A Systematic Mapping Study of Access Control in the Internet of Things

Kaushik Ragothaman
Dakota State University
Kaushik.MuthusamyRagothaman@trojans.dsu.edu

Yong Wang
Dakota State University
Yong.Wang@dsu.edu

Abstract

Internet of Things (IoT) provide wide range of services in both domestic and industrial environments. Access control plays a crucial role as to granting access rights to users and devices when an IoT device is connected to a network. Over the years, traditional access control models such as RBAC and ABAC have been extended to the IoT. Additionally, several other approaches have also been proposed for the IoT. This research performs a systematic mapping study of the research that has been conducted on the access control in the IoT. Based on the formulated search strategy, 1,617 articles were collected and screened for review. The systematic mapping study conducted in the paper answers three research questions regarding the access control in the IoT, i.e., what kind of access control related concerns have been raised in the IoT so far? what kind of solutions have been presented to improve access control in the IoT? what kind of research gaps have been identified in the access control research in the IoT? To the best of our knowledge, this is the first systematic mapping study performed on this topic.

1. Introduction

Internet of Things (IoT) provide many conveniences to users in both domestic and industrial environments. Gartner predicted that there would be 5.8 billion enterprise and automotive IoT endpoints in the year 2020 [1]. Security and privacy are two major concerns revolving around the IoT. IoT device manufacturers and service providers are required by regulations to ensure security of the devices, thereby protecting the privacy of their users.

Identity and Access Management (IAM) is one of the most important domains in security and a prime module in implementing security for any IoT application [2, 3]. Imagine a car manufacturer which sells smart cars to its customers, the manufacturer must design the vehicle's system in a way that it constantly collects and processes data from its surrounding environment through sensors embedded in the vehicle. The system will occasionally transmit the collected data to the manufacturer via the Internet. The data may contain personal information of the driver and sensitive information such as locations. The data that is being sent and shared with the manufacturer should be accessed by authorized users only. Moreover, appropriate controls must be placed if the manufacturer facilitates remote start functions to vehicle owners.

Access control provides the desired service to protect against unauthorized use of resources accessible. Traditional access control techniques are being adopted or extended for access provisioning and management for the IoT. However, the design and implementation of access control for the IoT is also complicated. IoT networks include devices with different hardware and software configurations. Their heterogeneous nature raises a huge challenge for any access control solution. In addition, IoT devices are resource constrained devices which have limited memory, computation power, and battery. This limits the use of complicated algorithms on the devices when designing an access control solution. Further, IoT networks have encountered major attacks in the recent years in many places in the world [4]. Governments of many countries have already initiated to formulate policies for the IoT. Hence, an appropriate access control technique is a need for any IoT network.

This research focuses on the current status of the research in the field of access control in the IoT. We use a systematic mapping study to analyze the literature. This research will answer the following three research questions (RQs):

- RQ1: What kind of access control related concerns have been raised in the IoT so far?
- RQ2: What kind of solutions have been presented to improve access control in the IoT?
- RQ3: What kind of research gaps have been identified in the access control research in the IoT?

URI: https://hdl.handle.net/10125/71474
978-0-9981331-4-0

The contributions of the paper includes, but are not limited to, 1) the paper presents a summary of the latest development of the access control in the IoT; 2) the paper compares different access control models available in the IoT; 3) the paper points out the gaps in the current access control research in the IoT which may lead to future research directions. To the best of our knowledge, this is the first systematic mapping study performed on this topic.

The remainder of this paper is organized as follows: Section 2 introduces the research methodology used for data collection and analysis. Section 3 presents the initial results obtained from the collected literature, followed by discussions of research questions 1, 2, and 3 in Sections 4, 5, and 6. Section 7 summarizes and concludes the paper.

2. Research Design and Implementation

This research uses systematic mapping study (SMS) as the methodology. An SMS is a secondary research study that is used to thematically analyze prior research in the selected field. It is different than a systematic literature review (SLR). An SLR is performed by using a defined scope or a framework [5]. Unlike the systematic literature review, the SMS does not summarize all the collected literature, rather it presents an overview of the selected research area in a structured way. Systematic literature reviews on access control in the IoT exist [6, 7]. However, the scope which the review uses in this paper is performed differently. An SMS is suitable when looking for obtaining an overview of a field of interest, and identifying subtopics where further primary studies are needed [8].

Figure 1 provides an outline of the systematic mapping study process [8] adopted in this paper. The steps performed in this research include: 1) Definition of research questions based on the objective of the research. 2) Definition of search queries in order to collect articles to answer the research questions. 3) Searching for relevant articles using search strings in scientific libraries and databases. 4) Screening the obtained set of articles based on the inclusion and exclusion criteria. Screening could happen in a sequential manner, as screening initially by title and abstract, analysis of whole document, browsing citations. 5) Extract data from the refined set of articles. 6) Analyze the extracted data to create systematic map, thereby answering the research questions.

