Type of the Paper (Review)

A Survey on Access Control in the Age of IoT

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

[1] Cyberspace Institute of Advanced Technology, Guangzhou University; qiujing@gzhu.edu.cn; johnsuhit@gmail.com; tianzhihong@gzhu.edu.cn
[2] School of Computer，North China University of Technology; duchunlai@ncut.edu.cn
[3] Beijing Computing Center; zuoqi@bcc.ac.cn
* Correspondence: Shen Su, johnsuhit@gmail.com; Qi Zuo, zuoqi@bcc.ac.cn

Abstract: With the development of IoT technology, various information resources, 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 IoT information Service model gradually change people's daily life. Facing the vast amounts of IoT information data, IoT search technology is used to quickly find accurate information to meet real-time search needs of users. However, IoT search requires to use a large number of user privacy Information, such as personal health information, location information, social relations information, to provide personalized services. User privacy information will meet security problems if an effective access control mechanism is missing during the IoT search process. Access control mechanism can effectively monitor the access activities of resources, and ensure authorized users to access information resources under legitimate conditions. This survey examines the growing literature on access control for IoT search. Problems and challenges of access control mechanism are analyzed to facilitate the adoption of access control solutions in real-life settings. This paper aims to provides theoretical, methodological and technical guidance for IoT search access control mechanism in large-scale dynamic heterogeneous environment. Based on the literature study, we also analyzed future development direction of access control in the age of IoT.

Keywords: IoT search; access control; attribute-based access control; survey

1. Introduction

IoT devices are collecting diverse data, such as electricity consumption, location information, and sensor data, from Internet, sensor networks, and online social networks. The development of IoT search realizes information sharing and improves the efficient use of devices. It can solve the problem of information island, improve the comprehensive utilization rate of social resources, and reduce the production and service costs. However, IoT search also collects, stores and analyses a large amount of private data, while providing convenience to users. Therefore, 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's also a serious threaten 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, can effectively monitor the access of resources and prevent the unauthorized flow of information. However, IoT search is a relatively new research field, traditional access control methods and techniques cannot fully solve the access control problems faced by IoT search because of node heterogeneity, open environment, multi-party sharing of resources.

In this survey, we present a thorough analysis of the current state-of-the-art technologies of access control for IoT search. We also provide an overview of the research challenges in access control. Such as, IoT search needs to integrate data from different data sources, so how to dynamic division

 doi:10.20944/preprints201811.0127.v1

of authorization for different data sources and integrate different access control policies are big challenges. The next section describes the background of access control for IoT search, which includes development history of access control and the Attribute-based access control (ABAC) model. Section 3 reviews the ABAC-based access control policy integration technologies. Section 4 reviews the ABAC-based access control policy authorization technologies. Section 5 reviews other ABAC-related technologies. Section 6 identifies open issues and draws a roadmap for future research. Finally, Section 7 concludes the article.

2. Background of Access Control for IoT Search

2.1. Access Control Background

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

By the 1970s, access control system is mainly used in mainframe system, such as BLP model [1] and Biba model [2]. BLP model is designed according to the military security policy, which aims to solve access control problem with confidential hierarchy information. It is the first mathematical model of access control model with strict theoretical proof. BLP model is widely used to describe the security of computer systems. Biba Model developed by Kenneth J. Biba in 1975. It is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Clark–Wilson model was described in 1987 by Clark and Wilson. This model is used to control and audit subject's state transition and run time adjustment of low-water-mark policy parameters. Compared with Biba, Clark–Wilson model provides a complete integrity protection by means of controlled state transaction, while Biba model provides a simple multi-level integrity access control scheme but it needs the introduction of trusted subject to ensure the usability.

By the 1980s, with the continuous improvement of requirements of the credibility of computer, researches proposed more flexible access control mechanisms. One of the representative works is the Trusted Computer System Evaluation Criteria (TCSEC) which is 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) [3] and Mandatory Access Control (MAC) [4] depend on different roles of access authority users. DAC model allows legitimate users to access objects as users or groups, while preventing unauthorized users from accessing objects, some users can also independently grant access rights to objects they own to other users. DAC model can meet the security needs of resource owners, however, because of the way of access depends on user authorization, the management of access authorities in DAC model is more decentralized. At the same time, DAC needs to manage the users, authorities and resources manually, which makes it not appropriate for IoT search due to the high complexity management works. 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 multi-level security model. Although MAC model solves the problem of decentralized resource management by centralizing authorization management, but for the users of IoT search, the management efficiency of MAC model is lower.

