A Survey on Access Control in the Age of Internet of Things

Article · January 2020

DOI: 10.1109/JIOT.2020.2969326

Jing Qiu

Guangzhou University

Zhihong Tian

Guangzhou University

Shen Su

Harbin Institute of Technology

A survey on Access Control in the Age of Internet of Things

Jing Qiu[1], Zhihong Tian[1,*], Chunlai Du[2], Qi Zuo,[3] Shen Su[1] and Binxing Fang[1]

***Abstract*—With the development of Internet of Things (IoT) technology, various types of information, such as social resources and physical resources, are deeply integrated for different comprehensive applications. Social networking, car networking, medical services, video surveillance and other forms of the IoT information service model gradually change people's daily lives. Facing the vast amounts of IoT information data, IoT search technology is used to quickly find accurate information to meet the real-time search needs of users. However, IoT search requires using a large amount of user private information, such as personal health information, location information and social relations information, to provide personalized services. Employing private information from users will encounter security problems if an effective access control mechanism is missing during the IoT search process. An access control mechanism can effectively monitor the access activities of resources and ensure that authorized users access information resources under legitimate conditions. This survey examines the growing literature on access control for an IoT search. Problems and challenges of access control mechanisms are analyzed to facilitate the adoption of access control solutions in real-life settings. This paper aims to provide theoretical, methodological and technical guidance for IoT search access control mechanisms in large-scale dynamic heterogeneous environments. Based on a literature review, we also analyzed the future development direction of access control in the age of IoT.**

***Index Terms*—IoT search, access control, attribute-based access control, survey**

I.INTRODUCTION

The IoT concept implements connection, interaction and data exchange between various devices, such as vehicles and home appliances. IoT devices are collecting diverse data, such as electricity consumption, location information, and sensor data, from the Internet, sensor networks, and online social networks. With the increasing scale of IoT, the scale of data generated by the IoT devices is increasing day by day. How to effectively utilize the rich information in the IoT is a major challenge for the development of IoT applications. To face this vast challenge, IoT search technology was proposed to integrate different types of data, provide all kinds of data retrieval services, and meet real-time search needs quickly and accurately [2, 3]. IoT search is a "double-edged sword". On the one hand, it will bring convenience to people's lives if it is used properly. On the other hand, it is also a serious threat to personal privacy and national security. Whether IoT search can be widely accepted and popularized depends on its ability of prevent sensitive information leakage.

Access control, as the backbone technology to ensure information security, brings the opportunities in overcoming the above challenges of IoT. Access control can effectively monitor the access of resources and prevent the unauthorized flow of information. However, IoT search is a relatively new research field, and traditional access control methods and techniques cannot fully solve the access control problems faced by IoT search.

IoT search environments cover Internet, sensor network, online social network and so on. The use of information extends from traditional web information to information covering Human, Cyber, and Physical. Data access under the IoT search environment has the following features.

1) Massive. The researchers explained that in USA only the M2M traffic volume increased by 250% in 2011, and it is expected to occupy nearly half of the total traffic of the Internet by 2020 [1]. Massive data brings new challenges to data maintenance, storage and retrieval.

2) Dynamic. In the IoT search environment, nodes and users are constantly changing, and access objects may be continuously added and deleted. This dynamic characteristic makes it difficult to predict all user information in advance and accurately understand the user and permission structure.

3) Strong privacy. With the improvement of data sharing, more and more attention has been paid to data privacy and security. To protect individual’s privacy, governments and researchers proposed many privacy principles, such as ISO/IEC 29100:2011 [6], Privacy by Design [7], General Data Protection Regulation [8], and Fair Information Practice Principles [9]. However, many researchers doubt whether these principles have benefited privacy, since some of the principles mainly maximizing individual control over the data instead of protecting the data [10].

4) Multi-party commonality. The data in IoT search are no longer limited to a single closed environment, but generated by different cooperative organizations. The Internet of things search service is actually composed of several information systems that are dynamically connected. Through the information exchange and sharing between different cooperation organizations to meet the complex application needs.

Funding: This research is supported by the Guangdong Province Key Research and Development Plan (2019B010137004, 2019B010136003), the National Key research and Development Plan (2018YFB0803504), the National Natural Science Foundation of China (61871140, 61872100, U1636215), and Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019).

1 Cyberspace Institute of Advanced Technology, Guangzhou University; qiujing@gzhu.edu.cn; tianzhihong@gzhu.edu.cn; johnsuhit@gmail.com; fangbx@bupt.edu.cn

2 School of Computer, North China University of Technology; duchunlai@ncut.edu.cn

3 Beijing Computing Center; zuoqi@bcc.ac.cn

* Correspondence: Zhihong Tian, tianzhihong@gzhu.edu.cn

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.2969326, IEEE Internet of Things Journal

Access control, as the backbone technology to ensure information security, can effectively monitor the access of resources and prevent the unauthorized flow of information. However, IoT search is a relatively new research field, and traditional access control methods and techniques cannot fully solve the access control problems faced by IoT search. In the IoT environment, data is continuously transmitted and shared among things and users to achieve particular goals [11, 12]. Authentication, confidentiality, and access control are important to ensure secure communication in this sharing environment [13]. Authentication and confidentiality are needed to establish a secure communication system under this sharing environment. For example, how to ensure that the edge device can reliably determine the query or command comes from the authorized device, and how the edge device can confirm this authority. Public key cryptography, signature, and authentication are often used to achieve authentication and confidentiality [14]. The object of access control in IoT environment is data stream more than traditional DBMS (Database Management System). Under this scenario, the challenges of access control include guarantee the access permission, manage the scalable IoT architecture, handle the huge amount of data stream, and so on.

In summary, though Access control can benefit IoT search, there are also a number of challenges need to be addressed. This paper aims to present an in-depth survey on the state-of-the-art characteristics, requirements, technologies, challenges, and open research issues in access control for IoT search

A. Comparison Between This Paper and Existing Surveys

Access control is the process of ensuring every request of resources and data is managed by a system that can make a decision to grant or deny the request. For any information management system, the most important thing is to protect the privacy and integrity of resources and data. According to different security policies required by different systems, different access control decisions are made and enforced to ensure that only authorized accesses can take place. Accordingly, all unauthorized disclosure and unauthorized modifications to resources and data are prohibited, while resources and data are available to legitimate uses. A large body of literature summarized the development of access control. In [15], the development of an access control system is carried out in three phases as a security policy, a security model and a security mechanism. The literature illustrates a review of different access control policies and models, while security mechanisms are also investigated deeply. In [16], a survey of access control mechanisms along with their deployment details are presented to illustrate different access control models that are required by different application domains, and different deployment details that are required by different usage environments.

In the age of IoT, information search objects extend from static content to dynamic content (a variety of things or objects, such as multimedia and mobile phones) [17], and the environment changes from a single domain to a multidomain collaborative environment. As mentioned above, different application domains and environments require different characteristics of access control models and mechanisms [18-20]. Access control oriented to IoT applications has been the subject of a large body of research work. There are a number of literature reviews summarizing these research works, which we briefly discuss here. In [21], benefits and weaknesses of the early access models in collaborative systems are discussed to show the development status before 2005. This is a very comprehensive review of access control in Collaborative Systems. Authors analyzed the access control requirements for collaboration firstly, then examined existing access control models in collaborative environment, finally given a set of criteria to evaluate these models. This article is very helpfur for the design and evaluation of access control model in a collaborative environment. With the widespread use of WBSNs (web-based social networks) services, information sharing and dissemination is becoming more and more convenient, which pose serious security and privacy concerns. In [22], the authors discussed the main requirements related to access control and privacy enforcement with the features of WBSNs. According to these requirements, they review the research activities proposed before 2008 on access control in this field. In [23], online social networks (OSN) are chosen as the application domain to discuss how access control models and solutions could meet the security and privacy requirements of OSN. In [24], access control models are categorized into relationship-based, attributes-based, community structure-based and a user activity centric model. The authors reviewed different access control models in social networks according to these categories. In [25], the authors focus on attribute-based access control (ABAC), which is a popular access control model for IoT-oriented applications. The current research status of ABAC is discussed based on taxonomic categories. In [26], the research proposals on access control for collaborative systems centered on communities are surveyed. Firstly, the characteristics of community-centered collaborative systems are summarized based on a thorough analysis of the literatures, real-world scenarios, and the current state of affair of community-centered systems. Then several important requirements are summarized span from policy specification, governance, transparency, to evaluation. To satisfy these requirements, the features of access control systems are identified and analyzed. By overview many models and mechanisms for community-centered systems, main research trends and major gaps are identified to guide future research. The authors also summarized the challenges to be addressed in this field.

However, most of the existing surveys suffer from the following limitations: 1) there is no clear definition of IoT search; 2) there is no overview of access control specifically for IoT search (some of them aim to provide the big picture understanding of access control in a variety of usage environments, some focus on a certain IoT scenario); 3) other important issues like policy mining are missing.

Table I provides a comparison of our survey with the other related surveys. The comparison is based on the type of access control aspects of IoT search in our survey, namely, policy description method, policy and model combination, conflicts detection and resolution, attribute discovery mechanism, policy

TABLE I
Comparison of Our Survey to Other reaOther Related Works

	Our Survey	Samarati & Vimercati [15]	Suhendra [16]	Tolone et al. [21]	Carminati & Ferrari [22]	Kayes. & Iamnitchi [23]	Asim & Malik [24]	Servos, Osborn [25]	Paci et al. [26]
Access Control Policy Combination and Conflicts Resolution									
Policy Description Method	✓		✓	✓			✓	✓	✓
Policy and Model Combination	✓	✓	✓			✓	✓	✓	✓
Conflicts Detection and Resolution	✓	✓	✓	✓			✓		✓
Access Control Policy Authoring									
Attribute Discovery Mechanism	✓	✓	✓			✓	✓	✓	✓
Policy Mining	✓							✓	
Policy authorization	✓	✓	✓	✓	✓	✓	✓	✓	✓

mining, and policy authorization. Compared to our work, the literature reviews Suhendra [16], Asim & Malik [24], and Paci et al. [26], focus on five of the six aspects summarized in this paper and do not consider policy mining. Servos & Osborn [25] reviews the aspect of policy mining while not considering conflicts detection and resolution. Samarati & Vimercati [15] do not consider policy mining, and they discuss Logic-Based Authorization Languages not access policy language we mentioned in policy description method. Kayes & Iamnitchi [23] and Tolone et al. [21] review three of the six aspects. In contrast, our survey provides a more comprehensive review of existing research works that focus on access control in IoT environments.

