Cluster Computing
https://doi.org/10.1007/s10586-018-1850-7

Survey of access control models and technologies for cloud computing

Fangbo Cai[1] · Nafei Zhu[1] · Jingsha He[1] · Pengyu Mu[1] · Wenxin Li[1] · Yi Yu[1]

Received: 10 November 2017 / Revised: 11 January 2018 / Accepted: 13 January 2018

Abstract
Access control is an important measure for the protection of information and system resources to prevent illegitimate users from getting access to protected objects and legitimate users from attempting to access the objects in ways that exceed what they are allowed. The restriction placed on access from a subject to an object is determined by the access policy. With the rapid development of cloud computing, cloud security has increasingly become a common concern and should be dealt with seriously. In this paper, we survey access control models and policies in different application scenarios, especially for cloud computing, by following the development of the internet as the main line and by examining different network environments and user requirements. Our focus in the survey is on the relationships among different models and technologies along with the application scenarios as well as the pros and cons of each model. Special attention will be placed on access control for cloud computing, which is reflected in the summaries of the access control models and methods. We also identify some emerging issues of access control and point out some future research directions for cloud computing.

Keywords Access control · Cloud security · Access control strategy · Access control model

1 Introduction

Access control is a core technology in information security. It allows legitimate users to gain access to information and system resources within legitimate time periods and prevent unauthorized users from accessing information and system resources by denying the access. Access control models and technologies have been in existence for about 50 years since the early 1970s during which period they have experienced a tremendous change from the scratch, from simple to complex and from theory to practice [1]. Access control was initially introduced to solve the problem of authorizing access to shared data on a mainframe. Discretionary access control (DAC) and mandatory access control (MAC) thus emerged [2]. DAC has the advantage of flexibility, but it is not well suited for large-scale networks with high security requirement due to its properties of decentralized resource management and complex authorization management. MAC can solved the problem caused by the decentralization of resource management, but it suffers from the problem of too strict authority management. For a system with a large number of users and many kinds of information and resources that are not clearly defined, MAC could incur excessive workload, low efficiency and lack of flexibility.

The development and popularization of computer and network technologies has made DAC and MAC access control models incapable of meeting the needs of practical applications. As the result, role based access control (RBAC) models emerged [3]. After the introduction of the initial model, a series of models, such as RBAC96 [3], ARBAC97 [4], ARBAC99 [5], ARBAC02 [6] and NIST RBAC [7], have been developed on the basis of the original RBAC model. RBAC can deal effectively with the problem of security caused by the flexibility of DAC and the limitation of MAC. In open network environments, information system requires a hierarchical structure in access control and in the management of users and information resources, resulting in task based access control (TBAC) model to be developed in which security models and mechanisms are constructed based on the notion of tasks. A dynamic and real-time security management scheme was proposed targeted for the time period of task processing [8]. Later, combination of RBAC and TBAC was attempted, resulting in the development of a task role based access control model [9] and that of a task and role-based delegation model [10].

Since 1990s, workflow technology has attracted the attention of researchers in the field of computer security. A

✉ Fangbo Cai
caifangbo@emails.bjut.edu.cn

[1] Faculty of Information Technology, Beijing University of Technology, Beijing, China

Published online: 01 February 2018

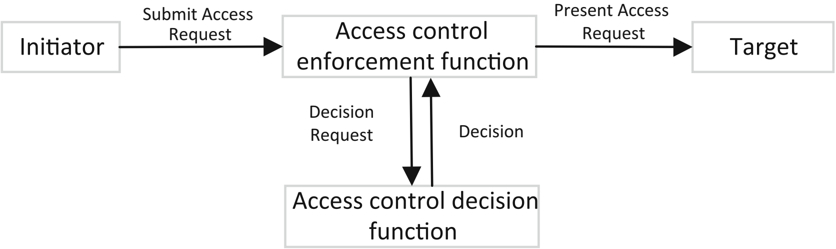


Fig. 1 The process of access control

workflow is a business process that is made up of multiple related tasks in order to accomplish a goal during which data is transferred among different users according to a set of rules defined [11]. When data flows in the workflow, the user who performs the operation is constantly changing along with the change of permissions. Traditional access control technologies can hardly meet the security requirements the dynamic authorization involved. Thus, methods for dynamically building access control matrix with workflow [12] and typical user hierarchy [13] were developed.

Cloud computing, Internet of things (IoT) and other new computing models can provide more convenient data sharing and efficient computing services, greatly improving the efficiency of information sharing as well as the utilization of computing and storage resources. However, should these new computing models fail to provide adequate data protection, information leakage will bring tremendous loss to the user. As the result, secure access to the Cloud has become an increasingly critical issue in a cloud computing environment. It is uncertain whether the data stored on the server is out of control or well protected or whether the computing task is properly executed. Therefore, it is necessary to design security mechanisms and architectures to protect the confidentiality, integrity and availability of cloud data [14,15].

This paper will first review the development of access control models and technologies. In Sect. 2, we describe the basic principle of access control. In Sect. 3, we introduce the distributed access control in cloud environment. In Sect. 4, we present access control based on security attributes in the cloud environment. In Sect. 5, we summarize the problems of cloud access control. Finally, in Sect. 6, we conclude this paper and also describe our future work.