The following search string is used to collect articles on access control in the IoT from different databases : ((“access control”) OR (“access management”)) AND ((“smart things”) OR (“smart home”) OR (“smart cities”) OR (“iot”) OR (“iiot”) OR (“internet of things”) OR (“industrial internet of things”)). Three online digital libraries were selected, namely ACM digital library, IEEE Xplore, and ScienceDirect. The reason to choose the above three libraries is because they are relevant databases where we could find articles related to the information technology field.

The following inclusion criteria was set, which means the article will be selected for review only if it meets the criteria below:

- Published between 1.1.2010 and 4.30.2020
- Topic is related to IoT and access control
- Scientific and peer reviewed articles
- Relevant to research questions
- Articles written in English language

The following set of exclusion criteria were used:

- Articles concerning specific protocols, applications, architectures
- Editorials and non-peer reviewed articles
- Articles that are not fully available
- Duplicates and already included papers

3. Analysis of Search Results

The defined search query resulted in 1,617 articles from the three digital libraries. The obtained set is subject to screening using the defined inclusion and exclusion criteria as discussed in Section 2. As a next step, topic modeling and keyword generation are performed in Web of Science database to help the screening process. The same query from the Web of Science database provided 1,366 articles. A bibliometric analysis tool called NAILS is selected for topic modeling. NAILS is an open source tool based on R language that utilizes the Latent Dirichlet Allocation (LDA) topic modeling algorithm [9]. It is widely used for social network analysis on literature review articles [10]. Four topics were obtained from the dataset as shown in the Table 1. Topics 1 and 3 are related to security and privacy and network. Topics 2 and 4 are related to Internet of Things and access control. Topics 2 and 4 are closely related to the objectives of this study. A clear category of papers under interest can be found using the topics and keywords identified to examine the obtained articles from the three digital libraries. NAILS also shows the journals and the number of articles published in the IoT. As shown in Figure 2,

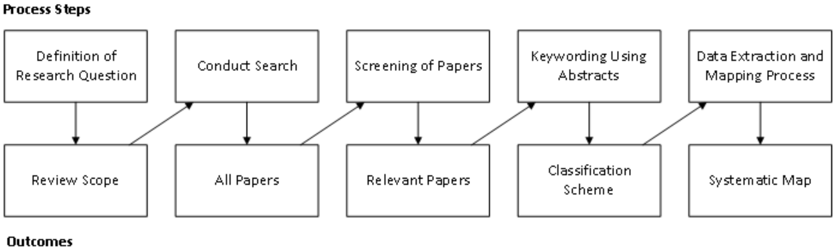

Figure 1. The Systematic Mapping Process [8]

the publications that printed a greater number of articles in the IoT are IEEE Access, IEEE Internet of Things Journal, and the Journal of Sensors. This publication trend is also used in our screening process.

Table 1. LDA Based Web of Science Topics

Topic 1 Security and Privacy	**Topic 2** Internet of Things	**Topic 3** Network	**Topic 4** Access Control
secur	iot	network	access
data	thing	protocol	control
smart	internet	sensor	devic
user	model	mac	system
privaci	manag	perform	propos
cloud	servic	wireless	environ
approach	blockchain	time	base
scheme	paper	node	polici
provid	applic	result	comput
inform	technolog	paper	mechan

To find out how the topics and the keywords are relevant to each other and this research, word co-occurrence study was conducted next. The same Web of Science dataset was further processed by Vosviewer [11]. Vosviewer helps researchers in building and visualizing bibliometric networks. Figure 3 shows a map of the co-occurrences of the keywords derived from the Web of Science dataset. As shown in the figure, the larger node 'internet of things' is strongly linked to 'access control', which in turn is linked to keywords that fall into the objectives of this paper. This indicates that the dataset obtained from Web of Science reveals the articles of our interest fall into the keywords that the 'access control' node is linked to. These keywords are among the important terms in access control in the IoT. They are used to further screening the articles for our systematic mapping study.

Among the 1,617 articles from the three digital libraries, they are first screened using the defined inclusion and exclusion criteria. Then, based on the topic categories and keywords generated using the tools above, the articles were classified under the four topics. As Topics 2 and 4 are closely related to the objectives of this study, 33 articles were selected for detailed data extraction. Table 2 displays the number of articles obtained from each database and the number of articles selected for the data extraction.