B. Contributions

In view of prior work, we aim to: 1) provide a conceptual introduction on IoT search and access control technologies; 2) present a thorough analysis of the current state-of-the-art technologies of access control for IoT search; and 3) give discussions of technical challenges enabling access control for IoT search. The main contributions of this paper are highlighted as follows.

1) A brief introduction on Access Control is first given, which includes the classic access control models and the access control technologies in the new application scenarios.

2) The definition of IoT search is then given with a summary of key characteristics of IoT search and a taxonomy of requirements of access control models and mechanisms that are needed by IoT search.

3) To provide accurate access control policy management, heterogeneous policies of different agents need to be integrated. Policy combination and conflict resolution is then discussed.

4) Based on the policy combination and conflict resolution, collaborative authoring of access control policies is required. Access control policy authorization also discussed from three aspects, attribute discovery mechanism, policy mining, and policy authorization.

5) Furthermore, this paper summarize the research gaps and open research issues to guide the future research in access control for IoT search.

The article is organized as follows. The next section describes the background of access control for IoT search. Section III analyzes the features of IoT applications and delineates the main requirements that access control models and mechanisms should meet in this field. Section IV reviews the existing literature on access control policy combination and conflict resolution technologies and analyzes the available access control models that meet this requirement. Section V reviews the recent developments in access control policy authorization which includes attribute discovery mechanism, policy mining and authorization model. Section VI identifies open issues for future research. The conclusion of the article is given in Section VII.

II.Access Control Background

While providing convenience to people, IoT search uses a large amount of authorized personal private data. However, the protection of these private data is not sufficient. Once the private data is leaked, it may bring massive losses to the organizations. Access control technology ensures that resources can only be accessed by authorized users according to the predefined access control policy, so it can prevent unauthorized access to private information.

By the 1970s, access control systems were mainly used in the mainframe system, such as the BLP model [27] and Biba model [28]. The BLP model is designed according to the military security policy, which aims to solve the access control problem with confidential hierarchy information. It is the first mathematical model of an access control model with a strict theoretical proof. The Biba Model was developed by Kenneth J. Biba in 1975. It is a formal state transition system of the computer security policy that describes a set of access control rules designed to ensure data integrity. The Clark–Wilson model was described in 1987 by Clark and Wilson. This model is used to control and audit the subject's state transition and run time adjustment of the low-water-mark policy parameters. Compared with Biba, the Clark–Wilson model provides a complete integrity protection by means of controlled state transaction, while the Biba model provides a simple multilevel integrity access control scheme but needs the introduction of a trusted subject to ensure the usability.

By the 1980s, with the continuous improvement of requirements of the credibility of computers, studies proposed more flexible access control mechanisms. One of the representative works is the Trusted Computer System Evaluation Criteria (TCSEC) which was created by the United States Government Department of Defense (DoD). TCSEC is a standard that sets basic requirements for assessing the effectiveness of security. According to TCSEC, access control can be divided into discretionary access control (DAC) [29] and mandatory access control (MAC) [30] depending on different roles of access authority users. The DAC model allows legitimate users to access objects as users or groups, while preventing unauthorized users from accessing objects, and some users can also independently grant access rights to objects that they own to other users. The DAC model can meet the security needs of resource owners; however, because of the way that access depends on user authorization, the management of access authorities in the DAC model is more decentralized. At the same time, DAC needs to manage the users, authorities and resources manually, which makes it inappropriate for IoT search due to the high complexity management work. The MAC model is a means of assigning access rights based on regulations by a central authority. This class of policies includes examples from both industry and government. The applications of MAC are usually based on a multilevel security model. Although the MAC model solves the problem of decentralized resource management by centralizing authorization management, for the users of IoT search, the management efficiency of the MAC model is lower.

By approximately the 2000 timeframe, with the development of the Internet and the increasing large-scale applications of information system in enterprises, the traditional models of access control (i.e., DAC, MAC and its extension models) encountered difficulties addressing complex application layer access requirements. To solve this problem, role-based access control (RBAC) [31] was posed to restrict system access to authorized users. The components of RBAC (i.e., role-permissions, user-role and role-role relationships) make it simple to perform user assignments. Figure 1 shows the relationship between roles and users in the RBAC model. RBAC can be used to facilitate administration of security in large organizations and meet the information integrity requirements of information systems. RBAC is different from MAC and DAC; however, it can enforce these policies without any complication.

The fast development of new computing environments such as IoT search brings vast challenges to the applications of access control technology. Traditional closed environment-oriented access control models (i.e., DAC, MAC, RBAC) are not adapted to the new computing environments. In this case, attribute-based access control (ABAC) [32] is proposed as an emerging form of access control, where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions [25]. The concept of role is very common in real life. Ferraiolo and Kuhn first introduced it into the Information System Access Control Research Institute in 1992 and named it RBAC [31]. Different from the traditional access control models with manual assignment of roles, ownership, or security labels by a system administrator, ABAC allows for the creation of access policies based on the existing attributes of the users and objects in the system.

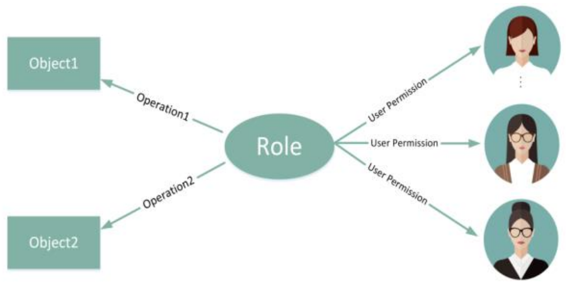

Figure 1. Role and user relationship of RBAC.

Since attributes can describe entities in different views, they allow users to change access control strategies according to actual situations. Temporal-RBAC (TRBAC) [33] is an extension of the RBAC model, which supports periodic role enabling, disabling, and temporal dependencies by using role triggers. Besides temporal information, location constraints are also need to be considered in the IoT environment. Spatio-Temporal RBAC (STRBAC) [34] is proposed by researchers to provide high level description of Access Control when the access to the resources requires to consider both time and location information. Concept usage control (UCON) was developed in [35], which enables finer-grained control over usage of digital objects than that of traditional access control policies and models. The advantages of ABAC can effectively solve the problem of fine-grained access control in dynamic large-scale environments. ABAC is an ideal access control model in the new computing environment and has broad application prospects.

ABAC makes access control decisions based on the attributes of access control entities. These attributes are often represented by a four-tuple $< S, O, P, E >$, where S is Subject Attributes, O is Object Attributes, P is Permission Attributes, and E is Environment Attributes.

A simplified ABAC model is given in Figure 2, where attribute assignment (AA) aims to assign attributes to subjects and objects, policy permission relation (PPR) is the relation between policies and the permissions they grant, and policy is the set of all policies that govern access in the system. Although ABAC achieves effective control over users' access to resources, the security of the private data is not fully considered. Based on the idea of traditional ABAC, researchers have proposed attribute-based encryption (ABE) [36], where objects are encrypted based on attribute-based access policies. ABE mainly consists of key-policy ABE (KP-ABE) [37] or ciphertext-policy ABE (CP-ABE) [38]. In KP-ABE, the access structure is combined with the user's private key, and the attribute set is associated with the resource to be accessed. The data owner cannot set the corresponding access control policies since only attributes can be used to describe the data in this model, and user freedom is relatively high while data owner freedom is lower. CP-ABE is the reverse of KP-ABE, using an

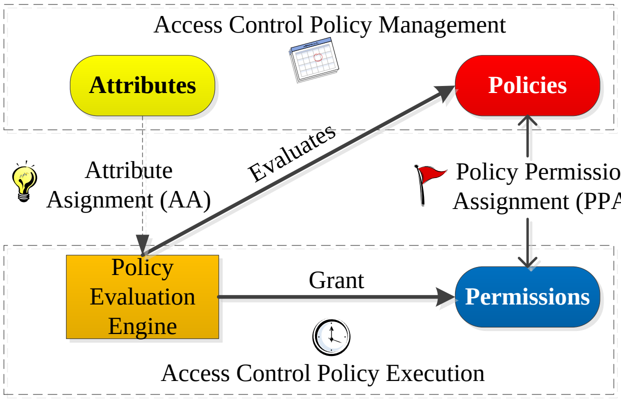
Access Control Policy Management
Attributes
Policies
Evaluates
Attribute Assignment (AA)
Policy Permission Assignment (PPA)
Policy Evaluation Engine
Grant
Permissions
Access Control Policy Execution

Figure 2. Core ABAC model. Attributes include both subject attributes and object attributes. Thin solid arrows denote many-to-many relations, thick solid lines denote relations with the policy engine, and dotted lines denote information used by the policy engine to evaluate a certain policy.

attribute-based policy to encrypt an object, where the access structure that is used to describe the access control policy is combined with the resource to be accessed, and the attribute set is associated with the user's private key. In this model, the access control policy is set by the data owner, so that the data owner freedom is higher.