2 General principle of access control

2.1 Basic elements of access control

The purpose of access control is to restrict access by an accessing subject to an accessed object and to make information resources accessible within the legal scope [16]. There are basically three components in the access control model: subject, object and access control policy. The subject is an active entity that makes the access request and, therefore, is the initiator of the access action. The object is a passive entity that receives access to other entities and, therefore, is the recipient of the access action. Access control policy is the set of access rules of the subject to the object. Figure 1 shows the main elements and the process of making authorization decisions through access control.

Table 1 Access control matrix

	Object_1	Object_2	,,,,,,	Object_n
Subject_1	Own, read, write	Write	,,,,,,	Own, read, write
Subject_2	Read	Read,	,,,,,,	Write
’’’’’’	’’’’’’	’’’’’’	’’’’’’	’’’’’’
Subject_n	Read, write	Read	,,,,,,	Own, read, write

The access matrix model uses a matrix to describe the access control policy of a system [17]. Lampson first abstracted the problem of access control and propose a formal representation that uses the subject, the object and an access control matrix [18]. In the model, the object is accessed by the subject and the system uses the notion of a reference monitor to control access based on the access matrix. An example is shown in Table 1.

2.2 Access control language

In the development and application of access control models and technologies, a variety of access control languages have been proposed to implement user access and permission management efficiently. Access control language is the bridge between the theory and the practice of access control [19]. Following are three common access control languages.

Security assertion markup language, called SAML [20], is developed based on the XML standard. It can be used to implement the exchange of authentication and authorization data between different security domains. The SMAL standard can define the work of authentication declaration, attribute declaration, and authorization for identity providers and service providers.

Service delivery markup language, called SPML [21], is also developed based on the XML standard. It is mainly used to create service requests for user accounts and service management related requests. The service provides markup language to make it easy to accurately configure security and audit requirements of the system and to implement the interoperation between different configuration systems.

Extensible access control markup language, called XACML [22], is a policy language based on XML that can provide effective access control for Web services. Protocol can be defined in a standardized format for representation of authorization rules and policies. It can also be used to define an assessment rule and strategy, which is the standard way of making authorization policies.

2.3 Access control strategy

Access control strategy is the main strategy of network security for the prevention and protection of objects with the goal of ensuring that network resources are not illegally used or accessed. There may be multiple access control policies in an access control system. When the subject, the object, and the authority of access control are subordinates to different access control strategies, it may lead to conflict of access control policies, which in turn leads to inconsistent system behavior and result in lower inefficiency and accuracy of the access control. There are definitely more security issues such as access control vulnerabilities.

2.4 Security analysis of access control strategy

Access control is an important part of the security analysis on cloud access control strategy. Security analysis of access control refers to the fact that this access strategy does not have risk and security threat during access authorization.

The way of performing analysis on cloud access control is primarily logic analysis based on state space reasoning [23]. Logic based specific analysis methods include theorem reasoning, mathematical model reasoning and quantitative analysis. In theorem reasoning [24], the axioms of the representative access control model is proved to be correct. However, it is not easy to find security axioms that can fully represent the model in practical applications. Mathematical model reasoning [25] uses mathematical models instead of access control policies to prove the security of access control. The drawback of this method is that it can only prove the part of the characteristics of security model. Quantitative analysis [26] relies on determining the level of security of the model by using quantifiable criteria in information entropy. Although this method is flexible and operable, it can only be evaluated from a certain aspect and can hardly be used to realize the security of an overall comprehensive assessment of a model. The state space reasoning method [27] refers to the security of the access control based on state space reasoning. At present, there is no unified strategy analysis method for security analysis of access control strategy. Rather, the analysis is usually performed based on different application scenarios for specific analysis. The common security strategy analysis method introduced in this paper is also applied to specific strategies with little extensibility. Analysis method based on state space reasoning, which has the advantages in terms of completeness and generality, is an important development direction of access control security analysis.

2.5 Consistency analysis of access control strategy

The research on policy conflict originates from the research on policy management framework, which means that two or more access strategies are inconsistent in one visit, resulting in conflicts in the execution of the access. Cross domain access behavior is very common in cloud environment. Building new interoperability could lead to the inconsistency between global security policy and local security policy, which brings potential security risks. The detection of conflict between access control strategies can be divided into static conflict detection and dynamic conflict detection. He et al. proposed a set of systematic conflicts subdivision standards based on the analysis of the causes of strategic conflict [28]. Yao et al. proposed a conflict detection mechanism based on the directed graph model [29], which solved the problem that formalization of conflict detection may be too complicated. In addition, there are detection methods that are based on priorities [30] and based on semantic conflict validation [31]. Such methods have some advantages in specific situations, but they suffer the disadvantages of high computational overhead. Therefore, research on access control policy conflict detection needs to seek balance between detection accuracy and computation efficiency according to different application scenarios.

