into the authorization rules and policies. This integration is achieved by fusing an Attribute-Based Access Control (ABAC) authorization engine with a Trust-Level-Evaluation-Engine (TLEE). This fusion ensures that policies are assessed without putting undue pressure on the device's computational resources. The architecture employs a microservices-inspired approach, optimizing performance by leveraging publish/subscribe protocols. This ensures maximum concurrency between various processes, such as policy parsing and attribute value retrieval. The benefit here is twofold: it maximizes system performance and minimizes reliance on high computational resources or low network latency.

C. POLICY EVALUATION AND ENFORCEMENT

1) PERFORMANCE

As IoT often involves real-time operations, the performance of the access control system becomes vital. This refers to the system's efficiency in processing requests and enforcing policies promptly. Any significant delay can impede the functionality of the device or system, so ensuring quick and effective access decisions is paramount for optimal IoT operations. Almost all implemented solutions were tested to ensure their performance, the following is an example: in the study [84], the BacS system, utilizing blockchain technology, addresses the pivotal need for performance in Distributed IoT. By emphasizing unified identity management through the node's account address and incorporating lightweight encryption, BacS offers an innovative approach to access control mechanisms. This not only bolsters data integrity but also augments system responsiveness, a crucial element for retaining user trust and propelling the adoption of IoT applications. The intricate relationship between performance and blockchain solutions becomes evident in shaping the future of IoT access control through BacS.

2) INTEROPERABILITY

Given the diverse range of devices, communication protocols, and software platforms in IoT, interoperability is non-negotiable. An access control system must function seamlessly across this varied ecosystem, promoting integration and consistent security measures irrespective of the device brand or platform. The study [95] proposes an interoperable access control framework for diverse Internet of Things (IoT) platforms, focusing on enhancing the current access control methods. The proposed approach uses an Interoperable Access Token (IAT) which simplifies permission management. The framework has been implemented on two open-source IoT platforms: Mobius and FIWARE. Where in [71], the emphasis is placed on the vital need for advanced cross-domain access control mechanisms within the Industrial Internet of Things (IIoT) to foster secure and efficient cross-domain interactions and resource-sharing amongst varying system departments integral to smart manufacturing. To address the interoperability requirement and the inherent challenges in achieving seamless interactions between diverse and heterogeneous systems in IIoT, the article proposes a decentralized, scalable primary-secondary chain structure, offering solutions beyond the conventional centralized and single-chain blockchain models. This proposed structure ensures enhanced security and reliability through a reputation-based node selection mechanism and introduces a nuanced access control method, amalgamat-

ing roles and attributes for high granularity, catering to the specific necessities of IIoT environments. A grouping strategy-based matching algorithm is also presented to refine the efficiency in attribute strategy matching, with experimental validations showcasing an 82% improvement in throughput over single-chain models. The concluding remarks pinpoint potential future directions, highlighting the incorporation of machine learning for intelligent access control enhancements and optimizations tailored to the diverse nature of IoT environments, focusing on overcoming network latency and ensuring unified management in access control systems.

3) AVAILABILITY

the resilience and reliability of the IoT access control system are gauged by its availability. Even in the face of failures, attacks, or adverse conditions, authorized users and devices should be able to access the necessary resources. Ensuring such availability means designing the system to be robust and adaptable, safeguarding continuous and reliable access when needed. From an availability perspective, the presented secure integrated framework in [14] for Fog-IoT systems is designed to enhance the resilience and uninterrupted functioning of Fog-IoT deployments. Fog-IoT systems, being set up in remote areas, are susceptible to a range of attacks, including insider threats and various external attacks like Denial of Service (DoS) and Distributed DoS. This framework integrates two vital components: the security component (SC) and the trust management component (TMC). SC's role is to maintain data confidentiality, integrity, authentication, and authorization, while TMC assesses the dependability of Fog-IoT entities based on a trust model grounded in Quality of Service (QoS) metrics and other performance indicators. Significantly, trust is embedded as an attribute in SC's access control policies, ensuring that only those entities with proven trustworthiness can access fog resources. The integration of these components aims to thwart potential disruptions, thereby ensuring consistent access to resources and maintaining the availability of Fog-IoT systems. Evaluations using the Raspberry Pi 3 Model B+ further confirm the lightweight nature of the proposed framework, indicating its suitability for resource-constrained environments and underlining its capability to sustain Fog-IoT system availability effectively. Another solution in the paper [19] presents a distributed fog-based access control architecture tailored for the healthcare domain, particularly focusing on IoT-driven medical services. Recognizing the vulnerabilities associated with centrally managed access controls, especially in healthcare where timely access to data is crucial, the proposed model decentralizes access control functions. By distributing policy decision-making and information mechanisms to the edges of the network, closer to the end nodes, the model effectively reduces latency and augments system availability. Thus, the key advantage of this architecture is the enhancement of data accessibility for authorized users, while concurrently ensuring the security of patients' data. The importance of these benefits is underscored by the authors' future intentions to further implement and evaluate this architecture using the XACML standard.

4) SCALABILITY

Lastly, scalability in IoT access control is paramount due to the exponential growth and interconnected nature of IoT devices. As the number of devices, users, and services in the IoT ecosystem multiply, the access control system must be able to efficiently manage an ever-increasing volume of access requests, permissions, and policy changes without compromising on performance or security. Without scalability, as the network expands, there may be delays in access decisions, bottlenecks in communication, or even potential vulnerabilities. Hence, a scalable access control mechanism ensures that as the IoT environment evolves and expands, it continues to provide timely, secure, and efficient access management across all devices and services. From a scalability perspective, the article [71] underlines the necessity of a highly scalable cross-domain access control model for the evolving Industrial Internet of Things (IIoT) landscape. The IIoT's shift from a traditional model to a multi-department, cross-domain data-sharing paradigm emphasizes the inadequacy of existing access control systems. Traditional centralized schemes, while efficient, are susceptible to single-point failures, and current blockchain-based models, predominantly single-chain structures, lack the scalability essential for the demands of the IIoT. To address this, the research introduces a decentralized primary-secondary chain access model, boasting enhanced scalability. Experimental results spotlight its superiority, showing an 82% surge in throughput compared to the single-chain models. This primary-secondary chain structure not only exhibits improvements in scalability but also augments throughput and reduces latency. The article concludes by highlighting the need for more expansive experiments and potential future optimizations, emphasizing scalability's indispensable role in IoT access control.

In Figure 4 illustrates the extent of interest in access control requirements within IoT, as shown by the selected studies. The automated decision requirement is the highest covered requirement with 96%, where IoT dynamicity, fine-grained, and performance in the next level with 48%, 44%, and 40% in the same order. The two requirements: availability and reduced overhead have the same percentage of 27%, followed by policy management and context-awareness with 25% and 22% in the same order. The lowest interest was in interoperability and usability with 10% for each. Table 2 shows each requirement categorization, description, importance and occurrence in the selected studies. Figure 5 shows the taxonomy of access control requirements in IoT context. These requirements were collected from selected studies.