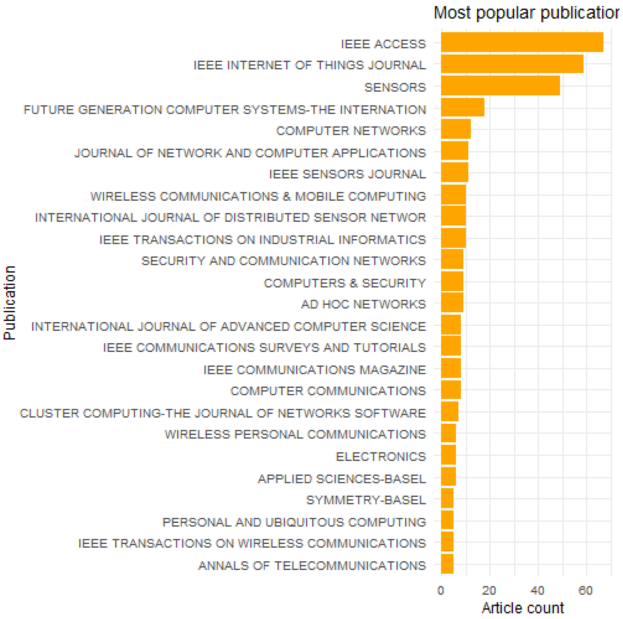

Figure 2. Publications Containing more Articles

Table 2. Search Results and Selected Articles

Database	**No. of Articles Found**	**No. of Articles Selected**
ACM Digital Library	175	10
IEEE Xplore	1,430	17
ScienceDirect	153	6
Total	**1,617**	**33**

Figure 4 shows the number of selected articles published each year from 2010 to 2020. The need of appropriate access control for IoT was indicated in 2010 [12]. It is evident that there has been steady increase in the number starting from 2015. Most of the articles that are related to the topic of interest are published between the years 2017 and 2019.

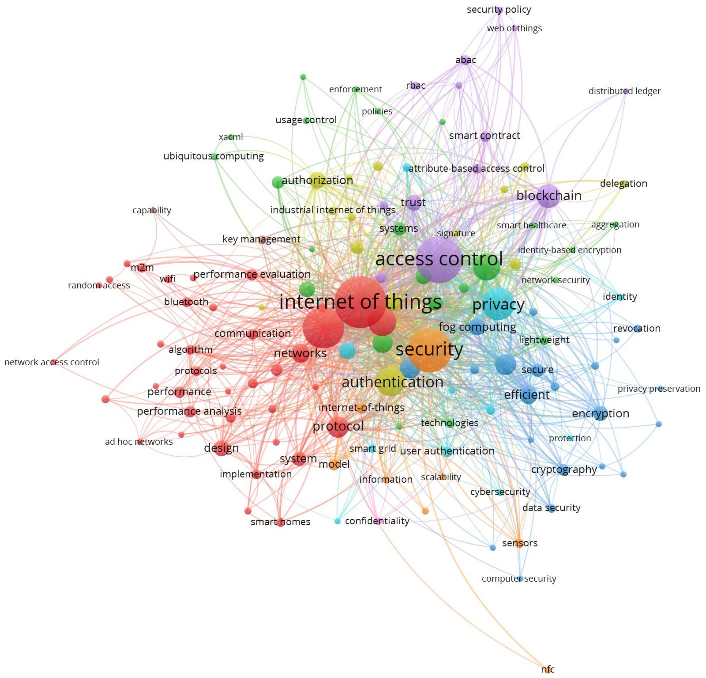

Figure 3. Word Co-Occurrences in Articles

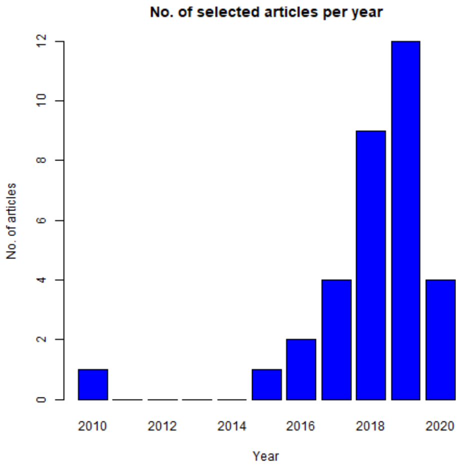

Figure 4. No. of Articles Each Year

4. RQ1: What kind of access control related concerns have been raised in the IoT so far?

The systematic mapping study reveals the latest development of the access control techniques in the IoT. This section presents a summary of the concerns which are related to the access control in the IoT.

Granularity: The fine-grained nature is a most important characteristic for any solution that is designed to manage access rights. Due to the heterogeneity property of the IoT networks and their dynamic nature, granularity is a major concern while designing the models. Most of the IoT frameworks enforce coarse-grained policies [7, 13].

Policy Specification: The policies that are developed for the access control models should be able to handle dynamicity, allow and monitor delegation. An IoT network may contain large number of devices which are present in various forms and locations. Hence, access control policies should consider all of these to govern the network in an effective manner [7].