2.6 Resolution of non-uniform access control strategy

In access control models, policy conflict resolution is often used in conjunction with conflict detection. According to the stage where the digestion process is located, policy conflict resolution can be performed before or during the execution of strategies. Li et al. proposed a method of setting priority for the policy inconsistency problem [32]. In this strategy conflict resolution method, the research uses the method of setting the strategy to execute the priority. Li et al. proposed the minimum cost method and dictionary editing method based on priority levels according to different objectives of the strategies [33]. Lu et al. [34] proposed an algorithm based on the priority maximization consistency subbase. Using a single method of conflict resolution may result in different results, which eventually leads to inconsistency of the results. It is usually necessary to develop appropriate strategy conflict resolution methods based on the characteristics of the application scenarios. At present, different access con-

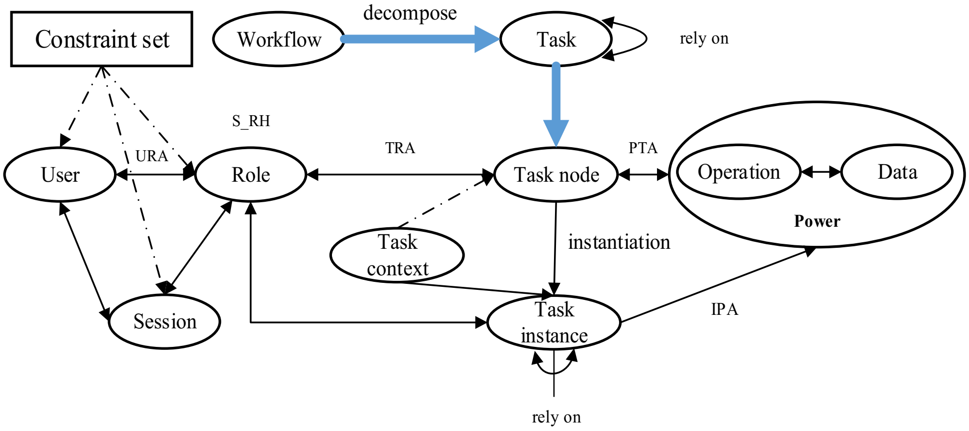


Fig. 2 T-RBAC model architecture

trol mechanisms adopted by major carriers are different. The research on conflict resolution of access control strategy is still in the stage of finding temporary remedy for problems. Therefore, further study is necessary on how to detect and resolve conflict of control strategies in the cloud computing environment.

3 Cloud computing access control models

With the development of open network and cloud technologies, traditional access control models present different advantages and disadvantages. Researchers have proposed many extended models in recent years on access control [35]. As a cloud computing model is mostly based on resource sharing, there is the need for excessive use of resources to take strong defensive measures. However, cloud computing has the characteristics of being a large-scale, distributed and virtual complex information system, traditional access control models and technologies face new challenges to support cloud applications [36].

3.1 Task based access control

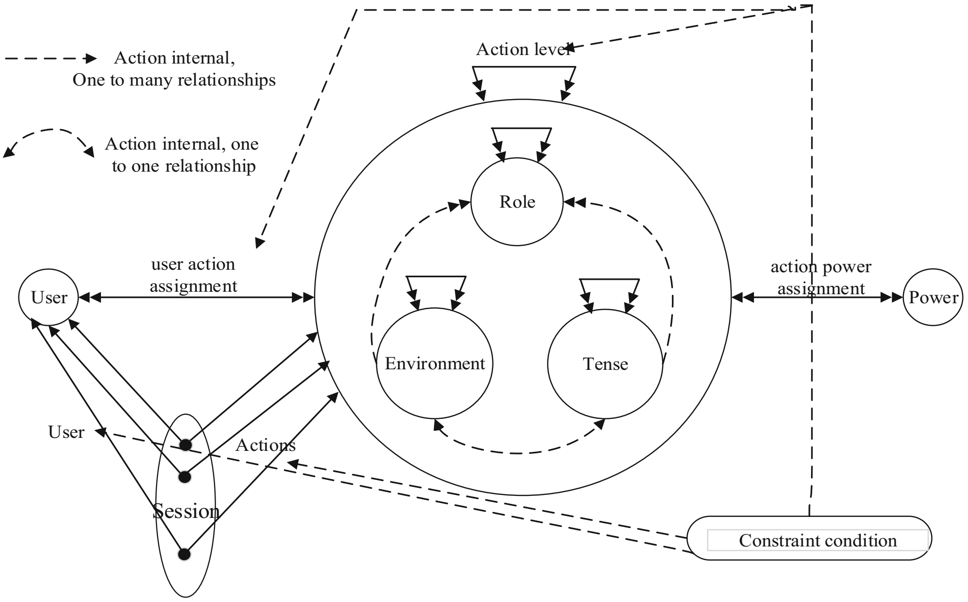
In 1997, Thomas et al. adopted the notion of task and proposed a task-based access control model [37]. The model can implement different access control strategies for different workflows. It can also implement different access control strategies in real time for different tasks of the same job. Botha et al. applied the RBAC model to extend workflow systems to effectively enhance the security in granting to the user access to workflow systems. However, the resulting model failed to solve such problems as separation of duties [38]. In view of this problem, the work in [39] proposed a T-RBAC model by combining task and RBAC [40,41]. The cloud server authorized by the owner of an object acts as a trusted intermediary to pass the access request during the authorization process. Introducing the concept of task into the RBAC architecture could refine the functions of the system into a single task as well as the role and the task. The authority and the task are linked to achieve dynamic management of access rights [42]. Then, the security of access control does not have to entirely depend on the credibility of the cloud server. At the same time, the cloud server would share part of the authorization work, lowering the burden on the user [43]. The T-RBAC model is shown in Fig. 2.