In response to RQ2: 'Which technologies and methodologies have been proposed or adopted for access control in IoT, and what are their advantages, limitations, and applicability in various IoT scenarios?' we found that various technologies,

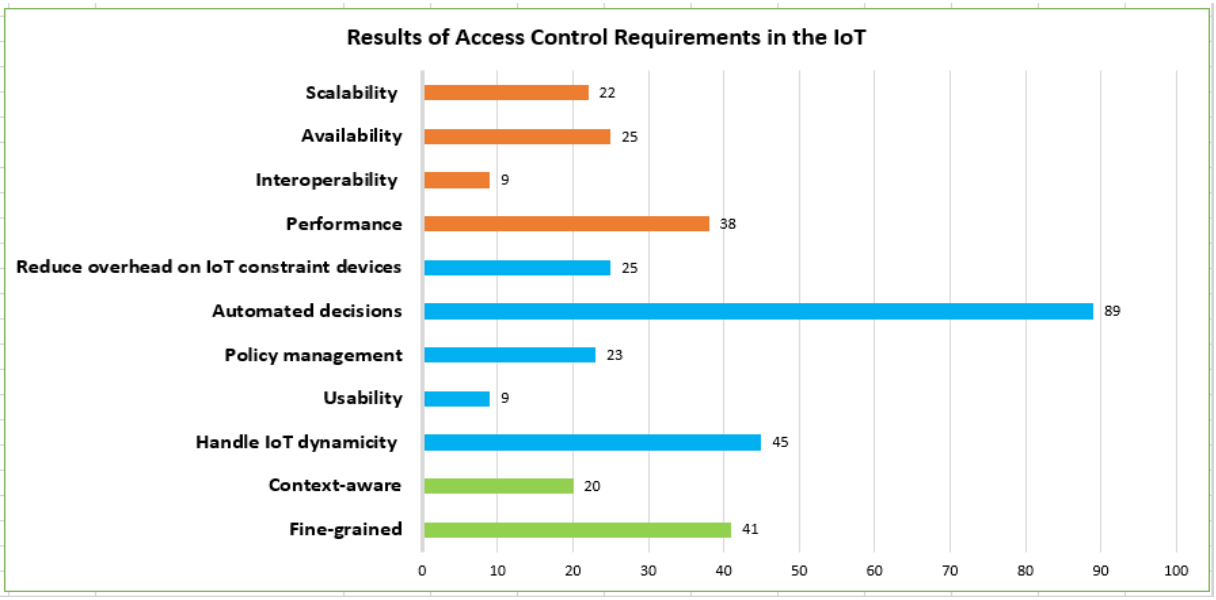

FIGURE 4. Summary of the requirements results.

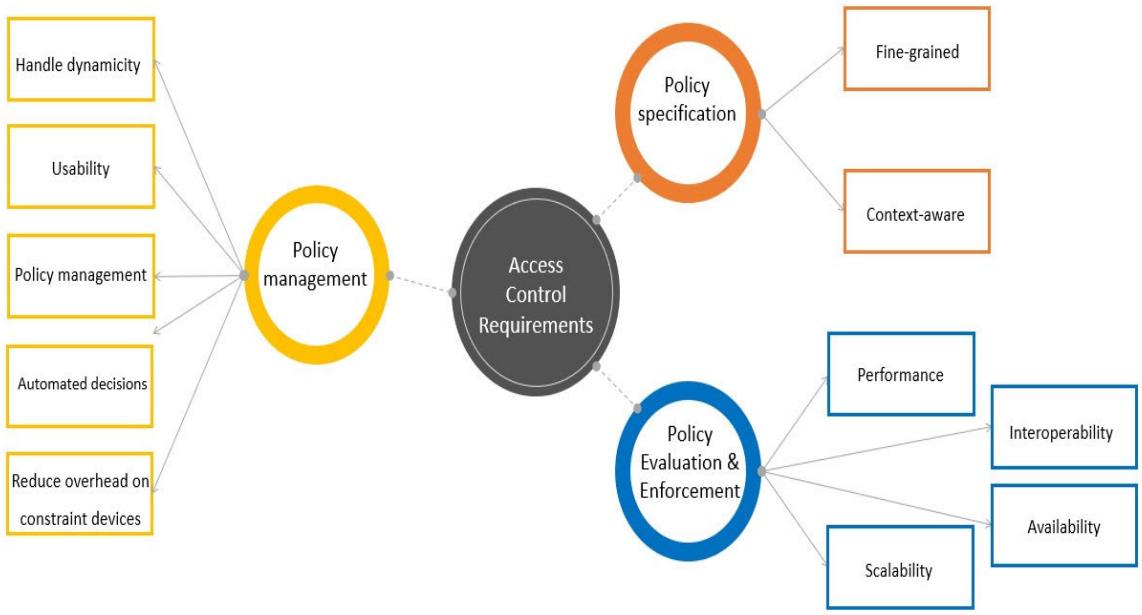

FIGURE 5. Taxonomy of access control requirements in IoT context.

models, and architectures are used to build access control models within the IoT framework. The most commonly applied access control model type was ABAC (33%), followed by RBAC (10%) and CBAC (3%). Blockchain (31%), cloud-based (14%), and edge computing (3%) were the most common technologies used. Two types of IoT architectural styles were reported: distributed IoT architecture (40%) and centralized architecture style (25%). The highest communication protocol is MQTT with a rate of (10%). The access control data format was either XACML (10%) or JSON (10%). Finally, we found that 55% of the access control models were in the theoretical or design phases, while (45%) were developed as simulations or prototypes, and evaluated to prove the effectiveness and robustness of the proposed models.

5) ACCESS CONTROL MODELS

1. Role-Based Access Control (RBAC): This model assigns roles to users, with permissions associated with roles rather than individual users, thereby simplifying management in large-scale environments. In [79],

TABLE 2. Analysis of existing models in the selected studies for IoT access control requirements.

Requirement Category	Requirement	Description	Importance	Study Ref.
Policy specification	Fine-grained	About the detailed and specific nature of rules or conditions.	Enhances precision and specificity in access control.	[14-16, 19, 20, 22-24, 26, 28-30, 33, 34, 36-40, 46, 47, 49, 51, 52, 55, 56, 58, 61, 63, 64, 66, 67, 70, 71, 73, 74, 78, 80, 90, 96, 98, 108]
	Context-aware	Adjusting access decisions based on the surrounding environment, user, or device state.	Ensures dynamic and relevant security measures.	[15, 17, 23, 25, 27, 28, 31, 34, 37-39, 51, 52, 54, 61, 65, 66, 68, 70, 73, 92]
Policy Administration	Handle IoT dynamicity	The ability to adapt to the frequent changes in IoT environments such as device addition, removal, or state change	Maintains security in ever-changing IoT ecosystems.	[15, 17, 18, 21, 22, 24, 25, 27, 29, 30, 33-39, 43, 46, 49, 51, 52, 54, 55, 57, 59-63, 65-69, 71-75, 78, 80, 84, 88, 106, 107] [108] [109]
	Usability	How user-friendly and intuitive access control mechanisms are for end-users and administrators.	Balances security with ease-of-use.	[30, 34, 35, 44, 50, 52, 70, 73, 75]
	Policy management	Tools and processes to define, deploy, and update access control policies across IoT devices.	Centralizes and streamlines security rule sets.	[14, 24, 26, 29, 30, 32, 34-37, 39, 49, 51, 55, 57, 59, 61, 65, 67, 69, 71, 73, 75] [107] [108]
	Automated decisions	The capability of the system to make access control decisions without human intervention based on predefined rules.	Speeds up access processes and reduces human errors. IoT devices can grant or deny access based on set rules, reducing the need for manual oversight.	[14-40, 42-46, 49-62, 64-76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104-107] [108]
	Reduce overhead on IoT constraint devices	Minimizing the computational and memory demands on devices with limited resources when enforcing access controls. Designing lightweight access controls that don't strain small IoT devices.	Ensures efficient operation of resource-constrained devices.	[14, 19, 20, 23, 27, 30, 32-35, 46, 50, 51, 54, 55, 58, 63, 67, 69, 70, 72, 82, 86, 94, 96] [109]
Policy Evaluation and Enforcement	Performance	How efficiently an access control system processes requests and enforces policies without introducing significant delays. An effective system ensures quick access decisions without affecting device operations.	Guarantees timely responses, crucial for real-time IoT operations.	[14, 16, 18, 22, 28-37, 39-43, 46, 47, 53-55, 57-59, 62, 67, 70-73, 75, 80, 84, 92, 105, 107] [108] [109]
	Interoperability	The ability of the access control system to work seamlessly across diverse devices, protocols, and platforms in the IoT ecosystem.	Promotes integration in varied IoT environments.	[17, 31-33, 45, 59, 70, 71, 94] [95]
	Availability	Ensuring that authorized users and devices can access IoT resources when needed, even in the face of failures or attacks. Designing the system to be resilient, so that IoT devices and data remain accessible even under adverse conditions.	Prevents service disruptions and ensures reliable access.	[14, 19, 24, 27, 28, 30-32, 35, 37, 41, 42, 45, 46, 49, 50, 53, 54, 62, 64, 65, 67, 69, 71, 73, 94]
	Scalability	Scalability in IoT access control means the system's ability to handle a growing number of devices and users efficiently without compromising security or performance.	it maintains optimal performance despite increased access requests and upholds stringent security measures.	[71] [101] [89] [55] [88] [80] [58] [48] [92] [42] [38] [28] [24] [22] [61] [57] [80] [50] [41] [37] [33] [31] [109]

The article introduces the ‘‘Role-based Reputed Access Control (RRAC)’’ method, tailored for Intelligent IoT platforms to address the challenges presented by malicious risks. This method is rooted in the Role-Based

Access Control (RBAC) model but extends its capabilities. RRAC works in two dimensions: an internal adaptive certificate authentication, which ensures that communications between users and resources are authentic, and an external security feature, which focuses on facilitating secure service discovery and user selection. The essence of the RRAC method is to enhance the reliability of IoT communications. Each IoT device's role is ascertained by its reputation, gauged by the service provider (SP). This SP evaluates a device's communication behaviors to determine its reputation. A notable feature is the system's ability to filter out unreliable devices that present inaccurate reputation data. To fortify the security of communications among recognized devices, the article incorporates linear hashing and hyperelliptic curve-based digital signatures. The method's effectiveness was validated through experiments, which showed that RRAC not only boosts malicious activity detection rates but also reduces false positives, misdetection, and detection times, leading to a more secure and efficient IoT communication environment.