Handling Complexity: IoT networks are heterogeneous networks which are characterized by resource constrained devices, multiple hop links, unreliable communications, none or limited physical security, etc. Access control models should be able to handle the complex nature of the IoT networks [14].

Interoperability: There are many device manufacturers that provide variety of IoT devices to customers. There is a high possibility that an IoT network may contain devices from different manufacturers and function together. Therefore, access control policies should support this interoperable nature [15].

Facilitation of Users: IoT devices may be shared and accessed by multiple users. For example, in home environments virtual assistants and other smart home products will be used by family members and sometimes guests. Access control policies must allow users to delegate access to other users instead of handling all at a single administrative point [16, 17].

Automation: The complex nature of IoT environments and the number of access decisions to be made at a given time make it difficult to provision or make decisions on individual basis. Hence the policy analysis process should be automated for the IoT [18, 13].

Resource Constraints: IoT is a resource constrained environment. The devices possess low memory and processing power when compared to regular computing machines. These constraints also raise challenges in developing access control solutions [14, 19].

Coherence: In case of multiple administrative points in an access control model, all the administrative nodes should be coherent with the management and provisioning of access control [7]. The type of IoT networks is a concern for this type of solution design.

Resolving Identities: IoT devices come with several attributes such as model number, serial number, IP address, physical address, location, etc. These devices are in turn accessed by other devices and human users when connected to a network. How to leverage the combination of the existing device attributes to uniquely identify the devices in the network poses a concern during the access control specification and implementation [13]. In addition, since a given device can be used by multiple users, appropriate mechanism is required to control the sharing of data.

Downtime: The dynamic nature of the IoT environments throws a serious test of time for access control solutions. Since access decisions are made on a frequent basis, there should be no question for downtime [6, 7, 18]. The design of a centralized administrative point or a distributive one decides this. In a centralized model, if the administrative node fails, it causes single point of failure. In a distributed model, failure of one administrative node causes lack of coherence.

Security: The design of a secure model is another major concern. Access control solutions should be resistant to cyber attacks [4, 14, 19].

The concerns presented above should all be considered when designing and implementing an access control solution for IoT in order for it to be effective. Hence, they shall be transformed into requirements for the design of a solution. Table 3 summarize these requirements.

5. RQ2: What kind of solutions have been presented to improve access control in the IoT?

An access control solution is designed by a set of governing high level policies, the architecture that holds the components, and the underlying access control models. This section reviews the existing solutions in the three components.

5.1. Policies

An access control policy is a mandatory requirement for any IoT device as it defines access permissions when it connects to a network. Policies primarily administer and manage the entire solution. For IoT networks, the formulated access control policies should meet several objectives [6]. For example, in a smart home environment, the IoT device owners must be able to assign permissions to other users to access their devices. The process should not be a complex one for them to understand. The policy also should consider usability [20]. In an enterprise setting, IoT devices that connect to the enterprise network should be flexible to conform to the security policies of the enterprise, so that they do not introduce any risk to their network. However, due to the nature of IoT, it is clear that framing access control policies is domain-specific. The policies must adapt to that particular environment and its characteristics. The smart home products available in market today facilitate the users with policies that allow access delegation, but they are not as fine-grained as the users expect [21, 22]. Further, users expect that smart device manufacturers consider the context of relationships among users to be defined [21]. For instance, the Nest thermostat provides a homeowner an option to add family members, which gives them complete access to the device, although they might not intend to give the family member full access [21]. This type of policy leads to over-privileges. Many current policies define the properties of delegation and context which are required for dynamicity. However, when it comes to access decision or administration, it happens at a single node. Additionally, Access Control List (ACL) based policies are administered manually. Various commercial IoT services such as AWS IoT and NiagaraAx support ACL and role based policies [23]. It becomes unsuitable to create roles and permissions when devices are added at scale. Sticky policies, where-in machine readable policies travel together with data, can provide a data owner-centric approach for the IoT [24]. Sticky policies would allow clever control over the authorization of IoT resources. However, it has many limitations because there is no standard technique

Table 3. Access Control Requirements for IoT

Requirement	Description
Granularity	The access control solution should be fine-grained.
Policy Specification	The access control policy should handle dynamicity and delegation..
Complexity	The access control is able to handle the complex nature of the IoT networks.
Interoprability	The access control solution should support interoperability.
Facilitation of Users	The access control policy should allow users to configure and delegate controls.
Automation	The policy enforcement process shall be automated to support dynamicity and scalability.
Resource Constraints	The access control solution should consider the constrained nature of IoT devices.
Coherence	The access control solution should be coherent at administrative level.
Identity	The access control solution should possess attributes used for device identification.
Downtime	The access control solution should possess multiple administration points to avoid downtime.
Security	The access control solution should be secure to be immune to any cyber attack.

for ciphering the policy and the data while transmission. There is no established language for policy either. Due to pinning of the policy with data, it also increases the computational overhead on the devices [24].