3.2 Action based access control

With the popularity of mobile Internet and mobile computers, communication network and systems have become more open and heterogeneous, supporting complex computing requirements, such as mobile computing and cloud computing [42]. In order to meet the growing demand for personalized services by the Internet, temporal and environmental information related to the concept of state is considered and introduced into access control models. Li et al. introduced the concept of action and proposed an action based access control model (ABAC) [44] as shown in Fig. 3 and further discussed the relationship between the roles, tenses and environment and provided the formal description of the action state management function [45].

Through the comprehensive consideration and analysis of the role, the tense and the environment, AcBAC can be applied flexibly to deal with access control problems in a variety of information systems. On this basis, in order to solve the decision-making problem of information system resource authorization, Li et al. proposed an information system access control mechanism based on the AcBAC model [46] and, at the same time, designed a security architecture for Web services based on AcBAC [47] that considers the location and temporal elements of user access to solve the confidentiality and integrity of the cloud computing environment. Lin et al. further extended the AcBAC model based on behavior characteristics of cloud computing environment and the combination of the Bell-LaPadula and Biba models. A cloud

Fig. 3 Action based access control



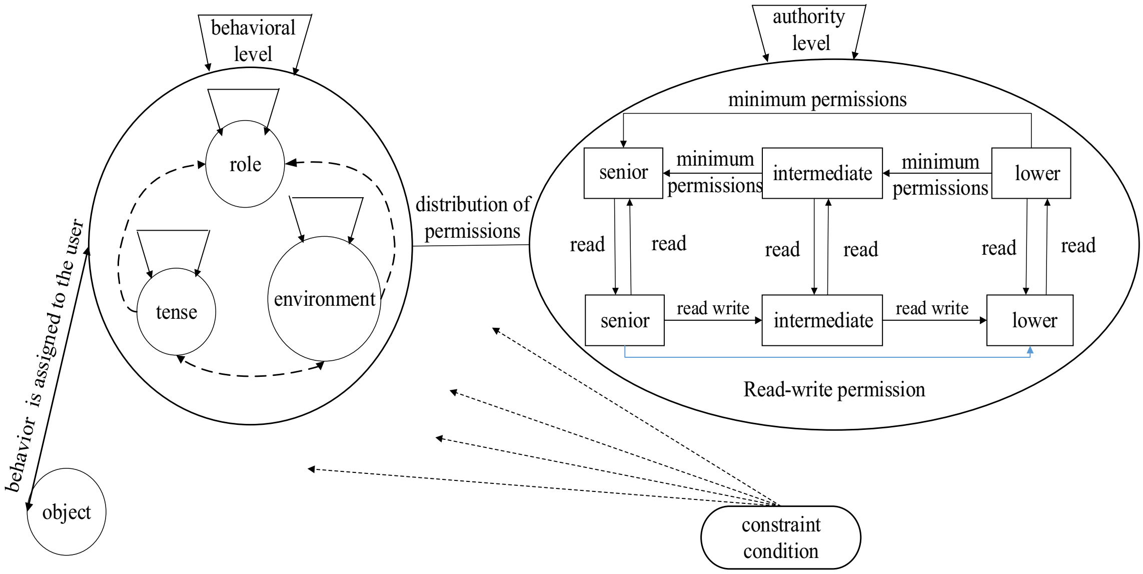


Fig. 4 Architecture of the CCACSM model

computing access control security model (CCACSM) was proposed [48] and the execution flow of the model is shown in Fig. 4.

3.3 Attribute based access control

The emergence of new computing models, such as mobile computing and cloud computing, has contributed to the progress of the Internet while bringing new challenge to access control models. Due to the network environment characteristics of heterogeneity and diversity, access control technology research began to develop in the direction of fine-grained, hierarchical authorization according to object oriented security related properties. Attribute based access control aims at addressing the problem of fine grained access control and large-scale user dynamic expansion in the current complex information systems.

The concept of entity attributes has been applied to access control strategies, models, and implementation mechanisms. Through the same way of modeling subjects, objects, permissions and environment attributes, one can describe authorization and access control constraints in a flexible and extensible manner. Yuan et al. proposed an attribute based access control model [49] to manage access to objects through description and operation of the principal attribute expression. The execution process of the model is shown in Fig. 5. In the ABAC model, all the subjects, objects, resources and access policies are described through using