Around 2000, with the development of Internet and increasing large-scale applications of information system in enterprises, the traditional models of access control (i.e. DAC, MAC and its extension models) are difficult to handle complex application layer access requirements. To solve this problem, Role-Based Access Control (RBAC) [5] is prosed to restricting system access to authorized

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 November 2018 doi:10.20944/preprints201811.0127.v1

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 RBAC model. RBAC can be used to facilitate administration of security in large organizations, and meeting the information integrity requirements of information systems. RBAC is different from MAC and DAC, however it can enforce these policies without any complication.

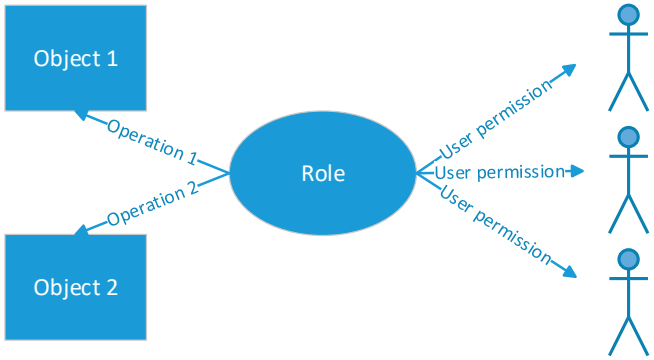

Figure 1. Role and user relationship of RBAC.

Fast development of new computing environments such as IOT search brings big challenges to the applications of access control technology. Traditional closed environment-oriented access control models (i.e. DAC, MAC, RBAC) are not adapt to the new computing environments. In this case, Attribute-Based Access Control (ABAC) [6] 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 [7]. 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 [5]. Such Different from the traditional access control models which 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.

Since attributes can describe entities in different views, it allows user to change access control strategies according to actual situations. Temporal-RBAC (TRBAC) [8] is an extension of RBAC model, which supports periodic role enabling, disabling, and temporal dependencies by using role triggers. Concept Usage Control (UCON) was developed in [9], 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 environment. ABAC is an ideal access control model in new computing environment, and has broad application prospects.

2.2. ABAC Background

ABAC makes access control decisions based on the attributes of access control entities. These attributes are often represented by a four tuple $< S, O, P, E >$.

S Attributes (Subject Attributes). Attributes of the subjects of the system. Such as name, age, home address, job title and so on.

O Attributes (Object Attributes). Attributes of the resources of the system. Such as documents, pictures, audio files and so on.

P Attributes (Permission Attributes). Various operations on object resources. Such as files or database read, write, create operations and so on.

E Attributes (Environment Attributes). Attributes derived from the current state of the system's environment. Such as session start time, system location and so on.

The ABAC system can be divided into two stages depending on the type of operation it performs: Access control policy Management and Access control policy execution. The access control

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 November 2018 doi:10.20944/preprints201811.0127.v1

Policy Management is primarily responsible for the collection of attributes, and describing and matching access control policies. The access control policy execution phase is primarily responsible for responding to access requests.

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, Policy is the set of all policies that govern access in the system.

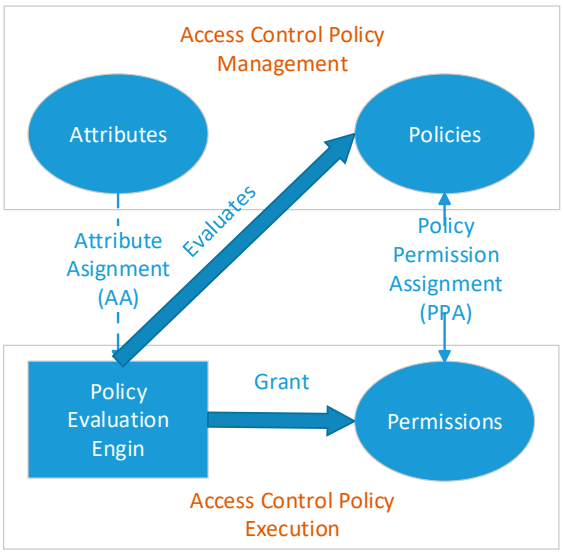

Figure 2. Core ABAC model. Attributes include both subject attributes and object attributes. Thin solid arrows denote many-to-many relations, thick solid lines denote relation with policy engine, and dotted lines denote information used by the policy engine to evaluate a certain policy.