5.2. Architectures

IoT networks can be broadly divided into two categories: centralized architecture and distributed architecture. Hence, access control is predominantly implemented within these two types of architectures. In a centralized architecture, a single node is used for policy administration and management, i.e., access provisioning and revocation happening from a single entity [14]. One of the limitations in centralized architecture is the single point of failure (SPOF). In a dynamic environment like IoT, the entity that administers access control decisions is expected to be always online. Distributed architecture, in contrast, can handle multiple nodes for administration [14]. Although it is easier to facilitate delegation and scalability, a challenge in designing access control solution in distributed architecture is coherence as discussed in Section 4. A decision or a change made at one node should reflect in all the other managing nodes. Designing an appropriate access control solution depends on the architecture of the IoT network.

There are also different types of authorization architectures available. The common ones are the policy-based XACML architecture, the token-based OAuth architecture, and the hybrid User Managed Access architecture [6]. There are other customized architectures that were either derived from the above three, or specific to the applications they were proposed.

Policy-based XACML Architecture: The eXtensible Access Control Markup Language (XACML) is an access control language based on XML which is standardized by the OASIS consortium [6]. It is a popular standard that provides fine-grained access control. XACML describes access control language, request/response language, and a reference architecture. The architecture consists of components namely the Policy Enforcement Point (PEP) to perform access control, Policy Decision Point (PDP) to offer authorization, Policy Information Point (PIP) as a source of attributes, Policy Administration Point (PAP) to create and administer the policy. XACML and Attribute-Based Access Control in combination can offer rich and fine-grained solution. The interpretation of attributes and the language used to define the access control policies is complex. This makes this standard a limitation in terms of usability [14].

Token-based OAuth Architecture: The Open Authorization (OAuth) is an open source authorization standard which is mainly used to provide access to web applications and services. With OAuth, users can provide access for the protected resources to third party applications without disclosing their login credentials. Major OAuth service providers include Google, Microsoft, and Facebook [6]. These service providers are identity providers, who verify the users and provide external applications access to the users' information stored in their ends with their consent. OAuth has several advantages in terms of scalability, interoperability, and flexibility. However, research finds that it lacks fine-grained property and security during implementation. Due to the requirement of the user registration, the client registration, and the nature of IoT networks, implementation and configuration are not easy on the service provider's side. The Internet Engineering Task Force (IETF) is working on extending OAuth 2.0 to be implemented for IoT environments [6].

Hybrid User Managed Access Architecture: The User Managed Access (UMA) is developed as part of the Kantara Initiative. It is an OAuth based protocol. Unlike OAuth, the access to third party applications for the resources is granted regardless of where those resources reside. Hence, this follows a capability based approach, in which an entity with a defined capability and an access token will have access to a resource [6, 14]. The UMA is a user-oriented standard. However, it is new and evolving to be adopted to the IoT environments.

5.3. Access Control Models

Several access control models exist for traditional computing and networking environments. An overview of such models implemented for the IoT and the issues they face are discussed below.

Discretionary Access Control (DAC): DAC is one of the primary access control techniques introduced in computing. It grants access by managing an access control matrix or an ACL [25]. For a dynamic environment like IoT, this model is not suitable. IoT network access decisions must be made under several criteria in different situations, whereas DAC is a static model. Once an access is granted in DAC, it remains forever until the administrator revokes them. In IoT, access should be continually monitored and evaluated for timely revocation. In addition, as new devices are being added or when existing devices are removed, the ACL must be manually updated by the administrator.

Role Based Access Control (RBAC): In RBAC, a user is granted access based on roles which are in turn assigned with appropriate permissions to access the resources [26]. Although it is easy to assign permissions to roles, many users may fall under a single role. RBAC is suitable for access rights in regular computing environments, but not in the IoT. As IoT devices come with variety of functionalities and offer a wide range of services, whenever a device with new functionality is added to a network, a new role must be created by the administrator. In a large enterprise network, this may lead to role explosion. This model does not support the property of dynamicity either.

Attribute Based Access Control (ABAC): ABAC is considered by many as one of the suitable models for the IoT to provision access rights because of its ability to support additional attributes with user roles. Using ABAC, different attributes of IoT such as device ID and location may be included to evaluate while providing access. Even though this model is being used in large scale projects like smart grid, ABAC faces the issue of complexity due to its centralized architecture [27, 28].