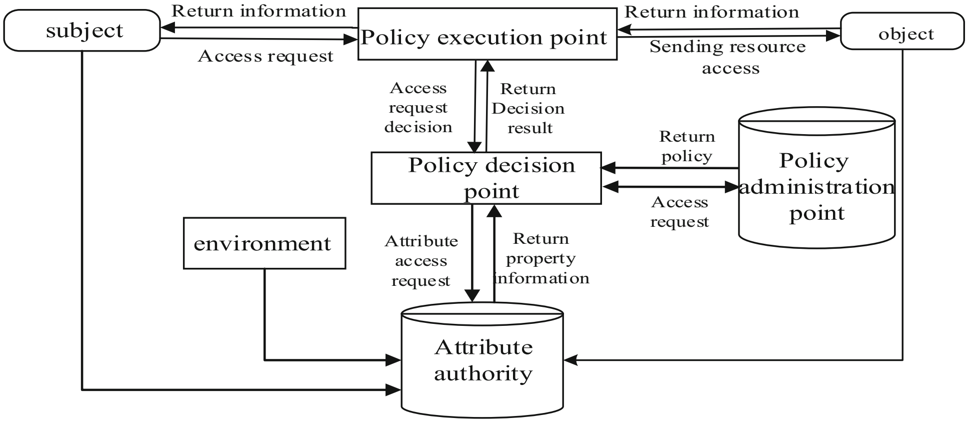


Fig. 5 The ABAC model

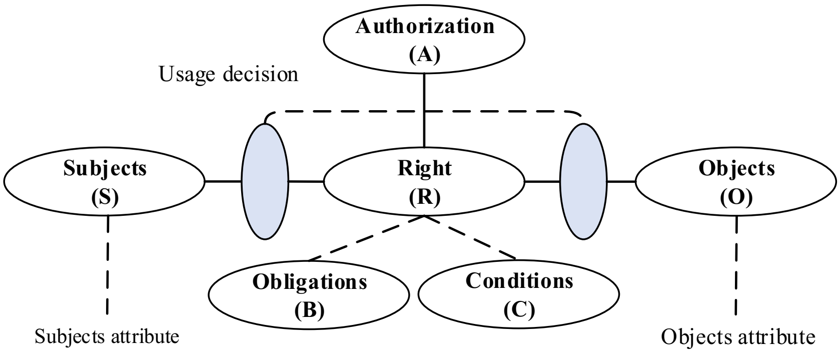


Fig. 6 The UCON model

attributes. Thus, when a user sends a request for access to an object resource, the attribute information about the user needs to be provided to the system. Since the attributes in ABAC access control may come from different organizational domains, semantic interoperation between different domains is another important issue to be dealt with. Combining ABAC with semantic Web technology, one can define more flexible access rules, realize semantic reasoning and effectively solve the problem of attribute semantic interoperability. The efficient access control decision of the ABAC model can guaranteed by the concept of semantic ontology. Combining the semantic Web technology, the description logical reasoning device (DL) can be used to classify the users and resources and to prove the consistency of the access control strategy [50]. Ei et al. summed up the cloud environment into three attributes [51] which include users of cloud resources, cloud resources and specific access environment.

3.4 Usage based access control

Usage based access control (UCON) has attracted the attention of experts in the field of information security and is said to represent the next generation of access control models. The UCON model mainly deals with new requirements for access control brought by the distributed environment. Besides the basic elements of the authorization process, ICON includes two additional elements: obligation and condition. Park et al. for the first time proposed to use the concept of control model [52] which is shown in Fig. 6. Chu et al. proposed a control implementation scheme in a distributed computing environment [53]. Although UCON has obvious advantages in distributed and cross-domain access control, the model has complex authorization management. Tavizi et al. constructed a new UCON model to solve the problems of attribute variability and obligation in the cloud computing environment [54]. Park et al. proposed an extended model called UCONABC by integrating authentication, responsibility and conditions into the UCON model [55]. While the most important feature of this model is to provide support for transaction variability and decision sustainability and to meet the requirements of data usage control in the current complex network environment, the efficiency of UCONABC model is low. Mashli et al. introduced a new entity evidence manager in the cloud environment to manage evidence between data providers and users and used the UCON models to model access control management in cloud computing and to manage the exchange of evidence between them through the model in the protection of cloud platform security policy [56]. UCON functions cover the traditional closely controlled environment and the dynamic open and uncontrollable environment [57,58]. UCON can not only solve the problems of traditional access control technologies [59,60], but also meet the needs of security and privacy issues in modern information systems.

4 Encryption based access control

Cryptography aims to protect data through encryption with a specified algorithm and key to protect the confidentiality of the data stored in a cloud server in the form of cipher text. Cryptography based access control can combine a cryptographic algorithm with policy based access control to achieve complementarity. Encryption based access control models can come with a variety of forms, such as attribute based encryption (ABE), timed release encryption (TRE), role based encryption (RBE) and identity based encryption (IBE).

4.1 Attribute based encryption

In attribute based encryption (ABE), users whose attribute set satisfies the corresponding access control policy can decrypt the cipher text with flexible implementation of one time encryption and multiple sharing. ABE also has good extensibility and flexible access strategy description capability. It also supports fine-grained access control with other superior features. Therefore, it is widely used in the environment of cloud computing. At present, the implementation mechanisms of ABE include basic ABE, key policy ABE (KP-ABE) and cipher text policy ABE (CP-ABE). Basic ABE only specifies the threshold policy, which can be used for simple application scenarios. The KP-ABE and CP-ABE mechanisms can support complex networks and have a broad application prospect in fine-grained data sharing and management control.

The ABE password system has four basic elements in the cloud computing environment: data provider, trusted third party authorization center, cloud storage server and user [62]. First, the trusted authorization center generates key and public parameters that pass the system public key to the data provider. After obtaining the system public key, the data provider encrypts a file with the policy tree and the system public key and uploads the cipher text and the policy tree to the cloud server. Then, when a new user joins the system, the user would upload its own set of properties to the trusted authorization center and submit a private key request. The trusted authorization center would calculate a public key for the user submitted property set and passes it to the user. Finally, the user downloads the data that is interested. If the attribute set satisfies the policy tree structure of cipher text data, it can successfully decrypt the cipher text. Otherwise, access to the data fails. The description of the model is shown in Fig. 7.