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) [10] where objects are encrypted based on attribute-based access policies. ABE mainly consists of key-policy ABE (KP-ABE) [11] or ciphertext-policy ABE (CP-ABE) [12]. In KP-ABE, the access structure used to describe the access control policy is combined with the user's private key, and the attribute set is associated with the resource to be accessed. In this model, user freedom is relatively high and data owner freedom is lower. Because only attributes can be used to describe the data, the data owner cannot set the corresponding access control policies. CP-ABE is the reverse of KP-ABE, using an attribute-based policy to encrypt an object, and the access structure used to describe the access control policy is combined with 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 data owner, so that data owner freedom is higher.

3. Conflicts Resolution and IoT Application

3.1. Conflicts Resolution and Model Combination

In large scale network, different policies . Thus, the policy conflicts detection and resolution has an important role in the ABAC, and there is a lot of research on it.

In the paper of XACML Policy Evaluation Engines design research [13], the authors mentioned Kolovski et al.[14] formalize XACML policies with description logics (DLs), a decidable fragment of the first-order logic, and exploit existing DL verifiers for policy verification, detecting redundant XACML rules and removing redundant rules from XACML policies. Other scholars [15-19] proposed other conflicts detection and resolution methods to

Servos D etc. [20] summarized research and open problems in ABAC. As they mentioned, 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. Sun et al. [21] have

 doi:10.20944/preprints201811.0127.v1

proposed ARBAC (attribute- and role-based access control) that has an advantage of both ABAC and RBAC to fulfill the needs of highly distributed network environment. They also have done a conflict detection and policy optimization.

Servos and Osborn [21] attempted to create a formal general model of ABAC that provides a group based hierarchical representation of object and user attributes. In this model, entitled Hierarchical Group and Attribute-Based Access Control (HGABAC), attributes are assigned both directly to access control entities and indirectly.

3.2. IoT Application

Much efforts have been done in application of traditional methods of access control to IoT scenarios. N. Ye [22] introduced ABAC in web services into IoT networks to reduce the number of rules resulting from role explosion.

Both in [23] and [24], scholars discussed the research direction in IoT. In [24], Sicari S etc. summarized the security, privacy and trust in IoT, they discussed the limitation of RBAC and ABAC in IoT. As mentioned in [24], Gusmeroli S etc. [25] affirm that authorization frameworks like 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.

Because of the large-scale network in the IoT area, there must be model combination and novel strategy, such as blockchain. In addition, although the research on combined model of ABAC has achieved certain research results, the application to IoT scenarios are lacking. The independent and complete set of ABAC strategy application and content-based access control is the basis for building access control system in IoT area. How to design an excellent algorithm to get the best mixed strategy with low computational complexity is the key scientific problem to be solved in the future.

4. Access Control and Authorization

4.1. 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) [26]. Because not considering the dynamic changes of IdP's reputation, an attribute aggregation method based on multi-node cooperation [27] 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 [28], 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 [29]. This mechanism enables aggregating data concerning several attributes of each entity in a single operation ensuring data authenticity and privacy. Literature [30-31] 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

 doi:10.20944/preprints201811.0127.v1

anonymous attribute based on encryption technique [32]. Attribute discovery depends on data aggregation which is responsible for increasing the network lifetime and reducing the energy consumption [33]. Literature [34] 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 [34]. 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.

4.2. Association Generation of Attribute and Permission

A wide variety of users and devices bring a huge variety of attributes in the IoT environment. These attributes contain too many redundant attributes, which are not necessary to build the access control system, to manually filter. Therefore, it is necessary to study the automated association between user-attribute and attribute-privilege. Literature [35] discusses the security threats in IoT including Authentication, Confidentiality and Access Control. Besides ABAC (Attribute-Based Access Control) [36], RBAC (Role-Based Access Control) is also a policy mechanism which are based on the role of users in the system and the permissions given to them [37]. Although RBAC is one of the access control types [38], RBAC can be seen a single attribute special case of ABAC. RBAC is suitable for scenarios where there is an easy identification of permitted tasks for each user or service [37].