Organization Based Access Control (OrBAC): OrBAC is an extension of the role based access control by including a new dimension called "organization" [29]. This additional attribute helps in granting access when multiple organizations play a role, or when an organization has many subdivisions. However, other than the above mentioned concept, this model is no different than its parent model RBAC and considered not suitable for heterogeneous and dynamic IoT environments.

Usage Based Access Control (UCON): The UCON model was introduced as a framework to protect digital resources that come under digital rights management (DRM). This model comes with three main concepts called Authorization (A), Obligation (O), Condition (C) [30]. The authorization represents evaluation as to whether a subject is eligible to be provided access or not. Obligation is a criteria that a subject must perform in order to be provided with or sustain access. Condition represents the criteria that a subject must satisfy. Due to the three categories of evaluation, UCON provides high dynamicity where the access is continually monitored, thereby it can be revoked whenever it is required per policy. However, this model does not explain the delegation property and follows a centralized architecture.

Capability Based Access Control (CapBAC): The concept of CapBAC was started as part of the IoT@Work project. It is an initiative by the European Union to leverage IoTs to automate various services in public sector entities [31]. CapBAC follows a distributed approach. It is implemented through various nodes by using Policy Decision Point (PDP), Policy Enforcement Point (PEP) [32]. In CapBAC, a resource requester must show a particular capability to request an access token. The PDP decides whether to issue the token to the requester or not. Once issued, the token is evaluated at the PEP for the requester to access the resource. Another advantage of CapBAC is the property of delegation, where nodes can be given the authority to provide access to other nodes. The level of delegation is determined while designing the model. But, whether to trust the requester or not, the model must depend on a central server for either identity verification or certificate, although access is issued based on the requester's capability. Further, CapBAC does not consider context while provisioning access [6].

Access control using blockchain: Blockchain technology has found its boom in providing security and privacy applications in the recent years. The important characteristic of this technology is that its distributed nature. The methods through which access control using blockchain is described in the literature can be further divided into transaction-based and smart-contract based access control [33, 34, 35]. Transactions can be used to grant, delegate or revoke access rights. Smart contract can be used to evaluate access request and make decision based on the access policy defined by the resource owner. In either case, an access token is generated and passed on to the requester which signifies the right to access. The main disadvantage of the transaction approach is that the access decision must be made by a centralized node, whereas the smart-contract approach may invoke large overheads due to the creation of contracts between nodes.

Table 4 presents a summary of the models discussed and their concerns to fulfill the access control requirements. As shown in the Table 4, all access control models have limitations when adopted in the IoT. This indicates that more research efforts are desired in the field.

In addition to the models discussed above, there are other access control models proposed in the literature. In History Based Access Control (HBAC), an access decision is made dynamically based on a context of access history in a given state. The model requires a centralized authorization system such as a certificate authority in place [36]. There are two access control models, Risk Adaptive and Proximity-Based access controls [37], available for implantable medical devices. In Risk Adaptive model, a decision is made by considering the risk factor evaluated by policies. In the proximity-based model, a programmer of the device must be in close proximity with the patient to generate the key to decrypt the communications from the device. This model has a potential physical security issue that an adversary should not be in close proximity with the patient [37]. The proximity-based model is used widely in the implantable devices. Trust-based models allow devices to be attached to user spaces within a short time period. In this model, the access permissions are assigned to users based on their levels of trust [16]. However, it is difficult to define how trust and relationships between users and devices and devices to devices are established. Examples of trusted-based models include Billing-based Access Control and Privilege-based Access Control. The billing-based approach is a business driven control where a service is provided to any user who receives an adequate reward [6]. Identity does not matter in this model. In the privilege-based model, a decision is made based on an organization's policies and the access is restricted only to particular users [6]. Trust is one of the important criteria in a heterogeneous environment such as IoT. It enhances both security and privacy [38]. However, trust systems in the IoT face challenges such as heterogeneity, scalability, and integrity [38].

6. RQ3: What kind of research gaps have been identified in the access control research in the IoT?

The comparisons in the Table 4 also indicate the research gaps in access control in the IoT. This section summarizes these research gaps and also points out future research directions.

Access control and identity management: Access control assumes IoT devices can be uniquely identified and access control policies can be applied to network traffic. As users are identified in a digital network by their unique identities, IoT devices also require their unique identities when connecting to a network. Users are often identified by something users know (e.g., username and password), something users have (e.g., a physical token or a smartcard), and something users are (e.g., fingerprint or face recognition). IoT devices can only be identified by something IoT devices have. A common identification technique of a device in a network is using the device's MAC address. However, MAC address is easy to be spoofed. Given the heterogeneity and the need to protect the information that IoT devices collect, device identities need to be addressed before access control [39]. Hence, Identity of Things (IDoT) is a field that will grow in the coming years.