Different application scenarios have different requirements for access control. Networked control system (NCS) is a complex fully distributed control system which integrates communication network and control system. In the process of data transmission in the network, data conflicts, blockages and packet dropouts often occur among groups of information from different network nodes, which restrict the control effect and real-time performance of the control network. In view of the advantages and disadvantages of the two access control modes of CDMA/CD and token transfer, according to the queuing theory in operational research, [39] proposes an access control mode applied to control networks, which optimizing token network based on QoS. Manufacturing Internet of Things (MIoT) is a deep integration of manufacturing and Internet of Things, which has two important characteristics, resource sharing and process collaboration. In [40], focus on multidomain MIoT environment, a resource sharing access control model is proposed based on the role-based access control. Firstly, it defined the Authorization Route Optimizing Problem (AROP). Secondly, a solution algorithm called PGAO* is designed based on graph-planning algorithm and the AO star algorithm to find the best authorization route. Experiments show that the proposed access control model and algorithms could decrease the security administrator workloads, and strengthen the access safety in resource sharing. In the environment of IoT, machine-type communications (MTC) provide autonomous connectivity between machines. Concurrent and massive access attempts of MTC devices may cause many problems, such as packet loss and intolerable delay. In [41], a joint access control and random access channel resource allocation strategy is proposed to solve the optimization problem for maximization of the random access efficiency with the access delay constraints. The effectiveness of the strategy is demonstrated via analysis and simulations by using a discrete-time Markov chain. In [42], authors focus on hidden dangers of wireless network, especially malicious attacks on wireless gateway. An adaptive intelligent wireless security gateway product is introduced in this paper, which applies 802.1x protocol and integrates access control function with packet filtering function.

III. Access Control Challenges in IoT search

Currently, IoT has become one of the hottest research fields in the information science and technology domain [43, 44]. Massive and heterogeneous sensors and devices are connected and managed in various IoT systems. A big data scenario is constructed in the IoT systems environment because massive and highly heterogeneous data are automatically sampled in real time from different devices with a high frequency. In this case, the traditional searching techniques that mainly focus on static or slowly evolving web data are not suitable for dynamically generated sampling data in the IoT environment. Therefore, increasingly more research works are devoted to search engine technology in IoT, called IoT search [45].

A. *Characteristics of IoT search*

IoT Search refers to a system that can quickly and accurately obtain various physical entities' information in real time from the IoT and sensor networks according to certain strategies and methods. The technology of IoT search helps us fully integrate various types of resources and data. With the rapid development of IoT, IoT search will be widely applied in many fields, such as medical treatment, education, transportation, social networking and so on. Some researchers show that, large searches in cyberspace, especially IoT searches, could greatly save user's time and improve work efficiency, which will greatly impact the global economy in the future [2].

IoT search covers a multiplicity sensors, cameras, SCADA networks and so on. The search engine of IoT support is multidimensional search, such as temporal dimension search, spatial dimension search, and content dimension search. Content search includes searching for information of people, objects and their status, and so on. Based on the characteristics of multidimensional search, the IoT search engine could provide many new search services in addition to those provided by the traditional Internet search engine. First, the multimedia information search service, such as the Semantic Web based IoT search engine [3], has a social and sensor network-based multimedia search engine [50, 51]. Second, the object state information real-time search service includes searching attributes, positions, and trajectories information of the object, such as an RFID tag-based real-time search engine [46-55]. Third, the people search service can discover people's social relationships by analyzing online social networks [53, 54].

By summarizing the above research works of IoT search, it is easy to find that data and service search, discovery, and access control methods and solutions are facing many new challenges in the IoT environment. Because of the distribution, scale,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.2969326, IEEE Internet of Things Journal

heterogeneity, and dynamics of the IoT environment, data and services should be discovered, ranked, selected, accessed, integrated, and understood efficiently from various resources. In Table II, we summarize the differences between IoT search and traditional Internet search. For traditional Internet search, information retrieval technology is used for keyword-based matches. However, for IoT search, spatiotemporal search and value-based search are also required by users, while the search content includes information, people, and objects.

TABLE II
STATE-OF-THE-ART OF POLICY MINING ALGORITHMS

	Internet Search	**IoT Sear**
	Static Web Search	Spatiotemporal
s	Ranked pages	Multimodal data attributes, traject
	Do the best	Accurate and r

While the IoT search provides convenience for our daily life, it also needs to use a large number of private information and data, such as personal health information, location information, social relationship information and so on. Through the IoT search engine, these private data could be shared with other entities without an effective access control mechanism. Therefore, preventing unauthorized search of resources and data is one of the strong demands of IoT search.

B. Requirements for access control in IoT search

Different from the traditional environment of the single-domain search service, as shown in Figure 3, the IoT search service is composed of several search engine agents that are deployed in different networks and systems. Resources and data are exchanged and shared across different management domains. During this process, different access control policies, models and mechanisms are adopted in different networks and systems, while different levels of data privacy and security attributes are defined separately. Traditional access control models and mechanisms cannot be applied to the IoT search environment directly.

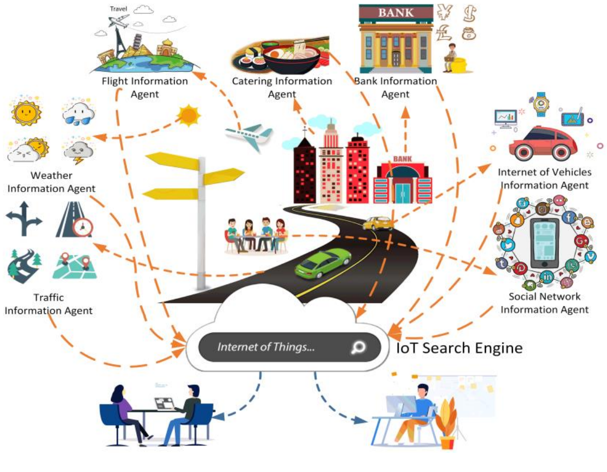
Travel
BANK
Flight Information Agent
Catering Information Agent
Bank Information Agent
Weather Information Agent
BANK
Internet of Vehicles Information Agent
Traffic Information Agent
Social Network Information Agent
Internet of Things...
IoT Search Engine

Figure 3. Schema of IoT search service.

To support access control in IoT search, we summarize a taxonomy requirement based on the characteristics of IoT search that we have discussed in the previous section. Access control policy management includes collecting and constructing access control policies to implement policy description and matching. There are many challenges in access control policy management for IoT search, such as integrating heterogeneous policies of different agents, policy detection, policy conflict resolution, user permission adjustment, policy matching, and so on. The summarized requirements can be organized into two main classes. The first class is access control policy composition, which can be divided into policy standardization and policy conflict resolution. The second class is access control policy authoring, which includes permission assignment and policy matching.

(1) *Access Control Policy Combination and Conflict Resolution.* IoT search is a typical multidomain environment, which is composed of different search agents. Depending on different access control requirements of each domain, different access control policies need to be integrated to ensure the security of resources and data shared across different domains. Policy composition consists of two steps:

a) *Policy Standardization and Combination.* This represents different access control policies in a standardized way. Then, different access control policies are combined to implement unified access control of resources cross different domains.

b) *Policy Conflict Detection and Resolution.* IoT search needs to address a large number of multiparty shared resources. Access control policy conflicts could be derived because different resource subjects have different security requirements. Therefore, policy conflict identification and resolution are very important requirements of access control for IoT search. Two types of policy conflict resolution are included in access control for IoT search:

(2) *Access Control Policy Authoring*. IoT search is a massive, dynamic, open environment, and these characteristics require real-time updating of the access control policy. Access control policy authorization in the IoT search environment includes the following two parts:

a) *Attribute Discovery*. Attribute-based access control is widely used in IoT search because the use attribute as the basic element of the access control policy can effectively solve the problem of dynamic change of massive subjects and objects. How to select appropriate attributes directly affects the performance of the access control system

b) *Policy Mining.* The IoT search platform contains massive data and users, which correspond a vast number of access control policies. An effective policy mining algorithm is the requirement of IoT search.

c) *Policy Authorization.* To grant authority to the right users, authentication is a necessary processing procedure for IoT search.

In the following Sections, we will discuss proposals aiming to achieve these requirements.

IV. Policy Combination and Conflicts Resolution

IOT search has the characteristics of multi-party sharing. In order to achieve the unified authorization of access control strategies in multi-party sharing environment, it is necessary to analyze and combine multi-party strategies. In the process of policy combination, the privacy requirements of different resource owners are different, thus the authorization settings for the same resource may be different. This will lead to policy conflicts which will affect the efficiency of resource dissemination and reduce the quality of search service. Therefore, policy combination and conflict resolution are very important research contents in access control of IoT search.

A. Policy Description Method

Since IoT exposes information that could be private or sensitive, it has brought new challenges to traditional access control models and protocols. An accurate and effective formal description of the security requirements of different users and resources ensures that the access control system responds accurately to various access requests. Therefore, the design of an expressive access control strategy description method is the research focus of access control.

Researchers use policy language to describe the access control strategy, mainly based on arithmetic concepts. There are two types of policy language, either generic access control language standards (such as language) or languages created specifically for use with a single model. “Common Policy Language (CPL)” [56] aims to develop a formal ABAC model that is just sufficiently expressive to capture DAC, MAC and RBAC. eXtensible Access Control Markup Language (XACML), a standard created by the Organization for the Advancement of Structured Information Standards (OASIS) is an XML-based access control policy language that is notable for its support of attribute-based policies and used in multiple access control products [57]. Similarly, security assertion markup language (SAML) [58], also developed by OASIS, provides a standardized markup language and protocol for exchanging attribute-based authorization and authentication information between service providers, identity/attribute providers, and users.

In response to the challenges faced by XACML and SAML in practical applications, researchers proposed different solutions. Aiming at the large amount of volatile data in the grid system, the data are encapsulated and redescribed by extending XACML or combining XACML with SAML. The researcher proposed an authorization framework that supports grid computing combining XACML and SAML [59]. To ensure security in cloud computing, a distributed fine-grained authorization method is proposed by extending the original XACML [60]. [61] proposes a hierarchical ABAC control framework for outsourcing data in cloud computing based on XACML, which increases the flexibility of the access control strategy description method and can effectively make accurate adjustments when the strategy changes. For the problem of limited resources of the IoT perception layer, [62] simplifies XACML, proposes a lightweight XACML and gives a corresponding implementation. Due to the nested recursive matching method in XACML, the computational complexity is higher. The XEngine system proposed in [63] reduces the time complexity of nested recursive matching in XACML by transforming XACML policy rules and requests into digital representations, and improves the efficiency of policy matching. However, the auxiliary arithmetic data structure introduced when translating the original strategy into a digital form introduces an extra amount of computation.