By drawing on the role engineering in RBAC, we can provide some ideas for the research of attribute association. Role engineering can be divided into top-down and bottom-up. The top-down method refers to the analysis of the security requirements and business processes by experts with the help of relevant knowledge, abstracting the role set, completing the role-permission assignment relationship, and ultimately achieving the goal of building a secure access control system. However, these methods mainly rely on experts to understand the real application scenarios, and the artificial dependence is strong. Using data mining techniques or matrix decomposition methods, the bottom-up method automatically filters and generates candidate role sets based on the existing user-privilege correspondence. Probabilistic approach is introduced into attribute extraction [39]. Literature [40] proposes a probabilistic model to reflect the correlation between role and privileges. With top-down and bottom-up methods, we can study the semantic relationship between the newly mined attributes, measure the similarity between the newly mined attributes and the attributes in the original access control system, and build the association between attribute and privilege.

For the generation and maintenance of ABAC rules, manually migrating to ABAC is more difficult than migrating to RBAC. The changes like mergers and acquisitions can make the rules inaccurate. If the change is too frequent, it is very difficult to manually specify or maintain an ABAC rule set. Therefore, automatically mining ABAC rules is an alternative. Literature [41] presents an ABAC policy mining algorithm which iterates over tuples in the given user-permission relation, uses selected tuples as seeds to construct candidate rules, and generalizes each candidate rule to cover additional tuples in the user-permission relation by replacing conjuncts in attribute expressions with constraints.

Since access logs reflect not only access control rules but also requesters' behaviors, so that mining the access logs helps to reconstruct the access rule for reducing the cost of migration to ABAC. Literature [42] analyzes that logs generally provide incomplete information about granted privilege and only a lower bound information. The algorithm does not take the order of log entries into account

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 November 2018 doi:10.20944/preprints201811.0127.v1

but summarize the log by the user-privilege relation induced by the log and the frequency function. Literature [43] use RBMs (Restricted Boltzmann Machines) to infer ABAC access rules from logs. RBMs are energy-based models capable to perform unsupervised learning so that they can work in the scenarios that there are only positive examples.

The access logs required by mining algorithm are not sparse. Otherwise these mining algorithms [41-43] as discussed above cannot mine useful ABAC policy. These sparse access logs maybe contain only a fraction of all possible requests. How to utilize sparse logs to mine useful ABAC policy become a requirement. Literature [44] proposes a mining algorithm Rhapsody which has been built on APRIORI-SD by replacing its last two stages with two new stages. On one hand, Rhapsody computes the reliability of each rule and removes those rules whose reliability value is below a given threshold. on the other hand, Rhapsody removes those rules that have equivalent shorter rules. In order to test the accuracy of mining algorithm, cross-validation is necessary which splits the log into a training and a testing log. Cross-validation on logs is shown in **Figure 1**. The Arabic numerals describe the processing stage. **Table 1** shows the comparison of mining algorithms mentioned above.

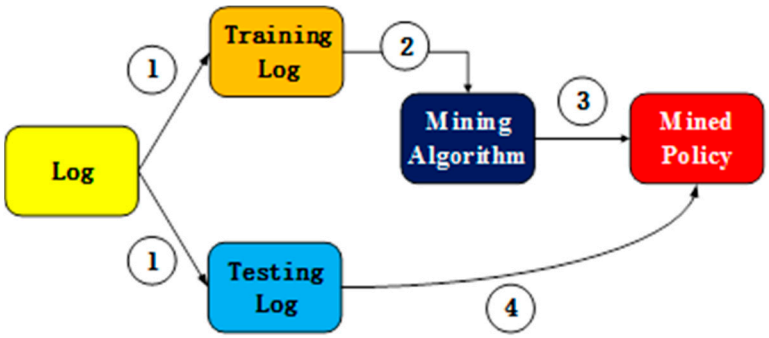

Figure 1. cross-validation

Table 1. State-of-the-art ABAC policy mining algorithms

Algorithm	Sparse logs	Shortest rules
Literature [16]	No	No
Literature [17]	No	No
Literature [18]	No	No
Literature [19]	YES	YES

There are two challenges. One is the limitations of existing approaches to policy mining is that the logs contain negative authorizations with varying levels of incompleteness. Another is noise in raw data which greatly affects the accuracy of results. How to deal with noise in raw data is a focus in the future.

4.3. Policy Matching

An efficient access control model or algorithm for the IoT requires to select an appropriate access policy language to implement corresponding access policies. The most well-known access control schemes used in IoT environments are XACML (Extensible Access Control Markup Language), OAuth (Open Authorization), and UMA (User-Managed Access). these protocols or frameworks will accelerate policy matching.