Access control and relationships: Relationships such as user-to-user, user-to-device, and device-to-device relationships can be utilized for identity management and access control. It is expected by many consumers that the IoT device manufactures include the concept of relationships for access provisioning. Thus, Identity Relationship Management (IRM) is gaining attentions and has been identified as the next promising IAM system for the IoT [40].

Policies specification and automation: A comprehensive review of the policies defined for the administration of access control reveals that existing solutions lack the dynamicity in policy generation, decision and evaluation [41]. Machine learning shall be used for policy automation where the policy is determined by model itself on a request by request basis. Therefore, automated policies will directly help in achieving dynamicity in an access control solution. With automation, there is no need to edit policies manually when devices are added at scale.

Access control and interoperability issues: In an IoT network, not all the devices come from the same manufacturer. When connected to a network, devices should be able to operate among one another. Access control is expected to function among a variety of devices too.

Blockchain and access control: Blockchain is still needed to be explored for access provisioning in IoT environments. Due to its distributed nature and property of delegation, it can well suit IoT networks. The area of blockchain for access control in IoT still needs to mature.

Access control and security: The security of access control models is a concern too. The security flaws in access control may occur in many places including design, protocols, implementations, and configurations.

Table 4. Access Control Models and Feature Matrix

Features	DAC	RBAC	ABAC	OrBAC	CapBAC	UCON	Blockchain
Granularity	Coarse	Coarse	Fine	Coarse	Coarse	Fine	Fine
Context-Aware	No	No	Yes	Yes	No	Yes	Yes
Dynamicity	No	No	Yes	No	Yes	Yes	Yes
Complexity	More	More	More	More	Less	More	More
Distributed Nature	No	No	No	No	Yes	No	Yes
Interoperability	No	No	Yes	Yes	Yes	No	Yes
Delegation	No	No	No	No	Yes	No	Yes
Revocation	No	No	No	No	Yes	Yes	Yes
Scalability	No	No	Yes	No	Yes	Yes	Yes

Although many access control models have been proposed for IoT, few work has been conducted on access control security analysis. Due to the importance of access control for any network, thorough studies on access control security analysis are desired.

7. Summary and Conclusion

This paper answered three research questions by conducting a systematic mapping study of the access control in the IoT. The systematic mapping study revealed the access control related concerns in the IoT, the access control solutions proposed so far, and the future research directions in this field. There is no one-size fits-all solution in access control in the IoT. It depends on the network environment and the architecture. IoT networks come with several requirements and there are a number of challenges that the networks pose to fulfill them. The requirements are often intertwined with one another. Therefore, it is possible that satisfying one requirement automatically paves the way to fulfill another. Hence, it is important that we leverage relevant technologies that make IoT devices usable while securing them at the same time.

References

[1] L. Goasduff, "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020." https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io, 2019.

[2] T. Macaulay, *Chapter 9 - Identity and Access Control Requirements in the IoT*, pp. 157–176. Boston: Morgan Kaufmann, 2017.

[3] A. Sharma, S. Sharma, and M. Dave, "Identity and access management- a comprehensive study," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 1481–1485, 2015.

[4] S. Bhattarai and Y. Wang, "End-to-end trust and security for internet of things applications," *Computer*, vol. 51, pp. 20–27, apr 2018.

[5] B. Kitchenham, S. Charters, *et al.*, "Guidelines for performing systematic literature reviews in software engineering version 2.3," *Engineering*, vol. 45, no. 4ve, p. 1051, 2007.

[6] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[7] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in internet-of-things: A survey," *Journal of Network and Computer Applications*, vol. 144, pp. 79–101, 2019.

[8] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*, pp. 1–10, 2008.

[9] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent dirichlet allocation," *Journal of machine Learning research*, vol. 3, no. Jan, pp. 993–1022, 2003.

[10] A. Knutas, A. Hajikhani, J. Salminen, J. Ikonen, and J. Porras, "Cloud-based bibliometric analysis service for systematic mapping studies," CompSysTech '15, pp. 184–191, Association for Computing Machinery, 2015.

[11] N. J. van Eck and L. Waltman, "Software survey: Vosviewer, a computer program for bibliometric mapping," *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010.

[12] R. H. Weber, "Internet of things – new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23 – 30, 2010.

[13] S. Pal, "Limitations and approaches in access control and identity management for constrained iot resources," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 431–432, 2019.

[14] 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," *Annals of Telecommunications*, vol. 74, no. 7-8, pp. 375–388, 2019.

[15] K. Cheung, M. Huth, L. Kirk, L.-N. Lundbæk, R. Marques, and J. Petsche, "Owner-centric sharing of physical resources, data, and data-driven insights in digital ecosystems," in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, SACMAT '19, (New York, NY, USA), p. 73–81, Association for Computing Machinery, 2019.