ABE consists generally of four steps as shown in Table 2:

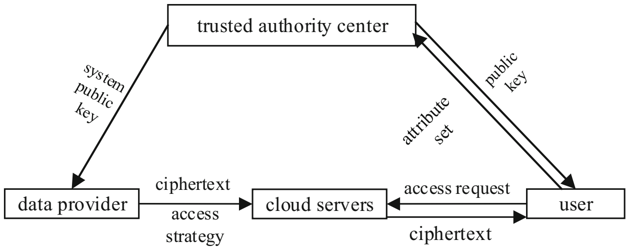


Fig. 7 The ABE model for cloud computing environment

Table 2 The steps of the ABE algorithm

Setup	Authorization center executes to generate the master key and the system public key
Encrypt	CT = Encrypt(PK, M, T), sender executes with attribute set T and plain text M, cipher text is CT
KeyGen	SK = KeyGen(MK, A), authorization center executes by to generate the user's private key SK
Decrypt	M = Decrypt(CT, SK), receiver executes using private key SK to get back message M

Sahai and Waters first proposed a scheme based on fuzzy identity cryptography [61] with the concept of attributes being introduced. Goyal et al. proposed an attribute based encryption scheme based on the fuzzy identity encryption scheme [62]. Then two ABE algorithms related to the strategy tree are derived, i.e., the key policy ABE and cipher text policy ABE. Sahai et al. introduced the concept of key strategy and described in the strategy a set of attributes associated with the cipher text so the decryption key is constrained by the policy tree [63]. When the access control strategy matches the attributes, the decryption key can be obtained. Therefore, the encryption party has no control over the cipher text and the key strategy is suitable for key management in large-scale network environments [64]. Sue et al. compared KP-ABE and CP-ABE and proposed attribute key revocation in the design of the CP-ABE access control mechanisms. Resistance to ABE collusion attacks along with other advantages lay a theoretical foundation for wide applications of ABE in cloud computing environments [65]. At the same time, some literature has also pointed out the applicable scenarios of KP-ABE and CP-ABE. Users in the KP-ABE mechanism could restrict the description of the receiving messages, which is used in the application of the query class, while senders in the CP-ABE mechanism could specify the strategy for the cipher text access, which is used in the application of access control.

Although it can ensure the security of data in the cloud computing environment, attribute based encryption affects the performance of access to the data. When the data is modified or the property is revoked, the whole data content needs to be re-encrypted. The cloud computing environment currently lacks a valid combination of the document model and the hierarchical security protection model. In response to the above problems, Xiong et al. combined the multilevel security and IBE algorithm and proposed a new composite document model and IBE-based composite document access control scheme [66]. Liu et al. proposed a multi-user data security sharing scheme based on dynamic group manager in a cloud environment [67] which uses group signature and broadcast encryption technology to allow users to share data anonymously with each other in the group.

The above discussion covered related mechanisms and techniques for access control through encryption technologies. The most prominent advantage of ABE is that it is well suited to situations where the descriptor is not fixed in a distributed environment. The encrypting party that encrypts a message does not need to know who decrypts it and only the decrypting party who conforms to the corresponding condition attribute can perform the decryption. Moreover, ABE has embedded the encryption rules in the encryption algorithm, which can avoid the cost of key distribution that frequently occurs in cipher based access control. However, the above work has not considered multi-factor access control in the data encryption scheme in encryption based access control. In the face of these problems, new access control models need to be designed to cope with a variety of security needs in complex network environments.

4.2 Other encryption-based access control

Timed release encryption (TRE) model allows data owners to encrypt data and send it to authorized users. Only when the predetermined future time is reached, can the authorized user obtain the correct key to decrypt the cipher text. Chen et al. introduced an efficient coding scheme with privacy protection capability and proposed a non-centralized TRE mechanism [68], which is applicable to application scenarios that require only a semi-reliable time server. Unruh et al, based on quantum cryptography, proposed a revocable, time-based encryption mechanism as well as an unknown recipient encryption mechanism [69]. This model would allow a message sender to send a message through a non-secure network and ensure that only one recipient can receive the message.

Role based encryption (RBE) model implements the data access control mechanism based on the layered RBAC model. Zhou et al. proposed a role-based encryption mechanism for cloud security storage [70] in which the owner of the data encrypts the data and stores it on the cloud server. Only the user who has specific role can decrypt the data to obtain the plaintext. Zhu et al. proposed a RBE mechanism that is based on partial order key hierarchy in public key cryptosystem and that supports revocation [71], which would allow senders to encrypt data using specified roles and only the users with higher roles can correctly decrypt cipher text. This mechanism supports dynamic user addition and deletion with the characteristics of a fixed length of the cipher text as well as the decryption key.

Identity based encryption (IBE) model is a public-key cryptography based algorithm. Shamir et al. proposed two mechanisms, i.e., identity based encryption and identity based signature [72]. Sahai et al. proposed the first fuzzy IBE scheme [73] that would tolerate certain errors between the user's encryption identity and the identity of the encrypted public key, which can support the implementation of biometrics as the public key. Unlike IBE, which uses a string of single identity information as a public key, fuzzy identity based encryption (FIBE) uses a string collection of multiple identity information as a public key and FIBE is considered to be a basic ABE solution.

5 Problems and challenges in cloud access control

Cloud computing is a rapidly developing new industry with bright prospects for further development and application. At the same time, challenges of security that it faces are unprecedented. It is, therefore, necessary for researchers in the field of IT and information security to develop more effective solutions. Meanwhile, security of cloud computing is not only a pure technical issue. It involves many other aspects, such as standardization, regulatory models, law and regulations, and so on.