B. Policy and Model Combination

To coordinate different access control policies between different domains and implement unified access control of resources, it is necessary to combine different access control policies. As summarized in [64], much efforts have been performed in the application of traditional access control methods to IoT scenarios, such as introducing ABAC in web services into IoT networks to reduce the number of rules.

To combine security policies, [65] proposes an expression of a triples collection with an algebraic operator. The authors express the policies as a collection of triples consisting of subjects, objects, and actions, with algebraic operators such as conjunction, subtraction, addition, etc. This method has a certain universality, which provides a basis for subsequent research. However, the simple intersection, intersection, and difference operations cannot accurately reflect the true synthesis strategy. [66] merges the access strategies, effectively realizes the calculation of synthetic algebra, and provides a new solution for the synthesis of access control strategies by transforming the access control policy into a multiterminal binary policy tree. On this basis, [67] designed a strategy similarity analysis method based on MTBDD, by constructing a policy query tree according to a user's query mechanism for policy query analysis, while [68] proposes a fine-grained strategy to synthesize algebra by combining MTBDD with three-valued logic. However, the expression of three-valued logic is relatively simple. When multiple strategies need to be cooperatively determined and cannot describe the relationship between multiple strategies, accurate access control decisions cannot be made based only on three-valued logic. In response to this problem, the researchers have proposed a method based on four-valued logic [69], six-valued logic [70] or eight-valued logic [71] to extend the formal description of the XACML strategy and strategy synthesis.

Literature [72] indicates that prior work has focused on the design of unsupervised conflict resolution mechanisms, and relationship-based access control (ReBAC) to support multiple ownership, in which a policy negotiation protocol is in place for co-owners to determine and provide consent to an access control policy in a structured manner. As mentioned in [25], which summarizes the research and open problems in ABAC, hybrid models of ABAC aim to combine attributes into existing models of access control or to extend the traditional models with identity-less or policy-based access control concepts. Thus, [73] proposes ARBAC (attribute and role-based access control) that has an advantage of both ABAC and RBAC to fulfill the needs of the highly distributed network environment, and performs a conflict detection and policy optimization. However, as mentioned in [74], authorization frameworks such as RBAC and ABAC (attribute-based access control) do not provide sufficient scalable, manageable, and effective mechanisms to support distributed systems with many interacting services and the dynamic and scaling needs of IoT text. A problem common to ACLs (access control lists), RBAC and ABAC is that in these systems, it is hard to enforce the principle of least privilege access.

For such reasons and other limitations of ABAC, researchers have tried to integrate more information, such as context or location, with ABAC to enhance the access model. [75] proposes the CSAAC model, which combines the RBAC and ABAC with extra contexts-states-awareness. The proposed model is implemented by using Semantic Web technologies with a sample ontology for the model and some access control policies in SWRL (Semantic Web Rule Language). To guarantee fairness, some game theory models such as negotiation models are considered to be included as future works. [76] proposes location-constrained access control model and verification methods. The authors use the environment model to describe the static topology configuration of cyber space and physical space, while using the LCRBAC model to describe dynamic behaviors of cyber entities and physical entities. They also use the reaction rule and policy modification proposals based on the verification results on the labeled transition system to utilize the cyber-physical interactions.

C. Conflicts Detection and Resolution

To ensure secure and accurate access to information in IoT search, it is necessary to accurately identify and eliminate access control policy conflicts. This leads to policy conflicts when multiparty policies are merged. These policy conflicts must be accurately resolved to ensure search service quality.

Typically, two types of conflicts, inconsistent policy conflicts and coexistent conflicts, are the research focus. Much research has been conducted on the detection and resolution of nonconformance policy conflicts. For instance, concepts of privacy loss, communication revenue and relationship strength are introduced to detect and resolve the conflicts. Researchers quantify the privacy loss and communication revenue caused by policy conflict by introducing the concept of data privacy level and propose a conflict resolution mechanism based on game theory [77]. To solve this problem, [78] uses the relationship strength and other attributes to calculate the impact of resource conflicts on user decision-making and proposes an adaptive access control strategy conflict resolution mechanism. In addition, [79] proposes a relationship-based access control strategy conflict resolution technique by defining different subject-permission mappings, object-permission mappings and inter privilege transfer relationships.

According to the expression and solution method, there are four commonly used techniques in policy conflict detection and resolution: naming description language, formal logic, ontology reasoning and directed graphs. The detection method based on description language can detect the access control strategy of multiple models. It has the characteristics of a simple structure and is object-oriented, so it is easier to master [80]. However, the detection method can only be applied to a specific description language, and the application scope has certain limitations. The formal logic-based detection method detects the existence of a conflicting strategy through logical reasoning, that is, it performs policy detection in the inference process. Through the strict display of logical reasoning, the detection process is closely integrated with the reasoning process, and then the relevant policy conflicts are detected in the reasoning process [81]. However, in the implementation process, the strategy administrator must not only have a solid application logic foundation but also have a development foundation. The ability of the corresponding strategic logic reasoning verification tool and the application of the form-based detection method for policy detection further improve the basic knowledge requirements for the administrator, and the implementation process is more complicated. The ontology-based conflict detection method has its own description and reasoning ability, which is more powerful in the process of heterogeneous network interoperability [82]. The limitation is that the ontology library may be overreliant on the process of policy detection, and the construction process of the ontology library itself is complex and cumbersome. Once there is a problem in the process of building the ontology library, it will directly affect the detection result. The policy conflict detection method based on a directed graph avoids the complex formal proof process, transforms the abstract policy conflict into the visual graph structure, and transforms the policy conflict detection problem into the

TABLE III
COMPARISON OF OUR SURVEY ON CONFLICTS TO OTHER RELATED WORKS

	Our Survey	Samarati & Vimercati [15]	Suhendra [16]	Asim & Malik [24]	Paci et al. [26]
Type of Conflicts					
Inconsistent Policy Conflicts	✓	✓	✓	✓	✓
Coexistent Policy Conflicts	✓				✓
Expression Methods					
naming description language	✓				
formal logic	✓	✓	✓	✓	✓
ontology reasoning	✓				
directed graphs	✓	✓	✓	✓	✓
Conflict Solution Type					
Static	✓	✓	✓	✓	✓
Semiautomated	✓				✓

connection of the triplet or directed graph nodes [83, 84]. The traditional access control model separates the subject and the object for policy detection and does not consider the objective connection between the subject and the object in the access control detection.

Most existing studies about conflict detection and resolution still require the strategy makers to manually participate in the adjustment of the strategy, which is subjective and lacks flexibility. In addition, there is no effective strategy conflict detection and resolution mechanism for strategic conflicts in the new environment of coexistent conflicts. Thus, researchers try to utilize modern techniques such as AI to design semiautomated methods. [85] formulates the incentive mechanism for cooperative intrusion detection as an evolutionary game and achieves an optimal solution to help nodes decide whether to participate in detection or not. The proposed mechanism can contend with the problems wherein cooperative nodes do not own complete knowledge about other nodes. [86] presents a mechanism to resolve conflicts among the services provided by IoT devices in such environments, by reformulating conflict resolution as a planning problem, creating a semantic policy framework for detecting conflicts within an IoT environment, and using planning with soft constraints (preferences) to resolve conflicts that arise when fulfilling multiple goals using varied services. [26] provides a thorough analysis of existing access control models and systems tailored to community-centered collaborative systems. As the authors proposed, in case of inconsistencies, rather than applying blanket policies, access control mechanisms should support easy-to-use semiautomated conflict resolution methods and enable transparent data management in a coherent fashion. We compare our survey to other related works of conflict types, expression methods and conflict solution types in table III.

V. Access Authorization

IoT security vulnerabilities include insufficient authentication and authorization, lack of transport encryption, insecure web interfaces, and insecure software updates, etc. IoT security in security mechanisms is built from the ground up. Therefore, every actor such as user, device, app and process must have a unique identity. All network communication must be encrypted and mutually authenticated. All access to device capabilities must be authorized and auditable.

A. Attribute Discovery Mechanism

The accessing entities and the accessed entities have many intrinsic attributes. How to select appropriate attributes directly affects performance of access control system. The conceptual model of attribute aggregation fuses the many user attributes contained in multiple IdPs (Identity Providers) and further generates a complete user attribute based on the reliability of the information provided by each LS (Linking Service) [87]. Because not considering the dynamic changes of IdP's reputation, an attribute aggregation method based on multi-node cooperation [88] is proposed to obtain attributes from multiple mutually cooperative nodes when an attribute that the system does not recognize appears. The nodes participating in cooperation calculate the reputation values of the neighboring nodes based on their background knowledge, and then upload the reputation value when the SPs (service providers) makes the attribute query. After the SP calculates all the reputation values, it determines whether the node providing data is trusted according to the preset threshold, and filters the information provided by the untrusted node. This method solves the problem of reputation in attribute aggregation. although solving multi-attribute aggregation problems by multi vector convergence operator [89], but the solution does not consider the security (for example: privacy exposure) caused by attribute aggregation. Thus, several recent researches have been conducted for the privacy-preserving for the IoT based services. PAgIoT which is a privacy preserving aggregation protocol suitable for IoT settings enables multi-attribute aggregation for groups of entities while allowing for privacy-preserving value correlation [90]. This mechanism enables aggregating data concerning several attributes of each entity in a single operation ensuring data authenticity and privacy. Literature [91, 92] achieves the scheme of attribute aggregation for privacy protection with OpenID or pseudo-ID. Location anonymization attempts to make user's location indistinguishable from a certain number of other users in open environment so that it is one of most important techniques of IoT. The FINE framework working for mobile devices employs anonymous attribute based on encryption technique [93]. Attribute discovery depends on data aggregation which is responsible for increasing the network lifetime and reducing the energy consumption [94]. Literature [95] proposed a method of lifetime balanced data aggregation, in which the aggregation delays of adjacent devices are adjusted together in a collaborative fashion.