[16] Y. Al-Halabi, N. Raeq, and F. Abu-Dabaseh, "Study on access control approaches in the context of internet of things: A survey," in *2017 International Conference on Engineering and Technology (ICET)*, pp. 1–7, 2017.

[17] M. Nguyen, M. O. Gani, and V. Raychoudhury, "Yours truly? survey on accessibility of our personal data in the connected world," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 292–297, 2019.

[18] I. Ray, R. Abdunabi, and R. Basnet, "Access control for internet of things applications," in *Proceedings of the 5th on Cyber-Physical System Security Workshop*, CPSS '19, pp. 35–36, Association for Computing Machinery, 2019.

[19] A. Kaur, Isha, G. Rai, and A. Malik, "Authentication and context awareness access control in internet of things: A review," in *2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, pp. 630–635, 2018.

[20] K. Kafle, K. Moran, S. Manandhar, A. Nadkarni, and D. Poshyvanyk, "A study of data store-based home automation," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, CODASPY '19, (New York, NY, USA), p. 73–84, Association for Computing Machinery, 2019.

[21] M. Tabassum, J. Kropczynski, P. Wisniewski, and H. R. Lipford, "Smart home beyond the home: A case for community-based access control," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, (New York, NY, USA), p. 1–12, Association for Computing Machinery, 2020.

[22] W. Jang, A. Chhabra, and A. Prasad, "Enabling multi-user controls in smart home devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, IoTS&P '17, (New York, NY, USA), p. 49–54, Association for Computing Machinery, 2017.

[23] J. Koh, D. Hong, S. Nagare, S. Boovaraghavan, Y. Agarwal, and R. Gupta, "Who can access what, and when? understanding minimal access requirements of building applications," in *Proceedings of the 6th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation*, BuildSys '19, (New York, NY, USA), p. 121–124, Association for Computing Machinery, 2019.

[24] D. Miorandi, A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Sticky policies: A survey," *IEEE Transactions on Knowledge and Data Engineering*, pp. 1–1, 2019.

[25] K. Albulayhi, A. Abuhussein, F. Alsubaei, and F. T. Sheldon, "Fine-grained access control in the era of cloud computing: An analytical review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0748–0755, 2020.

[26] T. L. Shan, S. A. Ismail, and A. Azizan, "Access control models for cloud computing: A review," in *2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN)*, pp. 155–158, 2018.

[27] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. Ait Ouahman, "Access control in iot: Survey state of the art," in *2016 5th International Conference on Multimedia Computing and Systems (ICMCS)*, pp. 272–277, 2016.

[28] D. Servos and S. L. Osborn, "Current research and open problems in attribute-based access control," *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, pp. 1–45, 2017.

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

[30] 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 of Things Journal*, pp. 1–1, 2020.

[31] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," *Mathematical and Computer Modelling*, vol. 58, no. 5, pp. 1189 – 1205, 2013.

[32] Y. Andaloussi, M. D. E. Ouadghiri, Y. Maurel, J. M. Bonnin, and H. Chaoui, "Access control in iot environments: Feasible scenarios," *Procedia Computer Science*, vol. 130, pp. 1031–1036, 2018.

[33] I. Riabi, H. K. B. Ayed, and L. A. Saidane, "A survey on blockchain based access control for internet of things," in *2019 15th International Wireless Communications Mobile Computing Conference (IWCMC)*, pp. 502–507, 2019.

[34] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the internet of things," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1568–1573, 2018.

[35] P. E. Sedgewick and R. de Lemos, "Self-adaptation made easy with blockchains," in *2018 IEEE/ACM 13th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, pp. 192–193, 2018.

[36] L. Tandon, P. W. L. Fong, and R. Safavi-Naini, "Hcap: A history-based capability system for iot devices," in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, SACMAT '18, (New York, NY, USA), p. 247–258, Association for Computing Machinery, 2018.

[37] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access control schemes for implantable medical devices: A survey," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1272–1283, 2017.

[38] R. Thirukkumaran and P. Muthu kannan, "Survey: Security and trust management in internet of things," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pp. 131–134, 2018.

[39] S. Wachter, "Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr," *Computer Law & Security Review*, vol. 34, no. 3, pp. 436–449, 2018.

[40] N. W. Hardy, "The internet of things ecosystem: Survey of the current landscape, identity relationship management, multifactor authentication mechanisms, and underlying protocols," *International Journal of Computer and Information Engineering*, vol. 10, no. 6, pp. 1202–1206, 2016.

[41] S. Calo, D. Verma, S. Chakraborty, E. Bertino, E. Lupu, and G. Cirincione, "Self-generation of access control policies," in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, SACMAT '18, (New York, NY, USA), p. 39–47, Association for Computing Machinery, 2018.