The XACML provide a standardized description of access control policies and is used in many IoT-related works such as [45]. XACML evaluation engine uses traversal matching so that Literature [46] uses the statistical analysis to reorder the policies and rules, put the frequently invoked policies and rules in front and cluster the policies, and clusters the policies and rules. Based on the XACML logic model, a decision graph of multiple types of data is proposed to manage the XACML strategy [47]. The mechanism of Hybrid access control enforces XML access control. HyXAC preprocese user

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 November 2018 doi:10.20944/preprints201811.0127.v1

queries by rewriting queries and removing parts of violating access control rules, and evaluates the re-written queries using subviews [48]. OAuth has been designed to provide an access control scheme to Web Services and applications. OAuth provides OAuth-based solutions for IoT. Literature [49] proposes a secure authentication policy, using OAuth 2.0 protocol. UMA which extends OAuth is a promising mechanism for access control. Literature [50] proposes a multi-level cache optimization mechanism that reduces the size of the strategy and digitizes the attribute values to improve the matching speed. Literature [51] selects XACML for the proposed AdRBAC (Adaptive Risk-Based Access Control) model. AdRBAC has four inputs which are user context, resource sensitivity, action severity and risk history. These four factors are used to estimate the security risk associated with each access request. The estimated risk value is then compared against the risk policies to make the final access decision.

Literature [52] proposes a Blockchain-based framework for access authorizations. Although the Blockchain was design for Bitcoin transactions, it uses the Blockchain to store access control rules, relationships, contexts and accountability information. Blockchain include Relationships Blockchain, Context Blockchain, Accountability Blockchain and Rules Blockchain as shown in Figure 2. The access information should be recorded on the Accountability Blockchain by the access control. It proposes a Decoder but lacking details that how to translate ABAC model and rules to the four Blockchain. **Although authors do not explain the technical details of Decoder for which there is not theoretical proof or experimental test [52], it is worth introducing Blockchain to the research of access control of IoT**.

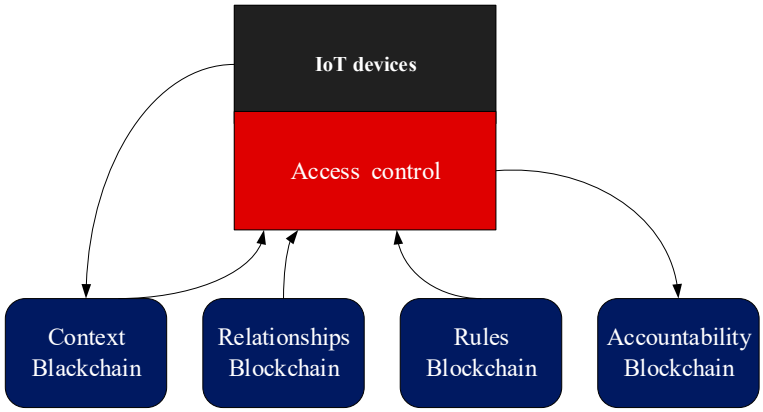

Figure 2. Framework overview

5. Other ABAC Models

Permissions in ABAC are closely related to attributes, and changes in user attributes can lead to corresponding changes in their access permissions. Access permission could be revoked on user level, user attribute level, and system attribute level. In either permission revoke level, new access control policies need to be generated when attributes are changed. The large-scale attributes and the many-to-many relationship between attributes and permissions in IoT search increase the complexity of permission updating.

Some researchers proposed to maintain attribute-permission list directly and manually. In [53], a simple direct revocation is described. In this method, labels of the revoked attributes are reversed to relate with permission policies to ensure these revoked attributes cannot be access by users. However, this way increases the description complexity of access control policies. To solve this problem, [54] proposed an attribute direct-revocable CP-ABE scheme with constant ciphertext length.

Although direct revocation can achieve fine-grained access control, it cannot achieve efficient fine-grained management between attributes and permissions. To overcome this limitation, researchers proposed indirect revocation. In [55], an identity-based encryption scheme was proposed to significantly improves key-update efficiency on the side of the trusted party, and ensure efficient

 doi:10.20944/preprints201811.0127.v1

for the users at the same time. This method updates the access control policy periodically, and revocation only occur when the period of user attributes is expired. Thus, indirectly increasing the workload of authorization engine. To overcome this drawback, [56] describes an efficient and revocable data access control scheme for multi-authority cloud storage systems. Multiple authorities co-exist in the system, and each authority can issue attributes independently. A revocable multi-authority CP-ABE scheme is also proposed in this article, which is applied as the underlying techniques to design the data access control scheme. Indirect approach does not require a full list of users, however, the exchange of key and data, and access control must be performed through a trusted third party. In article [57] He et al. limit attributes to user credentials that have been verified by a trusted third party. Both static and dynamic delegation in the context of the Role Graph Model are presented, and sessions are added to the RGM. Edge-labeling method is using in RBAC model to achieve session-oriented dynamic delegation.