2. Attribute-Based Access Control (ABAC): Determines access rights based on attributes (e.g., device type, location, time) allowing for fine-grained and dynamic access decisions. One study that worked on an ABAC model is [61]. The article introduces the HABACa model, an attribute-based access control system designed for smart-home IoT setups. Focusing on capturing diverse attributes such as user, environment, operation, and device characteristics, HABACa leverages a dynamic, fine-grained Attribute-Based Access Control (ABAC) approach. Its functionality and applicability were demonstrated through use-case scenarios and a proof-of-concept implementation in Amazon Web Services. The researchers also conducted a comparative analysis between HABACa and EGRBAC, an existing role-based access control model tailored for smart-home IoT. This comparison involved converting the specifications of each model into the other to assess their respective expressiveness. While EGRBAC effectively managed relatively static attributes, it struggled with dynamic attributes. On the other hand, HABACa had challenges in preventing specific future authorizations.
3. Based on a thorough theoretical comparison against established criteria for access control models, the paper concludes that a combined, or hybrid, model that integrates features of both HABACa and EGRBAC might be the optimal choice for IoT-enabled smart homes and likely other broader applications.
4. Capability-Based Access Control (CBAC): Devices or users are given tokens or "capabilities" that explicitly state their access rights. The article [92] addresses the security and privacy challenges prevalent in the heterogeneous IoT environment, especially in healthcare. As the medical sector increasingly adopts IoT for patient health data sharing and analysis, ensuring reliable authentication and access control becomes imperative. The paper introduces the Enhanced Context-Aware Capability-based Access Control (ECCAPAC) model, which integrates Elliptic Curve Cryptography for robust authentication. This model augments the existing Capability-based access control by integrating a trust value into the capability tag or token. This trust value is derived from the social relationship, emphasizing the importance of understanding the connections in a distributed environment. Moreover, the ECCAPAC model focuses on resilience, which is crucial given the healthcare sector's susceptibility to crypto attacks. Upon comparison with the standard Role-based Access Control (RBAC) model, ECCAPAC not only prioritizes context by assessing an object's trust value based on relevance and node importance but also proves to be more efficient in terms of security analysis and computation time. The findings suggest that the ECCAPAC model offers a more resilient and socially-aware access control mechanism for IoT in healthcare, paving the way for further enhancements in context evaluation and semantic relationships between entities.

6) ACCESS CONTROL ARCHITECTURE STYLE

Access control in IoT can be implemented in one of these two types of architectural styles: Centralized and Distributed architecture. The first is the centralized model, where a single authority or server manages access permissions. While this offers a streamlined control mechanism, it may introduce scalability and single-point failure issues. Conversely, the decentralized approach distributes the control across nodes or devices, enhancing scalability but potentially complicating policy enforcement and consistency. Peer-to-peer models, another notable style, enable devices to communicate and decide access controls directly amongst themselves without a central entity, fostering flexibility and resilience. Meanwhile, hierarchical structures, often seen in industrial IoT, organize devices into layered tiers, where superior levels manage and dictate access controls for the levels beneath them. Furthermore, hybrid models, combining features from multiple architectural styles, are also emerging to harness the strengths and mitigate the weaknesses of each style, ensuring adaptive, scalable, and efficient IoT access control.

The article [16] introduces "Heracles", a fine-grained access control system tailored for large-scale enterprise environments with numerous smart objects and users. Unlike conventional solutions that tend to offer limited access control granularity and often rely heavily on cloud backends, Heracles offers a more efficient and robust access control mechanism. This system utilizes a three-tier architectural design, emphasizing centralized policy formulation while still permitting distributed execution, making it apt for enterprise settings. Heracles operates through secure, unforgeable tokens which describe user authorizations for object access. These tokens pave the way for users to access IoT devices quickly and securely without the need for cloud intervention.

Notably, Heracles showcases substantial advantages in reducing updating overhead, particularly when there are frequent changes in user memberships and policies. In performance evaluations, the system demonstrated impressive responsiveness, especially in accessing objects within proximity. Thus, through its centralized policy approach combined with the capability to perform distributed execution, Heracles stands out as a viable solution for enterprise-scale IoT access control needs. The model presented in the paper [53] proposes an advanced Industrial Internet-of-Things (IIoT) architecture tailored for smart manufacturing. This layered architecture leverages the benefits of both Blockchain technology (BCT) and Machine Learning (ML) and is strategically structured into five distinctive layers: sensing, network/protocol, transport (reinforced with BCT components), application, and advanced services such as BCT data, ML, and cloud-based functionalities. One of the chief benefits of integrating BCT is the capability to efficiently accumulate sensor access control data. On the other hand, ML is employed to bolster the architecture's defence against a variety of potential cyberattacks, ranging from Denial of Service (DoS) and Distributed Denial of Service (DDoS) to cross-site scripting (XSS) and brute force attacks, by utilizing various classifiers to distinguish between regular and malicious activities. In the practical evaluation of the architecture, using the TON_IoT dataset, it was evident that combining the power of Blockchain's smart contracts with ML classifiers can considerably mitigate multiple types of cyberattacks, specifically highlighting significant reductions in the occurrences of DDoS, injection, brute force, and XSS attacks. This innovative approach not only champions the advantages of decentralized access control in IIoT networks but also showcases the potential of distributed technologies in enhancing security measures in smart manufacturing scenarios.

7) ACCESS CONTROL AUTHORIZATION ARCHITECTURE

1. Policy-Based Access Control (PBAC) makes decisions based on predefined policies. These policies are set by administrators and dictate who can do what, and under which conditions. It's not just about the identity of the user (like in traditional Role-Based Access Control) but takes into account various contextual information such as location, time, type of device, etc. Policy-based access control can be highly advantageous because of the diverse nature of devices, their operations, and the varied contexts in which they operate. For instance, a smart thermostat might be adjusted by a homeowner from a smartphone but might reject requests from other devices if they're outside of certain geolocations or if the request comes outside of typical operating hours. The article [96] is an important example of policy-based access control. The paper introduces an access control architecture tailored for constrained healthcare resources within the IoT context. Rooted in a policy-based approach, it zeroes in on a fine-grained access mechanism, where authorized users are permitted to services, simultaneously safeguarding vital resources from any unauthorized intrusion. The architecture adopts a unique hybrid stance, interweaving attributes, roles, and capabilities for its authorization model.