Because the data aggregation has an important role in the IoT, there is not any systematic and comprehensive study about analyzing its important mechanisms [95]. In addition, although the research on attribute discovery of IoT has achieved certain research results, the mining method of independent and complete attribute for large scale data are lacking in noisy environments. The independent and complete set of attributes is the basis for building ABAC. The independence of the attributes ensures that the set of attributes required to build access control does not contain redundant attributes with repeated meanings. And the completeness of the attributes ensures that the attribute set includes all the attributes needed to accurately respond to the access request. Therefore, under the condition of satisfying independent and complete constraints, how to design an excellent algorithm to get the best query attribute set with low computational complexity is the key scientific problem to be solved in the future.

B. Policy Mining

Access control is one of the essential services of information systems that protect underlying data from unauthorized access and improper modification. Although access control policies can be specified by enumerating each instance of authorized access, modern access control policy models require a more abstract and flexible approach to specifying authorization.

(1) *Security technology mining.* Most of the nodes in IoT lack enough storage capacity, power and CPUs; for this reason,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.2969326, IEEE Internet of Things Journal

directly applying some security techniques such as a public key encryption algorithm used in traditional networks cannot be accomplished. Moreover, a great number of RFID systems fall short of suitable authentication mechanisms, such that intruders can track the tagged node and then read or modify the carried data[96]. Therefore, security technologies of authentication and authorization used in perception layer, network layer and application layer in IoT are shown in Table IV.

(2) *Mode mining.* According to the topology of nodes, three policy modes can be used in IoT.

a) *Centralized Policy*. The node sends the access request to a specialized server that provides centralized authentication and authorization[97]. This mode is easy to implement and only suitable for small-scale nodes. As the number of nodes increases, the burden of the server increases and the efficiency decreases. At the same time, the centralized server is vulnerable to network attacks, affecting the robustness of the system.

b) *Distributed Policy*. There are no centralized authentication and authorization servers[98]. In this mode, severs have the same data copies used to authenticate and authorize. This mode enables the system to have strong robustness. However, with some nodes changing, all data copies in severs need to be updated synchronously.

c) *Locally Centralized and Globally Distributed Policy*. This mode extracts the advantages of the centralized policy and distributed policy. Nodes only register or require access authorization to the local centralized domain sever[99]. The trust relationship between domain severs is globally distributed and built by certificates. In this view, for nodes, their authentication and authorization are limited to local areas. Meanwhile, they can obtain the access right to other domains by the trust relationship between domain severs. This mode is flexible and easy to expand.

The selection of policy modes should consider not only the new authentication framework and access authorization model but also the integration of existing devices. In practical applications, according to the scale of the system and the nature of the nodes, the policy mode should be finally determined.

(3) *Characteristics mining.* It is essential to mine and analyze the node characteristics, such as attribute characteristics[100], role characteristics[101], capability characteristics[102], biometrics characteristics, and so on. Attribute mining is represented by ABAC. In ABAC, access rules can be determined based on various attributes, such subject attributes, object attributes, environment attributes, and so on. Role mining is represented by RBAC. The RBAC is composed of static elements, such as users, roles, permissions, conditions and devices. The relationship among these elements is many-to-many. Therefore, mining the relation is one of the core tasks in RBAC. Capabilities mining is the lookup of the mapping of capabilities into roles and permissions in each domain, such as a key, a ticket, a token, etc. In different domains, the same user has different access rights. Some devices in IoT have mobility, such as a mobile pedometer and vehicle equipment. Therefore, mining the invariant physical characteristics of mobile devices become the key emphasis, such as in biometrics, device products' ID, and so on. Biometrics characteristics include voice, gait, etc.

C. Authorization model

The authorization model involves the following two phases. According to system requirements, we should first determine a security policy mode and the technology of each layer discussed in last sub-section. Then, we must design the access control model to encapsulate the defined policy[103]. As time goes by or the position changes, the access rights of users and devices are changing. Therefore, how to realize the change and revocation of access authority has become a problem that needs to be studied. We describe the authorization by category as follows.

TABLE IV
SECURITY POLICY

Type	Algorithm	Function	Layer
Mathematical Theory	AES/ AES-CCM	Data Encryption	Perception Layer
	RAS/ECC	Asymmetric Encryption	
	DH	Key Agreement	
Security Protocol	TLS/SSL/IPSec/ PPSK	Authenticity	Network Layer
Mathematical Theory/Physical characteristics	RSA/DSA/ECC	Authenticity/ Access Control	Application Layer
	Biometric Recognition		
	Physical Characteristic Recognition		

(1) *Based on ABAC.* The subject and the object are all identified through the attributes associated with characteristics [103]. In the ABAC model, the user is granted an appropriate access right according to his attributes when submitting an access request. Because attributes might carry users' privacy information, whose leakage severely obstructs the further development of ABAC, recent research has focused on the premise of ensuring user privacy. Yang Xu[100] proposed the privacy-preserving ABAC (P-ABAC) scheme to defend against privacy leakage. In the P-ABAC, the sensitive attributes are handled on the user side by using homomorphic encryption. The authorization service is also able to make accurate access decisions according to the received attribute ciphertext with the help of the homomorphic encryption-based secure multiparty computation techniques, while learning no privacy information.

(2) *Based on RBAC.* RBAC provides an authorization framework that specifies users' access to resources based on their roles and supports security principles such as least privilege, partition of administrative functions and separation of duties. The pure RBAC model has a role explosion problem when the amount of resources grows or the access rules cover many administrative domains. To use in more IoT scenarios, Spiess Patrik[104] proposed a service-based RBAC model in

which devices make their functionality as a standard web service. To achieve a further scalable, flexible and lightweight access control mechanism, Guoping Zhang[105] proposed an extended RBAC model using the context information, which can be used as context constraints. Ezedine Barka [106] proposed RBAC in the Web of Things (WoTs) on the smart objects via the web.

(3) *Based on CapBAC.* In the CapBAC model, the users are granted access based on a token of authority (such as a key, a ticket, and so on), as well as the authorization chain. Identity management is not a critical role, which provides vast advantages, especially when carrying out a user's access control in cross-domain scenarios. Gusmeroli [107] discusses the difference of ACL and CapBAC. In the ACL model, the responsibility of access control is on the server provider side. In contrast, the responsibility of access control is on the user side in the CapBAC model. Ronghua Xu[108] proposed a BlendCAC model which is a blockchain-enabled decentralized CapBAC. In the BlendCAC model, a robust identity-based capability token management strategy is proposed, which takes advantage of a smart contract for registering, propagation and revocation of the access authorization. Luciano Barreto[109] proposed a cloud-based authentication framework. The IoT cloud allows users to access IoT-based resources and capabilities to manage many different intelligent pervasive environments. Ronghua Xu[110] proposed a federated CapBAC (FedCAC) framework in large-scale IoT systems. FedCAC presented an identity-based capability token management strategy that involves registering, propagation and revocation of the access.

(4) *Based on Usage Control (UCON)*. The UCON model in [111] put forward the problem of authorization in a continuous way before the access execution, during the execution and afterwards. Moreover, a variety of access attributes are supported, which means the granted access can be revoked and the usage can be cancelled while the user access is in progress. Aliaksandr Lazouski[112] points out that usage control is a novel and promising approach for access control in open, distributed, heterogeneous and network-connected computer environments. Xinwen Zhang [113] proposed a UCON-based security framework PEI that follows a layered approach with policy, enforcement and implementation of models. In the policy model layer, UCON policies are specified with predicates on subject and object attributes, along with system attributes as conditional constraints and user actions as obligations. The conditions constraints in UCON can be used to carry out context-based authorizations in temporary collaborations. It should be pointed out that the value of the access attribute can be modified only by an administrative action and not by the user's activity. Zhang Guoping [114] pointed out that further research of UCON will make the authorization for the access control of IoT easier and more feasible. In reference [115], the UCON helps the fine-grained dynamic control of access that is achieved by monitoring and evaluating the attributes defined within a dedicated security. To improve the scalability and run-time efficiency of the UCON, the policy risk aggregation framework is suggested as an addition to UCON for dynamic role allocation and service grouping management. Antonio La [116] apply UCON to increase the security of the MQTT protocol by enabling a fine-grained dynamic control of the rights of subscribers to access data and data streams over time.

(5) *Based on Organizational-Based Access Control (OrBAC).* OrBAC has extended the RBAC model and introduces the notion of "organization" as a new dimension. Khalifa Toumi [117] proposed the Trust-orBAC model, which adds the notion of trust management to OrBAC. Trust-orBAC defines two dynamic trust vectors, where one is used for the organizations and another one is used for users with different parameters. To enhance different organizations collaborating and avoid malicious behavior, Nawal Ait Aali [118] also proposed the Tr-OrBAC model into which Trust is integrated. Imane Bouij-Pasquier [119] proposed the SmartOrBAC model, separating the problem into different functional layers. SmartOrBAC distributes processing costs between constrained devices and less constrained ones. To restrict the access to the sensitive data that are out of the control of the data owner, it ensures that some users can access these data according to the plan of tasks/actions in advance. Therefore, Khalida Guesmia [120] proposed an extension of the OrBAC model using a temporal nonmonotonic description logic. This logic can used to formally represent the policy rules as a hierarchical plan. The plan includes a set of ordered tasks that may admit exceptions in special cases. When the access request is made, the proposed OrBAC model can dynamically infer the appropriate sequence of actions according to the current context environment.

(6) *Based on Biometrics Features or Blockchain.* With the richness of IoT devices, biofeatures are fast becoming one of the key elements used to authenticate the IoT devices and their users. Mohamed Amine Ferrag [121] presented a comprehensive review on the biofeatures used by authentication and authorization schemes for mobile IoT devices, which include voice, fingerprint and so on.

Aafaf Ouaddah [122] proposed a framework named FairAccess for access control in IoT based on the blockchain. FairAccess introduces new types of transactions that are used to grant, get, delegate, and revoke access. In FairAccess, the access token is required to obtain access to a protected resource, but the access token cannot be triggered until access control conditions are satisfied. During implementation using the UTXO model of blockchain, the main limitation of FairAccess is the real time and bloat blockchain issue. Oscar Novo [123] discusses the combination issue of blockchain, access control and IoT. The architecture proposed by it is a fully distributed access control system, while access control information is stored and distributed using blockchain technology. Nodes can use the blockchain interface to store and globally access the access control policy of specific devices.