In ABAC systems, user permissions are only associated with attributes, users may not be known until runtime due to this increased flexibility provided by attribute-based policies and the identity-less nature. At present, the research on auditing techniques of user identity in ABAC mainly focuses on Attribute-based Signature (ABS). Combined with the idea of digital signature, researchers proposed the ABS mechanism. The introduction of digital signature technology, such as ring signature [58] and group signature [59], guarantees the integrity of user attribute information. In article [60], an adaptive-predicate unforgeable and private attribute-based signature (ABS) scheme is described in the standard model. The ABS mechanism in multi-authority environment is designed and the corresponding security proof is given in the paper. In [61], the first decentralized multi-authority attribute-based signature (DMA-ABS) scheme is presented. No central authority and no trusted setup are required in this scheme. However, due to the limitation of access structure, the scheme is not suitable for large-scale environment. Although ABS mechanism protects the privacy of signers, malicious users may use ABS's anonymity to perform malicious operations. Traceable ABS mechanism is proposed to track user identity while ensure the privacy of signers. In [62], a traceable ABS mechanism (Decentralized TABS, DTABS) is proposed in distributed environment. Based on DTABS, paper [63] improve the state-of-art in three dimensions. The model proposed in the paper minimizes the trust placed in attribute authorities and provides a stronger definition for non-frameability. The model also captures the notion of tracing soundness.

6. Conclusions and Research Trends of Key Technologies

This article has introduced the background of access control and a taxonomy of current areas of ABAC for IoT search, provided a literature review of different ABAC models, and identified a number of open problems. Access control divided into Access control policy Management and Access control policy execution phases in this paper. For the first phase, Section 3 provides the review of ABAC oriented access control policy integration. For the second phase, the review of ABAC oriented access control and authorization in Section 4 describes the Attribute discovery mechanism, attribute-permission relation generation mechanism, and policy matching mechanism. Section 5 complements other key technologies in ABAC mechanism. The open problems examined in Section 6 serve as potential starting points for new research efforts.

The literature surveyed in this paper covered a number of different types of ABAC models. However, as the application environment becomes more and more diverse and complex, there is still challenge problems to be solved in ABAC research. One of the challenge problems to be solved is policy conflict resolution which is caused by features of IoT search. To ensure the security of IoT search and access control system, it is urgent to carry out related research. The other challenge problem is noise data identification and elimination for user-permission relations, since the noise data greatly affects the accuracy of the policy generation, and brings great security risks to access control systems.

Author Contributions: Introduction, Background of Access Control for IoT Search, Other ABAC Models, and Conclusions and Research Trends of Key Technologies, Jing Qiu and Zhihong Tian; Access Control and Authorization, Chunlai Du.

Funding: This research was funded in part by the National Natural Science Foundation of China (61871140, 61572153, U1636215, 61572492, 61672020), the National Key research and Development Plan (Grant No. 2018YFB0803504), and Open Fund of Beijing Key Laboratory of IOT Information Security Technology (J6V0011104).