2. Token-Based Access Control (TBAC) revolves around the use of tokens – cryptographic entities that prove the identity and permissions of a user or device. The user/device has to present a valid token to get access to a resource. These tokens are usually issued by a trusted authority after proper authentication. In the world of IoT, where there are numerous devices with varying levels of security, tokens can be a way to ensure that only devices with valid tokens can access certain resources. For example, a smart door lock might only unlock if it receives a signal accompanied by a valid token. This can prevent unauthorized devices or hackers from easily gaining control over IoT devices. Furthermore, tokens can be set to expire, offering temporary access, or can be quickly revoked if a device is believed to be compromised. In [31] a description of a solution that emerges to bridge this cross-domain connection is the delegation of access rights. However, with the diverse security constraints across IoT domains, crafting a one-size-fits-all authorization protocol proves challenging. Instead, specific carriers, like the OAuth token or the secret URL of IFTTT, are employed to grant users authorization capabilities within their IoT domain. This process allows these users to independently decide if they wish to transfer these access rights to users in other domains, often in situations demanding immediate or convenient response, termed as cross-domain delegation. For instance, a patient might delegate the access rights of his wearable ECG monitor to family members or caregivers. Another example could be a homeowner providing firefighters the capability to unlock smart doors during emergencies like fires, signifying an ad hoc right delegation. Utilizing such delegation mechanisms reduces the decision-making burden on trusted central servers. More importantly, this method aligns with the inherent decentralized and dynamic nature of IoT, positioning it as an essential feature for expansive IoT setups.

8) BLOCKCHAIN ACCESS CONTROL

Recently, there has been a surge in the application of blockchain technology for enhancing security and privacy. A defining feature of blockchain is its decentralized architecture. Various literature categorizes blockchain-based access control into two primary methods: transaction-centric and smart contract-centric access control. Transactions can be employed to allocate, delegate, or withdraw access privileges. On the other hand, smart contracts assess access petitions and arrive at decisions grounded on the guidelines set by the resource holder. Regardless of the method, an access token is produced and handed to the individual requesting access, symbolizing the permission to access. A notable drawback of the transaction-centric model is its dependency on a central node for making access decisions. Conversely, the smart contract-centric model might introduce significant overhead due to the need for contract establishments between nodes [27], [64], [67], [68].

TABLE 3. Analysis of existing models for IoT based on access control technologies.

Property	Technologies	Studies
AC model	ABAC	[17, 19, 24, 26-30, 34-37, 39, 46, 48, 49, 52, 54, 55, 57, 58, 61, 62, 66, 67, 69, 74, 80, 82, 88, 90, 100] [108] [109]
	RBAC	[38, 43, 45, 61, 71, 79, 104, 106]
	CBAC	[23, 70, 92]
Access Control Authorization Architecture	Policy-based	[14] [16] [17] [18] [19] [20] [21] [22] [23] [24] [26] [27] [28] [29] [30] [32] [34] [35] [37] [38] [39] [44] [46] [48] [49] [50] [52] [54] [55] [57] [58] [59] [61] [62] [63] [64] [66] [67] [69] [72] [73] [74] [75] [76] [78] [80] [82] [84] [86] [88] [90] [92] [96] [98] [100] [102] [106] [108] [109]
	Token-based	[31] [36] [51] [95] [40] [108]
Deployment	Blockchain	[22] [23] [26] [27] [28] [29] [30] [31] [32] [33] [35] [36] [37] [40] [44] [46] [48] [49] [50] [52] [53] [55] [57] [58] [64] [67] [68] [69] [71] [72] [84] [109]
	Cloud	[34, 48, 52, 54, 56, 66, 70, 74, 78, 88, 94, 98, 105] [108]
	Edge	[109]
	Fog-based	[14, 19, 60]
IoT Architectural Style	Centralized	[14-16, 18, 20, 21, 34, 39, 42, 43, 45-48, 51, 52, 54, 56, 61, 63, 70, 82, 102, 104, 105] [108]
	Distributed	[17, 22, 23, 26-32, 35-38, 40, 44, 49, 50, 53, 55, 58, 59, 64, 66, 68, 69, 71-73, 75, 78, 80, 84, 86, 88, 90, 92, 94, 96, 98] [109]
Communication Protocol	MQTT	[26, 34, 35, 44, 50, 53, 61, 74, 94, 96]
	HTTP	[34, 50, 53, 58]
	CoAP	[44, 50, 53, 94]
	Modbus protocol	[41]
Data Format	JSON	[28, 31, 33-35, 41, 58, 61, 73, 78]
	XACML	[19, 49, 52, 54, 59, 64, 76, 88, 96]

Figure 6 shows the access control technologies that can be used in the IoT context, with these technologies collected from the selected studies. Where Table 3 provides the information about technologies and the sources from selected studies as well.

For RQ3, 'How are the effectiveness and robustness of access control mechanisms in IoT evaluated in the literature, and what are the commonly accepted metrics and benchmarks?' the question comprises two parts: the first being 'How are the effectiveness and robustness of access control mechanisms in IoT evaluated in the literature?' and the second, 'What are the commonly accepted metrics and benchmarks?'. In addressing this research question, we discovered several evaluation metrics. The most widely used in the literature include:

- Response Time: defined as the time taken for the system to respond to a particular request or action. 43% of the selected articles used this metric. This metric can be calculated as $RT = t_{response} - t_{request}$.
- Delay: Defined as the time taken to transfer or process data or messages. Although similar to Latency, it can be more general or context-specific. This metric was used in 9% of the selected articles.
- Throughput: Defined as the number of successful messages or operations processed per unit of time. This metric was utilized in 8% of the selected articles.

These are the most commonly used metrics found in the literature. Other metrics are listed in Table 4, along with their definitions and calculation methods.

V. ACCESS CONTROL TAXONOMY

In Figure 6, we provide a comprehensive taxonomy of access control technologies used within the Internet of Things (IoT) context, organized into several key categories that reflect the multi-dimensional nature of IoT systems.

A. MODELS

- Attribute-Based Access Control (ABAC): This model grants access rights based on attributes associated with users, resources, and the environment, providing a high level of granularity and control.

- Role-Based Access Control (RBAC): Access rights are grouped by role names, and permissions are associated with roles rather than individuals, simplifying management across numerous users.

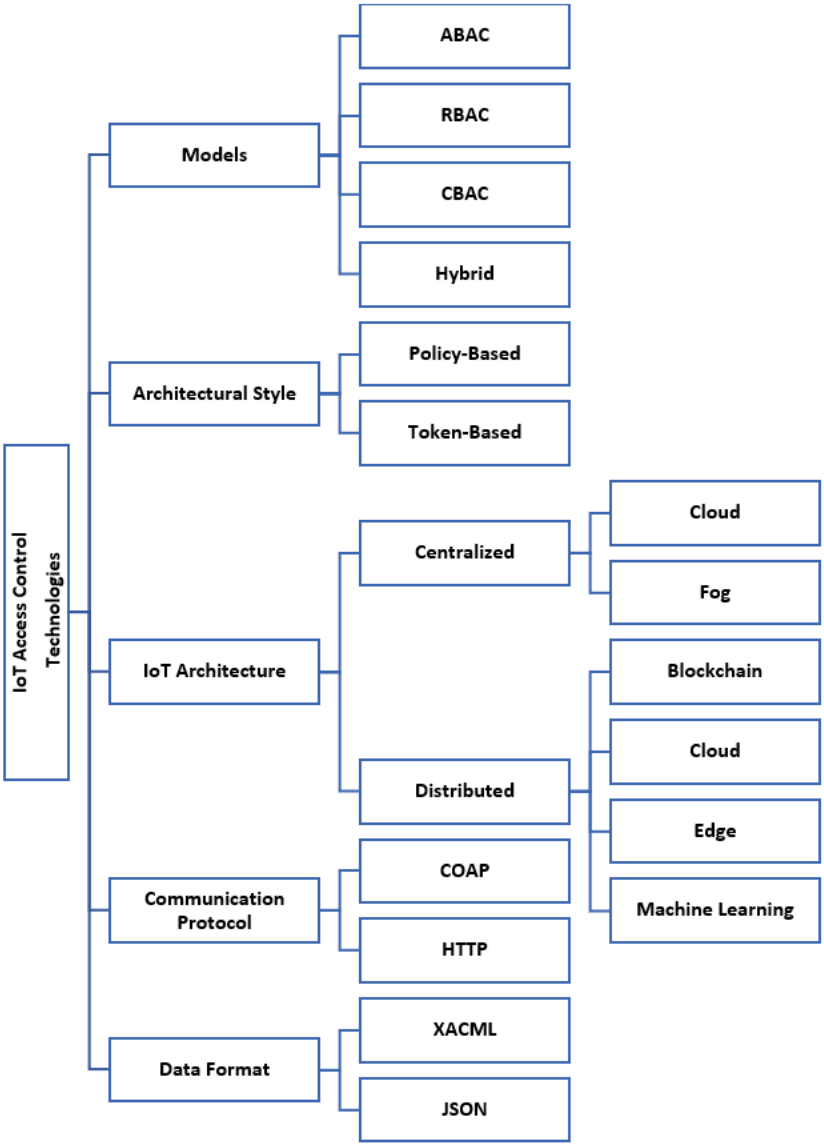

FIGURE 6. Taxonomy of access control technologies needed in IoT context.