(7) *Based on Open Authorization (OAuth).* OAuth is an access control framework for clients accessing resources on web servers. Most conventional solutions for both web and cloud applications cannot be directly used in the context environment. Savio Sciancalepore [124] proposed the OAuth-IoT framework for access control. OAuth-IoT leverages and properly

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.2969326, IEEE Internet of Things Journal

harmonizes existing open-standards. OAuth-IoT natively supports any token format for properly handling applications' authentication and authorization. Federico Fernández [125] proposed an OAuth model that allows managing roles and permissions for an application-scoped authorization. For all the required information that is provided with a token, OAuth 2.0 makes authorization extremely light. Furthermore, authorization can be delegated to an external system, so that an as-a-service access control mechanism is provided. Jalaluddin Khan [126] proposed an authentication scheme based on OAuth 2.0, which allows only authorized as true users by comparing user information and access tokens in the security manager local database.

VI. Open Research Issues

Access control has a long research and development history. Many access control models have already been applied in real-world applications. With the development of IoT technologies, various information resources are deeply integrated for comprehensive applications. The characteristics of IoT systems, such as the node heterogeneity, the open environment, and the multiparty sharing of resources, raise new requirements to the access control models and mechanisms. Despite these issues, many research efforts have focused on proposing novel models and mechanisms to provide fine-grained access to IoT systems and their resources. There are still many important issues and challenges that need to be addressed.

(1) *Policy conflict caused by different authorizations.* Our study introduced many access control models for IoT environments, such as RBAC and ABAC. Many RBAC-related proposals focus on incorporating interpersonal relationships in access decision making; however, they assume that resources are owned by a single entity, ignoring the characteristic of multiparty sharing. Many ABAC-related proposals use a simple strategy to address this situation, such as the access can be authorized only when all users allow the access. However, this strategy is too strict to be used in real-world applications since it will reduce the availability of resources. More efforts are required to focus on policy conflict resolution caused by different authorizations, which can help to improve the automation of the policy composition and the conflict resolution.

(2) *Policy conflict caused by multiparty relationship.* This kind of policy conflict problem is due to the novel characteristics of the IoT search environment. In the process of multiparty access control policy integration, the policies of different agents contain many constraints. One resource may have different owners who will set different constraints on resource access. Depending on these constraints, several access control decisions could be obtained that correspond to each resource. Each access control decision can satisfy the requirements of individual users. However, the decisions may be mutually exclusive. The combination of these constraints often causes inconsistencies and conflicts. Therefore, how to quickly and dynamically select and adjust access control decisions for different users is an urgent problem to be solved.

(3) *Attribute-Permission Assignment within Noise Data.* IOT search is a multidomain collaborative environment. Different access control policies are used in different domains. To implement unified management of an access control policy, other access control models need to be converted to the ABAC model since attributes act as basic elements of ABAC, and the access control decision is made based on the set of attributes of the requester. That makes ABAC fit for the IoT search environment by separating the policy management from the access control decision. To convert other types of policies into ABAC, it is necessary to generate high-quality attribute-permission correspondences based on role-permission and user-permission relations. In particular, noise data often exist in the original user-permission relations, which greatly affect the accuracy of the policy generation and bring great security risks to access control systems. How to address the attribute-permission assignment within noise data is a considerable research challenge in control access for IoT search.

(4) Modeling and Evaluation of IoT Security Search. We need to balance the quality, security and efficiency during the process of the IoT search. With the rapid development of the Internet of Things, the security of the Internet of Things has received more attention. Modeling and simulation (MS) have been successfully applied to many similar complex security problems in the past decades. IoT has a unique address and uses standard communication protocols to communicate, so MS methods and tools are also suitable for solving IoT problems. However, little work has been done on the modeling and evaluation of IoT security search.

(5) *Authentication and Anonymous Protection of Physical Devices in the IoT.* In the field of industrial control security IoT, there are many authentication methods aiming at real-time communication between the cloud platform and sensing devices. However, most of the time, the efficiency and security of these methods cannot be guaranteed at the same time. Therefore, the technology of device authentication and anonymity protection should be given more attention to ensure the trustworthiness of the data source, privacy and data availability.

VII.Conclusion

This article focusses on reviewing the existing access control models and systems in the IoT search environment. First, we introduced the background of access control. Then, two main classes of requirements are identified to support access control in IoT search. One is access control policy composition, and the other is access control policy authoring. We surveyed the current state-of-the-art literature by matching these two requirements and introduced the corresponding models and systems. In particular, we summarized the open research issues to help guide future research. Our goal is to drive research and development of novel access control models and mechanisms for the IoT search environment.

Acknowledgment

The authors express their sincere appreciation to the editors and the anonymous reviewers for their helpful comments.

References

[1] Mohammed Mahmoud Abd El-Hamid Nasr, Mohamed Fared Zaghloul, Reda Abo Elez and Ahmed Rashad Khalifa. The Future of 5G Technology Present & Previous Generations. International Journal of Scientific & Engineering Research, 2018, 9(9): 511-535.

[2] Fang B.X., Yan J., Li X.Y., Li A.P., Wu X.D. Big Search in Cyberspace. IEEE Transactions on Knowledge and Data Engineering, 2017, 29(9), DOI: 10.1109/TKDE.2017.2699675.

[3] Kamilaris A., Yumusak A., Ali M. WOTS2E: A search engine for a Semantic Web of Things, Proceedings of the IEEE World Forum on Internet of Things, 2016, DOI: 10.1109/WF-IoT.2016.7845448

[4] Tian Z., Li M., Qiu M., Sun Y., Su S.. Block-DEF: A Secure Digital Evidence Framework using Blockchain, Information Sciences. 491(2019) 151-165. DOI: 10.1016/j.ins.2019.04.011.

[5] Tan Q., Gao Y., Shi J., Wang X., Fang B. and Tian Z., Toward a Comprehensive Insight Into the Eclipse Attacks of Tor Hidden Services, IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1584-1593, April 2019.

[6] ISO/IEC 29100:2011 - Information technology - Security techniques-Privacy framework, JTC 1/SC 27 Std., 2011. [Online].Available: http://www.iso.org/iso/isocatalogue/cataloguetc/cataloguedetail.htm?csnumber=45123

[7] Foukia N., Billard D. and Solana E. PISCES: A framework for privacy by design in IoT. 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 706-713.

[8] Skendžić A., Kovačić B. and Tijan E. General data protection regulation — Protection of personal data in an organization. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018, pp. 1370-1375.

[9] Karyda M., Gritzalis S., Park J. H., Kokolakis S. Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. Internet Research, 2009, 19(2): pp.194-208.

[10] Cate, F.H. The failure of fair information practice principles. Winn, J.K. (Ed.), Consumer Protection in the Age of the Information Economy, Ashgate, Aldershot.

[11] Tian Z., Gao X., Su S., Qiu J., Du X. and Guizani M. Evaluating Reputation Management Schemes of Internet of Vehicles based on Evolutionary Game Theory. IEEE Transactions on Vehicular Technology. 2019. Vol 68(6): 5971-5980.

[12] Tian Z., Su S., Shi W., Du X., Guizani M. and Yu X.. A Data-driven Method for Future Internet Route Decision Modeling. Future Generation Computer Systems. 2019. Vol. 95, 212-220.

[13] Cerf V. G. Access Control and the Internet of Things. IEEE Internet Computing, 2015, 19(5): 96-c3.

[14] Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 2015, 76: 146-164.

[15] Samarati P., Vimercati S.C.D. Access Control: Policies, Models, and Mechanisms. In: Focardi R., Gorrieri R. (eds) Foundations of Security Analysis and Design. FOSAD 2000. Lecture Notes in Computer Science, vol 2171. Springer, Berlin, Heidelberg.

[16] Suhendra V. A Survey on Access Control Deployment. In: Kim T., Adeli H., Fang W., Villalba J.G., Arnett K.P., Khan M.K. (eds) Security Technology. SecTech 2011. Communications in Computer and Information Science, vol 259. Springer, Berlin, Heidelberg.

[17] Atzori L., Iera A., Morabito G. The Internet of Things: A survey. Computer Networks, 54(2010): 2787-2805.

[18] Cui B. and Xue T. Design and realization of an intelligent access control system based on voice recognition. 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, Sanya, 2009: 229-232.

[19] Saparkhojayev N., Dauitbayeva A., Nurtayev A. and Baimenshina G. NFC-enabled access control and management system. 2014 International Conference on Web and Open Access to Learning (ICWOAL), Dubai, 2014, pp. 1-4.

[20] Qing X., Fei Y., Wenchao X. and Yinxiao M. Discretization Algorithm Based on Attribute Importance and Incompatible Degrees. 2012 International Conference on Computer Science and Service System, Nanjing, 2012, pp. 110-112.

[21] Tolone W., Ahn G.J., Pai T., and Hong S.P. Access control in collaborative systems. ACM Computing Surveys, 2005, 37, 1: 29–41. DOI: http://dx.doi.org/10.1145/1057977.1057979.

[22] Carminati Barbara., Ferrari Elena. Access control and privacy in web-based social networks. International Journal of Web Information Systems, 4(4): 395-415.

[23] Kayes I. and Iamnitchi A. A survey on privacy and security in online social networks. Computer Science, 2015, DOI: 10.1016/j.osnem.2017.09.001.

[24] Asim Y. and Malik A.K. A Survey on Access Control Techniques for Social Networks. Innovative Solutions for Access Control Management, 2016, IGI Global, 1–32. DOI: http://dx.doi.org/10.4018/978-1-5225-0448-1.ch001.

[25] Servos D., Osborn S.L. Current Research and Open Problems in Attribute-Based Access Control. ACM Computing Surveys, 2017, 49(4), DOI: 10.1145/3007204.