5.1 Summary of the models

In practical applications, access control models should be selected according to different applications and environments. The ability, performance and security of access control models are summarized according to the metrics defined in document [74] to show the advantages and the disadvantages of the different access control models. Table 3

Table 3 Performance comparison among different types of access control models

	RBAC	TBAC	ABAC	UCON	ABE
Security					✓
Confidentiality					✓
Flexibility of authorization	✓			✓	
Minimum privilege	✓	✓			
Separation of duties	✓	✓			
Fine-grained control			✓	✓	✓
Cloud environment attributes		✓	✓	✓	
Constraints description	✓				
Compatibility			✓	✓	
Expansibility			✓	✓	

provides such a summary in which indicates good performance.

5.2 The problems of cloud data access

For cloud computing, access control is an important part of data security protection technology. Owing to the characteristics of data storage and access in the cloud environment, cloud data should be well managed. Thus, traditional information security technologies alone can hardly provide total guarantee of confidentiality, integrity and availability. Based on the analysis and description of the above application scenarios, cloud data access mainly has the following problems. First is the virtual server security problem, which states that when the physical host is damaged, the virtual server is likely to be attacked due to the communication between physical hosts. Another problem is the security for the data set since storage, processing and transmission of user data are all related to cloud computing, including how to store data effectively to avoid data loss or damage. Another problem is cloud platform usability in which attacks to user data and business applications in cloud platforms will affect service continuity, SLA and IT process, security strategy, event processing and analysis, etc. Cloud platforms could also suffer from the problem of attacks since cloud computing platforms can easily become the targets of hackers because of their high concentration of users and information resources. So, the consequence of data destruction and denial of service will have a much higher impact than traditional enterprise network application environments.

5.3 Research on key issues of access control for cloud computing

On account of the analysis of cloud application scenarios and data storage characteristics, current and future research on access control will face the complex and dynamic environment of cloud computing. In addition to ensuring that cloud resources and services are acquired and used by legitimate users, further study should be focused on the issues described in Sect. 5.2. The challenges facing the cloud data access control are mainly reflected in the aspects of standardization of cloud platforms and unified technical standards and industry specifications for cloud computing access control. At present, most cloud service providers still use traditional access control technologies and standards as the reference, which is not constructive to the implementation and supervision by standardization organizations. For fine grained access control, most existing cloud access control is based on user identity and some models even do not follow the minimum privilege principle of access control, thus bring security risks to multi-tenant environment in the cloud. For access control in cloud computing, cloud users, cloud resources and network environment are constantly changing, making traditional, static and centralized access control incapable of satisfying the dynamic security needs. Another issue is cross-domain authorization among cloud platforms since multiple security domains are the main characteristics of cloud access where cloud applications may belong to different domains and there is thus the requirement for cross-domain access control. There is also the need to study the interoperability of cross-domain authorization including the strategy for detection and resolution of policy conflict. Since virtual technology is a key technology of cloud computing, service providers must provide corresponding functions to ensure the security to the customers. Lastly, trusted cloud computing should be developed into cloud computing models. Research could be conducted on ways of implementing data through the means of non-object classes as a way of providing reliable cloud services.

Cloud computing security is not just a technical problem, it also involves standardization, supervision mode, laws and regulations and other aspects. Therefore, exploring solutions of cloud computing security only from a technical point of view is not enough, effort is really needed from academia, industry and different levels of government.

6 Conclusion

Access control is an important information security technology and has become indispensable for enterprises to protect data and resources in information systems. After many years of development, research on access control models has achieved noticeable progress. Cloud computing is a new paradigm, making access control critical in providing effective protection to cloud computing resources. This makes access control in cloud computing one of the most important issues in present research on cloud security. Therefore, a great deal of attention has been attracted from academia and industry. However, its characteristics of virtualization, distribution and multi-tenancy have brought many challenges to the development of access control technologies. In addition, access control in cloud computing is not just a technical problem, it also involves a lot of aspects such as standardization, laws and regulations, codes of conduct, etc. At present, research of cloud computing access control technologies is still in its early stage. Future studies should therefore emphasize more on the design of cloud access control models as well as on policy analysis and consistency analysis of access control in addition to other key technologies.

This paper investigated common access control mechanisms and reviewed some traditional access control models and technologies as well as the framework of access control for cloud computing. This paper also discussed research progress of access control in recent years and pointed out some key issues for future research on cloud access control. We hope that the discussion on challenges and issues of cloud computing access control would bring benefit to the future research.

Acknowledgements The work in this paper has been supported by National Natural Science Foundation of China (61602456) and National High Technology Research and Development Program of China (863 Program) (2015AA017204).