- **Capability-Based Access Control (CBAC):** It uses tokens or keys, granting capabilities for access, often used in distributed systems where direct authorization from a central authority is impractical.

- Hybrid: A combination of two or more access control models to leverage the benefits of each and provide a more comprehensive control mechanism.

B. ARCHITECTURAL STYLE

- Policy-Based: The access control is driven by policies defined by the organization, which can be dynamically adapted to changing circumstances.

- Token-Based: Access is granted based on possession of a token that provides certain rights, akin to capabilities in CBAC.

C. IoT ARCHITECTURE

- Centralized: All decision-making processes are handled by a central authority, which could be cloud-based, providing a centralized point for managing access controls.

- Distributed: Decision-making is spread across multiple nodes, which can include edge computing devices, improving scalability and reliability.

- Cloud: Utilizes cloud computing resources to manage access control, offering scalability and resource efficiency.

- Fog: A decentralized computing infrastructure in which data, compute, storage, and applications are located somewhere between the data source and the cloud.

- Blockchain: Utilizes blockchain technology for a decentralized and secure method of managing access controls, with an immutable record of transactions and policies.

TABLE 4. Evaluation metrics that are used in the tested models.

Metrics	Definition	Equation	References
Response Time	The time is taken for the system to respond to a particular request or action.	RT=tresponse−trequest	[14] [16] [18] [20] [22] [28] [30] [34] [36] [40] [46] [54, 80] [92] [48] [31] [33] [35] [37] [39] [47] [55] [57] [59] [61] [65] [67] [73] [105]
Access Success Rate	The percentage of successful access attempts to the total attempts.	$\frac{Successful\ Accesses}{Total\ Access\ Attempts} \times 100\%$	[80] [41]
Policy Updating and Revoking	Time or resources needed to update or revoke access policies.	Usually qualitative; sometimes measured in seconds or computational steps.	[48]
Delay	The time taken to transfer or process data or messages. Similar to Latency but can be more general or context-specific.	$D=t_{received}-t_{sent}$	[72] [29] [35] [43] [57] [71] [75] [105]
Energy or memory Consumption	Amount of energy or memory used during the access control operations.	Measured in Joules (for energy) or Bytes (for memory).	[18] [42] [47]
Average Number of Exchanged Messages	The average number of messages exchanged during access control procedures.	Simple average over a given period or set of operations.	[16] [32]
Throughput	The number of successful messages or operations processed per unit of time.	Typically measured in operations/second or Mbps.	[28] [84] [33] [35] [57] [71] [75] [109]
Storage overhead	Additional storage requirements are introduced by the access control mechanism.	Measured in Bytes or percentage increase.	[84] [31] [33] [67]
Computation overhead	Extra computational effort is due to access control mechanisms compared to a system without such mechanisms.	Qualitative or quantitative measures, such as extra CPU cycles.	[70] [84] [31] [33]
Smart Contract Evaluation	The performance, efficiency, and correctness of executing smart contracts in access control.	Qualitative assessment or time taken for contract execution.	[22] [58] [72]
Reputation Evolution	Changes in the reputation of a device or entity over time-based on its behavior or performance in the system.	Typically, a score or rank that update over time.	[72]
Accuracy	How correctly the access control mechanism makes decisions compared to a desired or known standard.	$\frac{Correct\ Decisions}{Total\ Decision} \times 100\%$	[62] [39] [53]
Number of attributes	The number of attributes or properties considered during access control decision-making.	Simple count of utilized attributes.	[20] [29] [107]

D. COMMUNICATION PROTOCOL

- Constrained Application Protocol (COAP): A specialized web transfer protocol for use with constrained nodes and networks in the IoT.

- Hypertext Transfer Protocol (HTTP): A widely used protocol for data communication on the World Wide Web, which can also be employed in IoT contexts.

E. DATA FORMAT

- eXtensible Access Control Markup Language (XACML): A declarative access control policy language implemented in XML and a processing model, describing both the access control policies and the request/response decision protocol.

- JavaScript Object Notation (JSON): A lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse and generate, often used for APIs in web services and IoT devices.

Each category in this taxonomy represents a critical choice point in the design of an IoT access control system, affecting scalability, security, complexity, and administrative overhead. By mapping out these categories, the taxonomy provides

a structured framework for understanding the landscape of access control technologies and their application in IoT scenarios.

VI. CONCLUSION AND FUTURE WORKS

This study conducts a comprehensive systematic review of access control in IoT, with focusing on requirements, technologies, and evaluation Metrics. In conclusion, access control in the realm of IoT stands as a foundation stone for ensuring the secure and continuous operation of the massive web of interconnected devices. A significant insight drawn from our analysis is the transition from traditional access control models like RBAC to more dynamic and granular models such as ABAC and CBAC. As IoT continues to be embedded into various domains – from smart homes to healthcare – the need for context-aware, attribute-centric, and capability-based models is ever-apparent. Technologies like edge computing, and cloud computing, while being instrumental in enhancing these models, also bring forth new challenges in terms of performance and scalability. It's noteworthy that while a rise of access control models for IoT exists, most are in the theoretical or design phases, with fewer making it to the prototype or evaluation stage. The many of architectural styles, from centralized to decentralized models, reflects the evolving nature of IoT's dynamic ecosystem. Techniques such as Policy-Based Access Control and Token-Based Access Control offer tailored solutions to address specific challenges faced by IoT devices in diverse contexts. Furthermore, the arrival of blockchain technology has introduced novel means to enhance the decentralization, transparency, and trustworthiness of access control mechanisms. The evaluation metrics, including response time, delay, and throughput, provide quantifiable measures that assist in gauging the effectiveness and robustness of these mechanisms. Finally, we listed requirements, technologies and evaluation metrics based on our findings, which can serve as a roadmap for the next level of research in this field.

For future work, there are many areas to explore, including scalability and interoperability, real-time adaptability, and economic considerations, especially when using blockchain technology, integration with emerging technologies is a need, such as AI-driven access control, and not to forget the need for real-world implementations. Because after theoretical models and simulations, the field could benefit from real-world implementations and evaluations of access control systems in diverse IoT deployments. Such evaluations can offer practical insights and highlight unexpected challenges for further driving innovation.

Additionally, it is essential to examine the specific needs and the relevant technologies pertinent to IoT applications. This detailed analysis will enable us to determine which solutions are most suitable for the varied scenarios presented by IoT deployments. For instance, while a particular feature may be fundamental for the functionality of smart homes, it might be less critical for smart cities, and possibly irrelevant for smart transportation systems. For example, consider the necessity of real-time data processing. In a smart home environment, real-time processing is crucial for systems like intrusion detection, where an immediate response is necessary. However, for a smart city infrastructure, while real-time data is important, some applications such as long-term urban planning can work with data that is not processed in real-time. In contrast, for smart transportation, especially in autonomous vehicles, real-time data processing is not just a convenience but an absolute necessity for safety and operational efficiency.

ACKNOWLEDGMENT

The authors would like to thank the support of student Michal Dobrovolny in consultations regarding application aspects.

REFERENCES

[1] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, "Internet of Things and edge cloud computing roadmap for manufacturing," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 66–73, Jul. 2016.

[2] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and challenges," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, Dec. 2014.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[4] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (ABAC) definition and considerations," Nat. Inst. Standards Technol. (NIST) Special Publication, Tech. Rep. 800-162, pp. 1–54, 2014.

[5] J. A. Ibañez-Ramírez and F. D. A. López-Fuentes, "Authentication mechanism to access multiple-domain multimedia data," in *Proc. 11th Int. Conf. Multimedia Netw. Inf. Syst. (MISSI)*. Wroclaw, Poland: Springer, 2018.