[26] Paci F., Squicciarinni A., Zannone N. Survey on Access Control for Community-Centered Collaborative Systems. ACM Computing Surveys, 2018, 51(1). DOI: https://doi.org/10.1145/3146025.

[27] Lapadula L. J., Bell D. E. Secure Computer Systems: Mathematical Foundations, MTR-2547, Volume 1, November 1973.

[28] Biba, K.J. Integrity Considerations for Secure Computer Systems, NTIS AD-A039 324, MTR 3153,ESD-TR-76-372, MITRE Corporation, Bedford, MA, 1977.

[29] Downs D.D., Rub J.R., Kung K.C., Jordan C.S. Issues in Discretionary Access Control. Proceedings of the IEEE Symposium on Security and Privacy, 1985, p. 208-218.

[30] Bertino E., Jajodia S., Samarati P. Enforcing Mandatory Access Control in Object Bases, Proceedings of the Conference Workshop on Security for Object-Oriented Systems, Berlin: Springer, 1993: 96-116.

[31] Ferraiolo D. F., R. Sandhu. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

[32] Bonatti, P. A., Samarati, P. A uniform framework for regulating service access and information release on the web. Journal of Computer Security, 2002, 10(3): 241-272.

[33] Bertino, E., Bonatti, P. A., Ferrari, E. TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security, 2001, 4(3): 191-233.

[34] Geepalla E., Bordbar B. and Du X. Spatio-temporal Role Based Access Control for Physical Access Control Systems. 2013 Fourth International Conference on Emerging Security Technologies, Cambridge, 2013: 39-42.

[35] Park, J., Ravi S. Towards usage control models: beyond traditional access control, Proceeding of the 7th ACM Symposium on Access Control Models and Technologies, New York, 2002: 57-64.

[36] Sahai, A., Waters, B. Fuzzy Identity-Based Encryption. Proceeding of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Berlin: Springer, 2005: 457-473.

[37] Goyal V., Pandey O., Sahai A., Waters B. Attribute-based encryption for fine-grained access control of encrypted data, Proceeding of the 13th ACM Conference on Computer and Communications Security, New York, 2006: 89-98.

[38] 23 Bethencourt, J., Waters, B. Ciphertext-Policy Attribute-Based Encryption, Proceeding of IEEE Symposium on Security and Privacy, Piscataway, NJ, 2007: 321-334.

[39] Lei Z., Sun H., Liu Z. and Liang T. Media access control manner with QoS for control network. 2008 27th Chinese Control Conference, Kunming, 2008: 204-207.

[40] Liu Q., Zhang H., Wan J. and Chen X. An Access Control Model for Resource Sharing Based on the Role-Based Access Control Intended for Multi-Domain Manufacturing Internet of Things. IEEE Access, 2017, 5: 7001-7011.

[41] Oh C., Hwang D. and Lee T. Joint Access Control and Resource Allocation for Concurrent and Massive Access of M2M Devices. IEEE Transactions on Wireless Communications, 2015, 14(8): 4182-4192.

[42] Zhang P., Liu X. and Tao L. Design of Security Access Control System of Adaptive Wireless Gateway. 2008 International Symposium on Information Science and Engineering, Shanghai, 2008: 20-23.

[43] Tian Z., Shi W., Wang Y., Zhu C., Du X., Su S., Sun Y., and Guizani N. Real Time Lateral Movement Detection based on Evidence Reasoning Network for Edge Computing Environment. IEEE Transactions on Industrial Informatics. 2019. Vol 15(7): 4285-4294.

[44] Qiu J., Chai Y., Liu Y., Gu Z., Li S., Tian Z.. Automatic Non-Taxonomic Relation Extraction from Big Data in Smart City. IEEE Access. vol. 6, pp. 74854-74864, 2018. DOI: 10.1109/ACCESS.2018.2881422.

[45] Ding Z. , Chen Z., and Yang Q. *IoT-SVKSearch: a real-time multimodal search engine mechanism for the internet of things*. *Int. J. Commun. Syst*. 2014, 27(6): 871-897, DOI=http://dx.doi.org/10.1002/dac.2647.

[46] Truong C., Römer K. and Chen K. Fuzzy-based sensor search in the Web of Things, 2012 3rd IEEE International Conference on the Internet of Things, Wuxi, 2012, pp: 127-134. DOI: 10.1109/IOT.2012.6402314.

[47] Aberer K., Hauswirth M. and Salehi A. Infrastructure for Data Processing in Large-Scale Interconnected Sensor Networks, 2007 International Conference on Mobile Data Management, Mannheim, 2007: 198-205, DOI: 10.1109/MDM.2007.36.

[48] Grosky W. I., Kansal A., Nath S., Liu J. and Zhao F. SenseWeb: An Infrastructure for Shared Sensing. IEEE MultiMedia, 2007, 14(4): 8-13, DOI: 10.1109/MMUL.2007.82.

[49] Mollah M. B., Azad M. A. K. and Vasilakos A. Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things. IEEE Cloud Computing, 2017, 4(1): 34-42, DOI: 10.1109/MCC.2017.9.

[50] Mendes P. Social-driven internet of connected objects. Proceeding of the Interconnecting Smart Objects with the Internet Workshop, 2011.

[51] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway. A Survey of Key Management Schemes in Wireless Sensor Networks. Journal of Computer Communications, 2007, 30(11-12): 2314-2341.

[52] Shemshadi A., Sheng Q. Z., Qin Y., Sun A., Zhang W. E., and Yao L. Searching for the internet of things: where it is and what it looks like. Personal and Ubiquitous Computing, 2017, 21(6): 1097-1112, DOI: https://doi.org/10.1007/s00779-017-1034-0.

[53] Barnaghi P. and Sheth A. On Searching the Internet of Things: Requirements and Challenges. in IEEE Intelligent Systems, vol. 31, no. 6, pp. 71-75, Nov.-Dec. 2016. DOI: 10.1109/MIS.2016.102.

[54] Chaochaisit W., Bessho M., Koshizuka N. and Sakamura K. Human Localization Sensor Ontology: Enabling OWL 2 DL-Based Search for User's Location-Aware Sensors in the IoT, IEEE Tenth International Conference on Semantic Computing (ICSC), Laguna Hills, CA, 2016: 107-111, DOI: 10.1109/ICSC.2016.31.

[55] X. Du, Y. Xiao, M. Guizani, and H. H. Chen. An Effective Key Management Scheme for Heterogeneous Sensor Networks. Ad Hoc Networks, Elsevier, Vol. 5, Issue 1, pp 24–34, Jan. 2007.

[56] Wang L, Wijesekera D, Jajodia S. A logic-based framework for attribute based access control, ACM Workshop on Formal Methods in Security Engineering. ACM, 2004:45-55.

[57] Simon Godik, Anne Anderson, Bill Parducci, Polar Humenn, and Sekhar Vajjhala. 2002. OASIS eXtensible Access Control Markup Language (XACML). Technical Report. OASIS.

[58] John Hughes and Eve Maler. 2005. Security Assertion Markup Language (SAML) V2.0 Technical Overview. Technical Report. OASIS.

[59] Demchenko Y, Gommans L, De Laat C. Using SAML and XACML for Complex Resource Provisioning in Grid Based Applications, Eighth IEEE International Workshop on Policies for Distributed Systems and Networks. IEEE, 2007:183-187.

[60] Dinh T T, Wang W, Datta A. City on the Sky: Extending XACML for Flexible, Secure Data Sharing on the Cloud. Journal of Grid Computing, 2012, 10(1):151-172.

[61] 55 Liu X, Xia Y, Jiang S, et al. Hierarchical Attribute-Based Access Control with Authentication for Outsourced Data in Cloud Computing, IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE Computer Society, 2013:477-484.

[62] X. Du, M. Guizani, Y. Xiao and H. H. Chen. A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks. IEEE Transactions on Wireless Communications, 2009, 8(3): 1223 - 1229.

[63] Liu A X, Chen F, Hwang J H, et al. Designing Fast and Scalable XACML Policy Evaluation Engines. IEEE Transactions on Computers, 2011, 60(12):1802-1817.

[64] Ranjan A K, Somani G. Access Control and Authentication in the Internet of Things Environment, Connectivity Frameworks for Smart Devices. Springer International Publishing, 2016.

[65] Bonatti, Piero, Vimercati D C D, et al. An algebra for composing access control policies. Acm Transactions on Information & System Security, 2002, 5(1):1-35.

[66] 60 Rao P, Lin D, Bertino E, et al. An algebra for fine-grained integration of XACML policies, ACM Symposium on Access Control MODELS and Technologies. ACM, 2009:63-72.

[67] Li N, Wang Q, Qardaji W, et al. Access control policy combining: theory meets practice, SACMAT 2009, ACM Symposium on Access Control MODELS and Technologies, Stresa, Italy, June 3-5, 2009, Proceedings. DBLP, 2009:135-144.

[68] Rao P, Lin D, Bertino E, et al. EXAM: An Environment for Access Control Policy Analysis and Management, Policies for Distributed Systems and Networks, 2008. POLICY 2008. IEEE Workshop on. IEEE, 2008:238-240.

[69] Bruns G, Huth M. Access control via Belnap logic: Intuitive, expressive, and analyzable policy composition. Acm Transactions on Information & System Security, 2011, 14(1):1-27.

[70] Ramli C D P K, Nielson H R, Nielson F. The Logic of XACML. Formal Aspects of Component Software. Springer Berlin Heidelberg, 2012:205-222.

[71] Ni Q, Bertino E, Lobo J. D-algebra for composing access control policy decisions, Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009:298-309.

[72] Fong P W L. Relationship-based access control: protection model and policy language, ACM Conference on Data and Application Security and Privacy. ACM, 2011:191-202.

[73] Servos D, Osborn S L. HGABAC: Towards a Formal Model of Hierarchical Attribute-Based Access Control, International Symposium on Foundations and Practice of Security. Springer, Cham, 2014:187-204.

[74] Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of Things[J]. Mathematical & Computer Modelling, 2013, 58(5-6):1189-1205.