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

References

1. Lapadula L. J., Bell D. E. *Secure Computer Systems: Mathematical Foundations*, MTR-2547, Volume 1, November 1973.
2. Biba, K.J. *Integrity Considerations for Secure Computer Systems*, NTIS AD-A039 324, MTR 3153,ESD-TR-76-372, MITRE Corporation, Bedford, MA, 1977.
3. 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.
4. 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.
5. 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.*
6. 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.*
7. Servos D., Osborn S. L. Current Research and Open Problems in Attribute-Based Access Control. *ACM Computing Survey, 2017, 49(4).*
8. 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.*
9. 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.
10. 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.
11. 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.
12. Bethencourt, J., Waters, B. Ciphertext-Policy Attribute-Based Encryption, Proceeding of IEEE Symposium on Security and Privacy, Piscataway, NJ, 2007: 321-334.
13. Liu A X, Chen F, Hwang J H, et al. Designing Fast and Scalable XACML Policy Evaluation Engines[J]. IEEE Transactions on Computers, 2011, 60(12):1802-1817.
14. V. Kolovski, J. Hendler, and B. Parsia, "Analyzing Web Access Control Policies," Proc. Int'l Conf. World Wide Web (WWW), pp. 677-686, 2007
15. Shu C C, Yang E Y, Arenas A E. Detecting Conflicts in ABAC Policies with Rule-Reduction and Binary-Search Techniques[C]// IEEE International Symposium on Policies for Distributed Systems and Networks. IEEE, 2009:182-185.
16. Liu J, Zhang H, Dai X, et al. A Static ABAC Policy Conflict Resolution Algorithm[C]// International Conference on Multimedia Information NETWORKING & Security. IEEE Computer Society, 2012:83-86.
17. Bonatti, Piero, Vimercati D C D, et al. An algebra for composing access control policies[J]. ACM Transactions on Information and System Security (TISSEC), 2002, 5(1):1-35.
18. Hu H, Ahn G J, Kulkarni K. Anomaly discovery and resolution in web access control policies[J]. IEEE Transactions on Dependable & Secure Computing, 2013, 10(6):341-354.
19. Rao P., Lin D., Bertino E., et al. An algebra for fine-grained integration of XACML policies[C]// ACM Symposium on Access Control MODELS and Technologies. ACM, 2009:63-72.
20. Servos D, Osborn S L. Current Research and Open Problems in Attribute-Based Access Control[J]. Acm Computing Surveys, 2017, 49(4).
21. Servos D, Osborn S L. HGABAC: Towards a Formal Model of Hierarchical Attribute-Based Access Control[C]// International Symposium on Foundations and Practice of Security. Springer, Cham, 2014:187-204.

22. N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and L. Qiao-min, "An efficient authentication and access control scheme for perception layer of internet of things," Applied Mathematics & Information Sciences, vol. 8, no. 4, p. 1617, 2014.
23. Ranjan A K, Somani G. Access Control and Authentication in the Internet of Things Environment[M]// Connectivity Frameworks for Smart Devices. Springer International Publishing, 2016.
24. Sicari S, Rizzardi A, Grieco L A, et al. Security, privacy and trust in Internet of Things[J]. Computer Networks, 2015, 76(C):146-164.
25. 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.
26. 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.
27. [2] Jaewon Lee, Heeyoul Kim, Joon Sung Hong. An Attribute Aggregation Architecture with Trust-based Evaluation for Access Control. Proceedings of IEEE Network Operations & Management Symposium. Piscataway, NJ:2008: 1011-1014, DOI: 10.1109/NOMS.2008.4575270
28. [3] Ghiselli Ricci, R. Mesiar, R. Multi-Attribute Aggregation Operators. Fuzzy Sets and Systems, 2011, 181(1): 1-13.
29. [4] 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.
30. [5] 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.
31. [6] 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.
32. [7] 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.
33. [8] 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.
34. [9] Li, Z., Zhang, W., Qiao, D., Peng, Y., Lifetime balanced data aggregation for the internet of things. Computers & Electrical Engineering. 2017.
35. [10] Sicari S, Rizzardi A, Grieco L, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer networks. 2015(76): 146–164.
36. [11] Hemdi, M.; Deters, R. Using REST based protocol to enable ABAC within IoT systems. In Proceedings of the 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference.2016:1-7
37. [12] Luis Cruz-Piris, Diego Rivera, Ivan Marsa-Maestre, Enrique de la Hoz and Juan R. Velasco. Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources. Sensors, 2018,18(3):1-21.
38. [13] Yunpeng Zhang and Xuqing Wu. Access Control in Internet of Things: A Survey. 2016, URL:https://arxiv.org/abs/1610.01065 (accessed on 30/10/2018).
39. [14] Lee T, Wang H. Attribute Extraction and Scoring: A Probabilistic Approach. Proceedings of IEEE 29th International Conference on Data Engineering. 2013:194-205.
40. [15] Frank M, Berkeley C. Role Mining with Probabilistic Models. ACM Transactions on Information and System Security, 2013, 15(4): 378-397.
41. [16] Zhongyuan Xu and Scott D. Stoller. Mining Attribute-based Access Control Policies. IEEE Transactions on Dependable and Secure Computing, 2015,12(5): 533-545.
42. [17] Zhongyuan Xu and Scott D. Stoller. Mining Attribute-Based Access Control Policies from Logs. Proceedings of the 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy XXVIII. 2014: 276-291.
43. [18] Decebal Constantin Mocanu, Fatih Turkmen, Antonio Liotta. Towards ABAC Policy Mining from Logs with Deep Learning. Proceedings of the 18th International Multiconference, Intelligent Systems, 2015.
44. [19] Carlos Cotrini, Thilo Weghorn, David Basin. Mining ABAC Rules from Sparse Logs. Proceedings of IEEE European Symposium on Security and Privacy (EuroS&P), 2018