[6] E. Bertin, D. Hussein, C. Sengul, and V. Frey, "Access control in the Internet of Things: A survey of existing approaches and open research questions," *Ann. Telecommun.*, vol. 74, nos. 7–8, pp. 375–388, Aug. 2019.

[7] J. S. Park, R. Sandhu, and G.-J. Ahn, "Role-based access control on the web," *ACM Trans. Inf. System Secur.*, vol. 4, no. 1, pp. 37–71, 2001.

[8] R. Sandhu and J. Park, "Usage control: A vision for next generation access control," in *Computer Network Security*. Berlin, Germany: Springer, 2003.

[9] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.

[10] Shruti, S. Rani, D. K. Sah, and G. Gianini, "Attribute-based encryption schemes for next generation wireless IoT networks: A comprehensive survey," *Sensors*, vol. 23, no. 13, p. 5921, Jun. 2023.

[11] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access control for IoT: A survey of existing research, dynamic policies and future directions," *Sensors*, vol. 23, no. 4, p. 1805, Feb. 2023.

[12] I. Butun and P. Österberg, "A review of distributed access control for blockchain systems towards securing the Internet of Things," *IEEE Access*, vol. 9, pp. 5428–5441, 2021.

[13] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," School Comput. Sci. Math., Keele Univ., Keele, U.K., Tech. Rep. EBSE-2007-01, 2007.

[14] A. K. Junejo, N. Komninos, and J. A. McCann, "A secure integrated framework for fog-assisted Internet-of-Things systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6840–6852, Apr. 2021.

[15] D. Genç, E. Tomur, and Y. M. Erten, "Context-aware operation-based access control for Internet of Things applications," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Jun. 2019, pp. 1–6.

[16] Q. Zhou, M. Elbadry, F. Ye, and Y. Yang, "Towards fine-grained access control in enterprise-scale Internet-of-Things," *IEEE Trans. Mobile Comput.*, vol. 20, no. 8, pp. 2701–2714, Aug. 2021.

[17] S. Dramé-Maigné, M. Laurent, and L. Castillo, "Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 1582–1587.

[18] M. U. Aftab, A. Oluwasanmi, A. Alharbi, O. Sohaib, X. Nie, Z. Qin, and S. T. Ngo, "Secure and dynamic access control for the Internet of Things (IoT) based traffic system," *PeerJ Comput. Sci.*, vol. 7, p. e471, May 2021.

[19] S. Alnefaie, A. Cherif, and S. Alshehri, "Towards a distributed access control model for IoT in healthcare," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–6.

[20] L. Zhang, J. Wang, and Y. Mu, "Privacy-preserving flexible access control for encrypted data in Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 19, pp. 14731–14745, Oct. 2021.

[21] N. Kashmar, M. Adda, M. Atieh, and H. Ibrahim, "A new dynamic smart-AC model methodology to enforce access control policy in IoT layers," in *Proc. IEEE/ACM 1st Int. Workshop Softw. Eng. Res. Practices Internet Things (SERP4IoT)*, May 2019, pp. 21–24.

[22] B. Chai, B. Yan, J. Yu, and G. Wang, "BHE-AC: A blockchain-based high-efficiency access control framework for Internet of Things," *Pers. Ubiquitous Comput.*, vol. 26, no. 4, pp. 971–982, Aug. 2022.

[23] S. K. Pinjala and K. M. Sivalingam, "DCACI: A decentralized lightweight capability based access control framework using IOTA for Internet of Things," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 13–18.

[24] V. V. Kimbahune, P. N. Mahalle, S. K. Pathan, and S. Naser, "Distributed access control scheme for machine-to-machine communication in IoT using trust factor," in *Security Issues and Privacy Threats in Smart Ubiquitous Computing*, P. N. Mahalle, et al., Eds. Singapore: Singapore, 2021, pp. 131–144.

[25] H. F. Atlam, R. J. Walters, G. B. Wills, and J. Daniel, "Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT," *Mobile Netw. Appl.*, vol. 26, no. 6, pp. 2545–2557, Dec. 2021.

[26] A. Iftekhar, X. Cui, Q. Tao, and C. Zheng, "Hyperledger fabric access control system for Internet of Things layer in blockchain-based applications," *Entropy*, vol. 23, no. 8, p. 1054, Aug. 2021.

[27] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[28] F. Sabrina and J. Jang-Jaccard, "Entitlement-based access control for smart cities using blockchain," *Sensors*, vol. 21, no. 16, p. 5264, Aug. 2021.

[29] J. Han, Y. Zhang, J. Liu, Z. Li, M. Xian, H. Wang, F. Mao, and Y. Chen, "A blockchain-based and SGX-enabled access control framework for IoT," *Electronics*, vol. 11, no. 17, p. 2710, Aug. 2022.

[30] P. Wang, N. Xu, H. Zhang, W. Sun, and A. Benslimane, "Dynamic access control and trust management for blockchain-empowered IoT," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 12997–13009, Aug. 2022.

[31] C. Li, F. Li, L. Yin, T. Luo, and B. Wang, "A blockchain-based IoT cross-domain delegation access control method," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Sep. 2021.

[32] R. Saha, G. Kumar, M. Conti, T. Devgun, T.-H. Kim, M. Alazab, and R. Thomas, "DHACS: Smart contract-based decentralized hybrid access control for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3452–3461, May 2022.

[33] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green Internet of Things," *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–20, Aug. 2021.

[34] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-based access control for AWS Internet of Things and secure industries of the future," *IEEE Access*, vol. 9, pp. 107200–107223, 2021.

[35] Y. Feng, W. Zhang, X. Luo, and B. Zhang, "A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2840–2848, Apr. 2022.

[36] L. Song, Z. Zhu, M. Li, L. Ma, and X. Ju, "A novel access control for Internet of Things based on blockchain smart contract," in *Proc. IEEE 5th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, vol. 5, Mar. 2021, pp. 111–117.

[37] H.-A. Pham, N. N. Do, and N. Huynh-Tuong, "A fine-grained access control model with enhanced flexibility and on-chain policy execution for IoT systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, 2023.

[38] H. B. Djilali, D. Tandjaoui, and H. Khemissa, "Enhanced dynamic team access control for collaborative Internet of Things using context," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 5, May 2021.

[39] R. Qiu, X. Xue, M. Chen, J. Zheng, S. Jing, and Y. Li, "A fine-grained dynamic access control method for power IoT based on kformer," *Infocommunications J.*, vol. 14, no. 4, pp. 79–85, 2022.

[40] L. Song, X. Ju, Z. Zhu, and M. Li, "An access control model for the Internet of Things based on zero-knowledge token and blockchain," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–20, Dec. 2021.

[41] S. Chi, S. Bi, M. Dong, B. Sun, and C. Xie, "A high-performance access control model for urban street lamp Internet of Things," in *Proc. IEEE Int. Conf. Real-time Comput. Robot. (RCAR)*, Aug. 2019, pp. 632–637.

[42] S. Sakthivel and G. Vidhya, "A trust-based access control mechanism for intra-sensor network communication in Internet of Things," *Arabian J. Sci. Eng.*, vol. 46, no. 4, pp. 3147–3153, Apr. 2021.

[43] M. U. Aftab, Y. Munir, A. Oluwasanmi, Z. Qin, M. H. Aziz, Zakria, N. T. Son, and V. D. Tran, "A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles," *IEEE Access*, vol. 8, pp. 24196–24208, 2020.

[44] Y. E. Oktian and S.-G. Lee, "BorderChain: Blockchain-based access control framework for the Internet of Things endpoint," *IEEE Access*, vol. 9, pp. 3592–3615, 2021.

[45] M. Bisma, F. Azam, Y. Rasheed, and M. W. Anwar, "A model-driven framework for ensuring role based access control in IoT devices," in *Proc. 6th Int. Conf. Comput. Artif. Intell.*, Apr. 2020.

[46] R. Zhang, G. Liu, S. Li, Y. Wei, and Q. Wang, "ABSAC: Attribute-based access control model supporting anonymous access for smart cities," *Secur. Commun. Netw.*, vol. 2021, Mar. 2021, Art. no. 5531369.

[47] Q. Zhang, Y. Li, C. Zheng, L. Zhu, J. Yuan, and S. Hu, "A permission-combination scalable access control model for Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 4, p. e4060, Apr. 2022.