[75] Yuji Dong, Kaiyu Wan, Xin Huang, Yong Yue. Contexts-States-Aware Access Control for Internet of Things. CSCWD 2018: 666-671.

[76] Baseri Y, Hafid A, Cherkaoui S. Privacy preserving fine-grained location-based access control for mobile cloud[J]. Computers & Security, 2018, 73.

[77] Manshaei M H, Zhu Q, Alpcan T, et al. Game theory meets network security and privacy. Acm Computing Surveys, 2013, 45(3):1-39.

[78] Such J M, Criado N. Resolving Multi-party Privacy Conflicts in Social Media. IEEE Transactions on Knowledge & Data Engineering, 2016, 28(7):1851-1863.

[79] Sarkis L C, Silva V T D, Braga C. Detecting indirect conflicts between access control policies, ACM Symposium on Applied Computing. ACM, 2016:1570-1572.

[80] Batista B , Fernandez M. PonderFlow: A New Policy Specification Language to SDN OpenFlow-based Networks. International Journal on Advances in Networks & Services, 2014, 7(3 and 4):163-172.

[81] Cau A , Janicke H , Moszkowski B . Verification and enforcement of access control policies. Formal Methods in System Design, 2013, 43(3):450-492.

[82] Shaikh R A, Adi K, Logrippo L. A Data Classification Method for Inconsistency and Incompleteness Detection in Access Control Policy Sets. International Journal of Information Security, 2017, 16(1):91-113.

[83] Yao J, Mao B, Xie L. A DAG-Based Security Policy Conflicts Detection Method. Journal of Computer Research & Development, 2005, 42(7).

[84] Shen L , Wang Z , Zhang X , et al. Study on the policy conflict detection in the security management model, 2015 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). IEEE, 2015.

[85] Guo Y., Zhang H., Zhang L., Fang L., Li F. (2018) Incentive Mechanism for Cooperative Intrusion Detection: An Evolutionary Game Approach. In: Shi Y. et al. (eds) Computational Science – ICCS 2018. ICCS 2018. Lecture Notes in Computer Science, vol 10860. Springer, Cham

[86] Emre Göynügür, Sara Bernardini, Geeth de Mel, Kartik Talamadupula, Murat Sensoy. Policy Conflict Resolution in IoT via Planning. Canadian Conference on AI 2017: 169-175.

[87] Chadwick, D W, Inman G. The Trusted Attribute Aggregation Service, Proceedings of IEEE International Conference on Availability, Reliability and Security, Pis-cataway. Pis-cataway, NJ: IEEE, 2013: 1-27.

[88] Jaewon Lee, Heeyoul Kim, Joon Sung Hong. An Attribute Aggregation Architecture with Trust-based Evaluation for Access Control.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.2969326, IEEE Internet of Things Journal

Proceedings of IEEE Network Operations＆Management Symposium. Piscataway, NJ:2008: 1011-1014, DOI: 10.1109/NOMS.2008.4575270

[89] Ghiselli Ricci, R. Mesiar, R. Multi-Attribute Aggregation Operators. Fuzzy Sets and Systems, 2011, 181(1): 1-13.

[90] González-Manzano, J de Fuentes, S Pastrana, et al. PAgIoT-Privacy-preserving Aggregation protocol for Internet of Things. Journal of Network and Computer Applications, 2016 (71): 59-71.

[91] Nakamura M, Nishimura T, Yamaji K, et al. Privacy Preserved Attribute Aggregation to Avoid Correlation of User Activities across Shibboleth SPs. Proceedings of IEEE 37th Annual Computer Software and Applications Conference, 2013:367-372.

[92] X. Zhu, H. Chi and S. Jiang. Using dynamic pseudo-IDs to protect privacy in location-based services. Proceedings of IEEE International Conference on Communications (ICC), 2014: 2307-2312.

[93] J. Shao, R. Lu and X. Lin. FINE: A fine-grained privacy-preserving location-based service framework for mobile devices. IEEE INFOCOM, 2014: 244-252.

[94] Behrouz Pourghebleh, Nima Jafari Navimipour. Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research. Journal of Network and Computer Applications. 2017.

[95] Li, Z., Zhang, W., Qiao, D., Peng, Y., Lifetime balanced data aggregation for the internet of things. Computers & Electrical Engineering. 2017.

[96] Engin Leloglu . A Review of Security Concerns in Internet of Things. Journal of Computer and Communications, 2017, 5, 121-136.

[97] Mahalle Parikshit N, Anggorojati Bayu, Prasad Neeli R, etc. Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. Journal of Cyber Security and Mobility, 2013: 309-348.

[98] Zahid Mahmood, Ata Ullah, Huansheng Ning, etc. Distributed Multiparty Key Management for Efficient Authentication in the Internet of Things. IEEE Access, 2018, 29460–29473.

[99] Hokeun Kim, Eunsuk Kang, Edward A. Lee, David Broman. A toolkit for construction of authorization service infrastructure for the internet of things. Proceedings of IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI),2017,147-158.

[100] Yang Xu, Quanrun Zeng Guojun Wang, etc. A Privacy-Preserving Attribute-Based Access Control Scheme. Proceedings of International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. 2018, 361-370.

[101] Md. Fasiul Alam, Stathes Hadjiefthymiades. Role Assignment in IoT Through Accelerated Hardware. Proceedings of Fifth International Conference on Internet of Things: Systems, Management and Security, 2018,93-98.

[102] Bayu Anggorojati, Parikshit Narendra Mahalle. Neeli Rashmi Prasad. Capability-based access control delegation model on the federated IoT network. Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications,2012.

[103] Aafaf Ouaddah, Hajar Mousannif, Anas Abou Elkalam, Abdellah Ait Ouahman. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 2017,237-262.

[104] Jia Jindou, Qiu Xiaofeng, Cheng Cheng. Access control method for web of things based on role and sns. Proceedings of IEEE 12th International Conference on Computer and Information Technology,2012.

[105] Guoping Zhang, Jiazheng Tian. An extended role based access control model for the Internet of Things, Proceedings of International Conference on Information, Networking and Automation (ICINA),2010,

[106] Ezedine Barka, Sujith Samuel MathewYacine Atif. Securing the Web of Things with Role-Based Access Control. Proceedings of International Conference on Codes, Cryptology, and Information Security,2015,14-26.

[107] Gusmeroli, S. Piccione, D. Rotondi. IoT Access Control Issues: A Capability Based Approach, Proceedings of Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012.

[108] Ronghua Xu, Yu Chen, Erik Blasch, etc. BlendCAC: A BLockchain-ENabled Decentralized Capability-based Access Control for IoTs, https://arxiv.org/pdf/1804.09267.pdf

[109] Luciano Barreto, Antonio Celesti, Massimo Villari, etc. An Authentication Model for IoT Clouds. Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2015, 1032-1035.

[110] Ronghua Xu, Yu Chen, Erik Blasch, etc. A Federated Capability-based Access Control Mechanism for internet of Things (IoTs). https://arxiv.org/pdf/1805.00825

[111] Xinwen Zhang, Francesco Parisi-Presicce, Ravi Sandhu. Formal model and policy specification of usage control. ACM Transactions on Information and System Security,2005,8(4), 351-387.

[112] Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori. Usage control in computer security: A survey. Computer Science Review 4, 2010,81-99.

[113] Xinwen Zhang, Masayuki Nakae, Michael J. Covington, etc. Toward a usage-based security framework for collaborative computing systems, ACM Transactions on Information and System Security,2008.11(1).

[114] Zhang Guoping, Gong Wentao. The research of access control based on UCON in the internet of things. Journal of Software, 2011,6(4),724-731.

[115] Vasileios Gkioulos, Athanasios Rizos, Christina Michailidou, etc. Enhancing Usage Control for Performance: A Proposal for Systems of Systems (Research Poster). Proceedings of International Conference on High Performance Computing & Simulation,2018

[116] Antonio La. MarraFabio, MartinelliPaolo Mori, etc. Introducing Usage Control in MQTT, Proceedings of SECPRE 2017, CyberICPS 2017: Computer Security,2017, 35-43.

[117] Khalifa Toumi, César Andrés, Ana Cavalli. Trust-orBAC: A Trust Access Control Model in Multi-Organization Environments. Proceedings of International Conference on Information Systems Security,2012,89-103.

[118] Nawal Ait Aali, Amine Baina, Loubna Echabbi. Tr-OrBAC: A trust model for collaborative systems within critical infrastructures. Proceeds of 5th World Congress on Information and Communication Technologies (WICT),2015.

[119] Imane Bouij-Pasquier, Anas Abou El Kalam, Abdellah Ait Ouahman, etc. A Security Framework for Internet of Things. Proceeds of International Conference on Cryptology and Network Security.2015,19-31.

[120] Khalida Guesmia, Narhimene Boustia. OrBAC from access control model to access usage model. Applied Intelligence, 2018, 48(8), 1996–2016.

[121] Mohamed Amine Ferrag, Leandros Maglaras, Abdelouahid Derhab. Authentication and Authorization for Mobile IoT Devices using Bio-features: Recent Advances and Future Trends. https://arxiv.org/abs/1901.09374

[122] Aafaf Ouaddah, Anas Abou Elkalam, Abdellah Ait Ouahman. FairAccess: a new Blockchain-based access control framework for the Internet of Things. 2016, https://doi.org/10.1002/sec.1748

[123] Oscar Novo. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal. 2018,5(2), 1184-1195.

[124] Savio Sciancalepore, Giuseppe Piro, Daniele Caldarola, etc. OAuth-IoT: an access control framework for the Internet of Things based on open standards. Proceeds of IEEE Symposium on Computers and Communications (ISCC),2017

[125] Federico Fernández, Alvaro Alonso, Lourdes Marco, etc. A Model to Enable Application-scoped Access Control as a Service for IoT Using OAuth 2.0. Proceeds of 20th Conference on Innovations in Clouds, Internet and Networks (ICIN),2017.

[126] Jalaluddin Khan, Jian ping Li, Ikram Ali, etc. An Authentication Technique Based on Oauth 2.0 Protocol for Internet of Things (IoT) Network. Proceeds of 15th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2018.