45. [20] Seitz L, Selander G, Gehrmann C. Authorization framework for the internet-of-things. In Proceedings of the 2013 IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013: 1–6.
46. [21] Said Marouf, Mohamed Shehab, Anna Squicciarini, Smitha Sundareswaran, et al. Adaptive reordering and clustering-based framework for efficient XACML policy evaluation. IEEE Transactions on Services Computing, 2011,4(4): 300-313.
47. [22] Canh Ngo, Yuri Demchenko, Cees de Laat. Decision Diagrams for XACML Policy Evaluation and Management. Computers & Security, 2015,49(3):1-16.
48. [23] Manogna Thimma, Fang Liu, Jingqiang Lin, Bo Luo. HyXAC: Hybrid XML Access Control Integrating View-Based and Query-Rewriting Approaches. IEEE Transactions on Knowledge and Data Engineering, 2015,27(8): 2190-2202.
49. [24] Shamini Emerson, Young-Kyu Choi, Dong-Yeop Hwang, Kang-Seok Kim, Ki-Hyung Kim. An oauth based authentication mechanism for iot networks. Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), 2015: 1072–1074.
50. [25] HPEngine: high performance XACML policy evaluation engine based on statistical analysis. journal on Communications, 2014,35(8):206-215.
51. [26] Hany F Atlam, Madini O Alassafi, Ahmed Alenezi, Robert J Walters. XACML for Building Access Control Policies in Internet of Things. Proceedings of 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS), 2018.
52. [27] Otto Julio Ahlert Pinno, André Ricardo Abed Grégio, Luis C E De Bona. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. Proceedings of IEEE Global Communications Conference (GLOBECOM), Singapore, 2017.
53. Ostrovsky,R, Sahai,A.,Waters, B. Attribute-based encryption with non-monotonic access structures, Proceeding of the 14th ACM Conference on Computer and Communications Security, New York, 2007: 195-203.
54. Zhang Y. H., Zheng D.，Jin L., Hui L., University X. Attribute Directly-revocable Attribute-based Encryption with Constant Ciphertext Length. *Journal of Cryptologic Research, 2014, 1(5): 465-480.*
55. Boldyreva, A. Kumar, V. Identity-based encryption with efficient revocation, Proceeding of the 15th ACM Conference on Computer and Communications Security, New York, 2008: 417-426.
56. Yang, K., Jia, X. Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage. *IEEE Transactions on Parallel and Distributed Systems, 2014, 25(7): 1735-1744.*
57. Wang H., Osborn S. Static and Dynamic Delegation in the Role Graph Model. *IEEE Transactions on Knowledge & Data Engineering, 2011 , 23 (10) :1569-1582.*
58. Rivest R.L., Shamir A., Tauman. Y. How to Leak a Secret, Proceeding of the 7th International Conference on the Theory and Application of Cryptology and Information Security, Berlin, 2001: 552-565.
59. Science, C. Group Signatures, Proceeding of Workshop on the Theory and Application of Cryptographic Techniques, Berlin, 1991: 257-265.
60. Okamoto, T. Takashima, K. Efficient Attribute-Based Signatures for Non-monotone Predicates in the Standard Model, Proceeding of International Workshop on Public Key Cryptography, Beilin, 2011: 35-52.
61. Okamoto T., Takashima, K. Decentralized Attribute-Based Signatures, Proceeding of the 16th International Conference on Practice and Theory in Public-Key Cryptography, Berlin, 2013: 125-142.
62. Kaafarani, A. El, Ghadafi, E., Khader, D. Decentralized Traceable Attribute-Based Signatures, Proceeding of Cryptographers5 Track at the RSA Conference, Cham, 2014: 327-348.
63. Ghadafi, E. Stronger Security Notions for Decentralized Traceable Attribute Based Signatures and More Efficient Constructions, Proceeding of Cryptographers9 Track at the RSA Conference, Chan, 2015: 391-409.