[48] Q. Zhang, H. Zhong, J. Cui, L. Ren, and W. Shi, "AC4AV: A flexible and dynamic access control framework for connected and autonomous vehicles," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1946–1958, Feb. 2021.

[49] J. Wang, P. Gong, H. Wang, W. Zhang, C. Sun, and B. Zhao, "A right transfer access control model of Internet of Things based on smart contract," *Secur. Commun. Netw.*, vol. 2022, pp. 1–11, May 2022.

[50] A. Prabhakar and T. Anjali, "A novel on-demand trust-based access control framework for resource-constrained IoT system," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2020, pp. 1–6.

[51] M. Wei, E. Liang, and Z. Nie, "A SDN-based IoT fine-grained access control method," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Barcelona, Spain, Jan. 2020, pp. 637–642.

[52] M. Burakgazi Bilgen and K. Bicakci, "Extending attribute-based access control model with authentication information for Internet of Things," in *Proc. Int. Conf. Inf. Secur. Cryptol. (ISCTURKEY)*, Dec. 2020, pp. 48–55.

[53] H. Mrabet, A. Alhomoud, A. Jemai, and D. Trentesaux, "A secured industrial Internet-of-Things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing," *Appl. Sci.*, vol. 12, no. 9, p. 4641, May 2022.

[54] T. Dimitrakos, T. Dilshener, A. Kravtsov, A. La Marra, F. Martinelli, A. Rizos, A. Rosetti, and A. Saracino, "Trust aware continuous authorization for zero trust in consumer Internet of Things," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1801–1812.

[55] W. Jiang, Z. Lin, and J. Tao, "An access control scheme for distributed Internet of Things based on adaptive trust evaluation and blockchain," *High-Confidence Comput.*, vol. 3, no. 1, 2023, Art. no. 100104.

[56] C. Huang, Z. Zhang, J. Huang, and F. Chen, "Fine-grained device and data access control of community medical Internet of Things," in *Proc. 16th Int. Conf. Mobility, Sens. Netw. (MSN)*, Dec. 2020, pp. 236–243.

[57] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "An attribute-based access control model for Internet of Things using hyperledger fabric blockchain," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–25, Jul. 2022.

[58] A. Qashlan, P. Nanda, and X. He, "Security and privacy implementation in smart home: Attributes based access control and smart contracts," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 951–958.

[59] S. El Bouanani, M. A. El Kiram, O. Achbarou, and A. Outchakoucht, "Pervasive-based access control model for IoT environments," *IEEE Access*, vol. 7, pp. 54575–54585, 2019.

[60] M. Wazid, M. S. Obaidat, A. K. Das, and P. Vijayakumar, "SAC-FIIoT: Secure access control scheme for fog-based industrial Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.

[61] S. Ameer, J. Benson, and R. Sandhu, "An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach," *Information*, vol. 13, no. 2, p. 33, Jan. 2022.

[62] Y. Zhao, M. Su, J. Wan, J. Hou, and D. Mei, "A novel scheme for access control policy generating and evaluating in IoT based on machine learning," in *Proc. Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData) IEEE Congr. Cybermatics (Cybermatics)*, Nov. 2020, pp. 411–418.

[63] H. Peng, Y. Chen, X. Li, and Z. Shi, "An efficient and dynamic data access control framework for IoT," in *Proc. 2nd Int. Conf. Internet Things Smart City (IoTSC*. SPIE. vol. 12249. SPIE, 2022.

[64] Y. Ding and H. Sato, "Bloccess: Towards fine-grained access control using blockchain in a distributed untrustworthy environment," in *Proc. 8th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Aug. 2020, pp. 17–22.

[65] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for risk-based access control model for IoT," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100052.

[66] S. Bhatt and R. Sandhu, "ABAC-CC: Attribute-based access control and communication control for Internet of Things," in *Proc. 25th ACM Symp. Access Control Models Technol. (SACMAT)*. Barcelona, Spain: Association for Computing Machinery, 2020, pp. 203–212.

[67] P. Zhai, J. He, and N. Zhu, "Blockchain-based Internet of Things access control technology in intelligent manufacturing," *Appl. Sci.*, vol. 12, no. 7, p. 3692, Apr. 2022.

[68] B. S. Ali, Y. Singh, P. K. Singh, and M. Simona Raboaca, "Dynamic access control in IoT: Monitoring user behavior using smart contracts," in *Proc. 12th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jun. 2020, pp. 1–6.

[69] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, "A blockchain-inspired attribute-based zero-trust access control model for IoT," *Information*, vol. 14, no. 2, p. 129, Feb. 2023.

[70] N. Sivaselvan, W. Asif, B. K. Vivekananda, and M. Rajarajan, "Authentication and capability-based access control: An integrated approach for IoT environment," in *Proc. 12th Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jun. 2020, pp. 110–117.

[71] Z. Zhang, X. Wu, and S. Wei, "Cross-domain access control model in industrial IoT environment," *Appl. Sci.*, vol. 13, no. 8, p. 5042, Apr. 2023.

[72] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trust management in decentralized IoT access control system," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–9.

[73] W. Jiang, E. Li, W. Zhou, Y. Yang, and T. Luo, "IoT access control model based on blockchain and trusted execution environment," *Processes*, vol. 11, no. 3, p. 723, Feb. 2023.

[74] D. Gupta, S. Bhatt, M. Gupta, O. Kayode, and A. S. Tosun, "Access control model for Google cloud IoT," in *Proc. IEEE 6th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform. Smart Comput., (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2020, pp. 198–208.

[75] M. Khalid, S. Hameed, A. Qadir, S. A. Shah, and D. Draheim, "Towards SDN-based smart contract solution for IoT access control," *Comput. Commun.*, vol. 198, pp. 1–31, Jan. 2023.

[76] L. A. Charaf, I. Alihamidi, A. Addaim, and A. A. Madi, "A distributed XACML based access control architecture for IoT systems," in *Proc. 1st Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET)*, Apr. 2020, pp. 1–5.

[77] X. Shen, P. Zhang, and Y. Zhang, "Research on access control decision model of Internet of Things based on attribute exploration," in *Proc. Int. Conf. Signal Process. Commun. Technol. (SPCT)*, Apr. 2022.

[78] A. Thakare, E. Lee, A. Kumar, V. B. Nikam, and Y.-G. Kim, "PARBAC: Priority-Attribute-Based RBAC model for azure IoT cloud," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2890–2900, Apr. 2020.

[79] M. Amoon, T. Altameem, and A. Altameem, "RRAC: Role based reputed access control method for mitigating malicious impact in intelligent IoT platforms," *Comput. Commun.*, vol. 151, pp. 238–246, Feb. 2020.

[80] J. Wang, H. Wang, and H. Zhang, "A trust and attribute-based access control framework in Internet of Things," *Int. J. Embedded Syst.*, vol. 12, no. 1, pp. 116–124, 2020.

[81] S. Nakamura, T. Enokido, and M. Takizawa, "Time-based legality of information flow in the capability-based access control model for the Internet of Things," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 23, p. e5944, Dec. 2021.

[82] H. Ouechtati, N. B. Azzouna, and L. B. Said, "A fuzzy logic based trust-ABAC model for the Internet of Things," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.*, in Advances in Intelligent Systems and Computing," 2020, pp. 1157–1168.

[83] D. H. Hussein, R. Anbarasu, A. Matrawy, and M. Ibnkahla, "Towards a decentralized access control system for IoT platforms based on blockchain technology," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–6.

[84] N. Shi, L. Tan, C. Yang, C. He, J. Xu, Y. Lu, and H. Xu, "BacS: A blockchain-based access control scheme in distributed Internet of Things," *Peer-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2585–2599, Sep. 2021.

[85] A. Kousalya, K. Sakthidasan, and A. Latha, "Reliable service availability and access control method for cloud assisted IoT communications," *Wireless Netw.*, vol. 27, no. 2, pp. 881–892, Feb. 2021.

[86] A. Outchakoucht, A. Abou, H. Es-Samaali, and S. Benhadou, "Machine learning based access control framework for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 331–340, 2020.

[87] Q. Xiong, "Reinforcement learning based access control architecture of Internet of Things big data peak clustering model," in *Proc. Int. Conf. Signal Process. Commun. Secur. (ICSPCS)*, vol. 12455. SPIE, 2022, pp. 1–8.

[88] F. Sifou, F. AlShahwan, M. Marwan, A. Hammoud, and A. Hammouch, "Implementing policy rules in attributes based access control with XACML within a cloud-enabled IoT environment," *J. Commun.*, vol. 15, no. 1, pp. 107–114, Jan. 2020.

[89] R. Nakanishi, Y. Zhang, M. Sasabe, and S. Kasahara, "IOTA-based access control framework for the Internet of Things," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 87–95.

[90] M. Yutaka, Y. Zhang, M. Sasabe, and S. Kasahara, "Using ethereum blockchain for distributed attribute-based access control in the Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[91] A. K. Malik, N. Emmanuel, S. Zafar, H. A. Khattak, B. Raza, S. Khan, A. H. Al-Bayatti, M. O. Alassafi, A. S. Alfakeeh, and M. A. Alqarni, "From conventional to state-of-the-art IoT access control models," *Electronics*, vol. 9, no. 10, p. 1693, Oct. 2020.

[92] J. Ahamed and F. Khan, "An enhanced context-aware capability-based access control model for the Internet of Things in healthcare," in *Proc. 6th HCT Inf. Technol. Trends (ITT)*, 2019, pp. 126–131.

[93] A. Kaur, I. Batra, and A. Bakshi, "An intelligent context aware based access control framework to prevent attacker nodes in Internet of Things," in *Proc. 4th Int. Conf. Comput. Sci. (ICCS)*, Aug. 2018, pp. 218–227.

[94] H. Al Breiki, L. Al Qassem, K. Salah, M. Habib Ur Rehman, and D. Sevtinovic, "Decentralized access control for IoT data using blockchain and trusted oracles," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Nov. 2019, pp. 248–257.

[95] S.-R. Oh, Y.-G. Kim, and S. Cho, "An interoperable access control framework for diverse IoT platforms based on OAuth and role," *Sensors*, vol. 19, no. 8, p. 1884, Apr. 2019.

[96] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, "Policy-based access control for constrained healthcare resources in the context of the Internet of Things," *J. Netw. Comput. Appl.*, vol. 139, pp. 57–74, Aug. 2019.

[97] Z. Li, J. Hao, J. Liu, H. Wang, and M. Xian, "An IoT-applicable access control model under double-layer blockchain," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 6, pp. 2102–2106, Jun. 2021.

[98] Q. Li, H. Zhu, J. Xiong, R. Mo, Z. Ying, and H. Wang, "Fine-grained multi-authority access control in IoT-enabled mHealth," *Ann. Telecommun.*, vol. 74, nos. 7–8, pp. 389–400, Aug. 2019.

[99] A. Alkhresheh, K. Elgazzar, and H. S. Hassanein, "DACIoT: Dynamic access control framework for IoT deployments," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11401–11419, Dec. 2020.

[100] I. Ray, R. Abdunabi, and R. Basnet, "Access control for Internet of Things applications," in *Proc. 5th ACM Cyber-Phys. Syst. Secur. Workshop, Co-Located With AsiaCCS*, 2019, pp. 35–36.

[101] A. Pozo, Á. Alonso, and J. Salvachúa, "Evaluation of an IoT application-scoped access control model over a publish/subscribe architecture based on FIWARE," *Sensors*, vol. 20, no. 15, p. 4341, Aug. 2020.

[102] H. Garg and M. Dave, "Securing user access at IoT middleware using attribute based access control," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–6.

[103] M. Yoshii, R. Banno, and O. Mizuno, "Evaluation of table-based access control in IoT data distribution method using fog computing," *IEICE Commun. Exp.*, vol. 10, no. 10, pp. 822–827, 2021.

[104] H.-C. Chen, "Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 839–852, Jun. 2019.

[105] M. Yoshii, R. Banno, and O. Mizuno, "Evaluation of ticket-based access control method applied to IoT data distribution," *IEICE Commun. Exp.*, vol. 11, no. 3, pp. 148–153, 2022.

[106] I. Riabi, Y. Dhif, H. K. Ben Ayed, and K. Zaatouri, "A blockchain based access control for IoT," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 2086–2091.

[107] L. Zhang, X. Li, Q. Wu, and F. Rezaeibagha, "Blockchain-aided anonymous traceable and revocable access control scheme with dynamic policy updating for the cloud IoT," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 526–542, 2024.

[108] P. Choksy, A. Chaurasia, U. P. Rao, and S. Kumar, "Attribute based access control (ABAC) scheme with a fully flexible delegation mechanism for IoT healthcare," *Peer-Peer Netw. Appl.*, vol. 16, no. 3, pp. 1445–1467, May 2023.

[109] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "TABI: Trust-based ABAC mechanism for edge-IoT using blockchain technology," *IEEE Access*, vol. 11, pp. 36379–36398, 2023.

[110] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, Oct. 2019.

ZEINAB M. IQAL received the M.Sc. degree in computer information systems (CIS) from The Arab Academy for Banking and Financial Sciences (AABFS), in 2007. She is currently pursuing the Ph.D. degree in computer science with Universiti Teknologi Malaysia (UTM). She started her career as a System Engineer, then she was a Lecturer with the University of Jeddah. Her research interests include the Internet of Things, machine learning, and security.

ALI SELAMAT (Member, IEEE) is currently a Full Professor with Universiti Teknologi Malaysia (UTM), Malaysia, where he has also been the Dean of the Malaysia Japan International Institute of Technology (MJIIT), since 2018. An academic institution established under the cooperation of the Japanese International Cooperation Agency (JICA) and the Ministry of Education Malaysia (MOE) to provide the Japanese style of education in Malaysia. He is also a Professor with the Software Engineering Department, School of Computing, UTM, and the Chair of the IEEE Computer Society Malaysia Section. He has published more than 120 research articles with IF JCR, with more than 2400 citations received in the Web of Science and H-index 26. His research interests include software engineering, software process improvement, software agents, web engineering, information retrievals, pattern recognition, genetic algorithms, neural networks, soft computing, collective computational intelligence, strategic management, key performance indicator, and knowledge management. He is an Editorial Board Member of the journal *Knowledge-Based Systems* (Elsevier).

ONDREJ KREJCAR is currently a Full Professor in systems engineering and informatics with the University of Hradec Králové (UHK), Czech Republic, where he is also the Vice-Dean of Science and Research with the Faculty of Informatics and Management. He is also the Director of the Center for Basic and Applied Research, UHK. At UHK, he is a Guarantee of the Doctoral Study Program in applied informatics, where he is focusing on lecturing on smart approaches to the development of information systems and applications in ubiquitous computing environments. His H-index is 20 (according to Web of Science), with more than 1500 citations received in the Web of Science. He has published more than 110 research articles with IF JCR. He has a number of collaborations throughout the world (e.g., Malaysia, Spain, U.K., Ireland, Ethiopia, Latvia, and Brazil). His research interests include control systems, smart sensors, ubiquitous computing, manufacturing, wireless technology, portable devices, biomedicine, image segmentation and recognition, biometrics, technical cybernetics, and ubiquitous computing, biomedicine (image analysis), biotelemetric system architecture (portable device architecture and wireless biosensors), and the development of applications for mobile devices with use of remote or embedded biomedical sensors.

He has also been a Management Committee Member substitute of the Project COST CA16226, since 2017. In 2018, he was the 14th Top-Peer Reviewer in Multidisciplinary in the World according to Publons. He is an Editorial Board Member of *Sensors* (MDPI) with JCR Index and several other ESCI indexed journals. He has been the Vice-Leader and a Management Committee Member at WG4 of the Project COST CA17136, since 2018. Since 2019, he has been the Chairperson of the Program Committee of the KAPPA Program, Technological Agency of the Czech Republic, as a Regulator of the EEA/Norwegian Financial Mechanism in the Czech Republic (2019–2024). Since 2014, he has been the Deputy Chairperson of the Panel 7 (Processing Industry, Robotics and Electrical Engineering) of the Epsilon Program, Technological Agency of the Czech Republic.