References

1. Li, F.H., Xiong, J.B.: Access control technology for complex network environment. The people's mail and telecommunications press (2015)
2. Bell, D.E., LaPadula, L.J.: Secure computer system: unified exposition and multics interpretation. DTIC Document, Mitre Corp Bedford MA, USA (1976)
3. Sandhu, R., Coyne, E.J., Feinstein, H.L., et al.: Role-based access control models. Computer **29**(2), 38–47 (1996)
4. Sandhu, R., Bhamidipati, V., Munawer, Q.: The ARBAC97 mode for role-based administration of roles. ACM Trans. Inf. Syst. Secur. (TISSEC) **2**(1), 105–135 (1999)
5. Sandhu, R., Munawer, Q.: The ARBAC99 model for administration of roles. In: Proceedings of 15th Annual Computer Security Applications Conference, pp. 229–238. IEEE, New York, NY, USA (1999)
6. Oh, S., Sandhu, R., Zhang, X.: An effective role administration model using organization structure. ACM Trans. Inf. Syst. Secur. (TISSEC) **9**(2), 113–137 (2006)
7. Ferraiolo, D.F., Sandhu, R., Gavrila, S., et al.: Proposed NIST standard for role-based access control. ACM Trans. Inf. Syst. Secur. (TISSEC) **4**(3), 224–274 (2001)
8. Thomas, R.K., Sandhu, R.: Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. In: Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Security XI: Status and Prospects, pp. 166–181. Chapman & Hall, Ltd., London, UK (1998)
9. Oh, S., Park, S.: Task-role-based access control model. Inf. Syst. **28**(6), 533–562 (2003)
10. Zhu, J.: Research on Group Perception and Access Control Technology in Role Coordination. College of computer science, Zhongshan University, Guangzhou (2009)
11. Bertino, E., Ferrari, E., Atluri, V.: The specification and enforcement of authorization constraints in workflow management systems. ACM Trans. Inf. Syst. Secur. **2**(1), 65–104 (1999)
12. Knorr, K.: Dynamic access control through Petri net workflows. In: 16th Annual Conference on Computer Security Applications, pp. 159–167 (2000)
13. Botha, R.A., Eloff, J.H.P.: Designing role hierarchies for access control in workflow systems. In: Proceedings of the 25th International Computer Software and Applications Conference, pp. 117–122. IEEE Computer Society, Washington, DC, USA (2001)
14. Curry, S., Darbyshire, J., Fisher, D.W., Hartman, B., Herrod, S., Kumar, V., Martins, F. et al.: Infrastructure security: getting to the bottom of compliance in the cloud. The Security Division of EMC (2010)
15. Kaur, P.J., Kaushal, S.: Security concerns in cloud computing. In: Proceedings of the HPAGC 2011. CCIS, vol. 169, pp. 103–112(2011)
16. Shen, H.B., Hong, F.: Review of access control model. Appl. Res. Comput. **22**(6), 9–11 (2005)
17. Han, D.J., Gao, J., Zhai, H.L., et al.: Research progress of access control model. Comput. Sci. **37**(11), 29–33 (2010)
18. Lampson, B.W.: A scheduling philosophy for multiprocessing systems. Commun. ACM **11**(5), 347–360 (1968)
19. Luo, Y., Wu, Z.H.: A new method of access control policy descriptive language and its authorization. J. Comput. 1-18 (2017)
20. Cantor, S., Moreh, J., Philpott, R., Maler, E.: Metadata for the OASIS security assertion markup language (SAML) V2.0. OASIS Open, (2005)
21. Gary, C., Sun, M.: OASIS service provisioning markup language (SPML) versions 2.0. OASIS Open (2006)
22. Erik, R., Axiomatics, B.: OASIS extensible access control markup language (XACML) versions 3.0. OASIS Open (2013)
23. Lv, S., Liu, L., Shi, L., et al.: Intelligent planning method based on automatic reasoning technology. J. Softw. **20**(5), 1226–1240 (2009)
24. Li, N., Tripunitaram, V.: Security analysis in role based access control. ACM Trans. Inf. Syst. Secur. **9**(4), 391–420 (2006)
25. Lin, B.G.: Analysis of extended information system security domain model. J. Commun. 9–14 (2009)
26. Ye, Y., Lu, T., et al.: Triple helix model and its quantitative analysis methods. China Soft Sci. **11**, 131–139 (2014)
27. Liu, Q.: Role-based access control techniques, South China University of technology press, pp. 55–60 (2010)
28. He, Z., Tian, J., Zhang, Y.: Style refinement and detection improvement of policy conflict. J. Jilin Univ. **25**(3), 287–293 (2005). (in Chinese)
29. Yao, J., Mao, B., Xie, L.: A DAG-based security policy conflicts detection method. J. Comput. Res. Dev. **42**(7), 1108–1114 (2005). (in Chinese)
30. Lupu, E.C., Sloman, M.: Conflicts in policy based distributed systems management. IEEE Trans. Softw. Eng. **25**(6), 852–869 (1999)
31. Cholvy, L., Cuppens, F.: Analyzing consistency of security policies. IEEE Symposium on Security & Privacy, IEEE, pp. 103–112 (1997)
32. Li, X., Meng, L., Jiao, L.: Problems in results of policy conflict resolutions and detection and resolution methods in network management systems. J. Comput. Res. Dev. **43**(7), 1297–1303 (2006). (in Chinese)
33. Li, R.X., Lu, J.F., Li, T.Y., et al.: A method of inconsistency conflict resolution for access control strategy. J. Comput. **36**(06), 1210–1223 (2013)
34. Lu, J.F., Yan, X., Peng, H., Han, J.M.: An optimized strategy for inconsistent conflict resolution. J. Huazhong Univ.Sci.Technol. **42**(11), 106–111 (2014)
35. Feng, D.G., Zhang, M., Zhang, Y.: The security research of cloud computing. J. Softw. **22**(1), 71–83 (2011)
36. Bertino, E., Ferrari, E., Atluri, V.: The specification and enforcement of authorization constraints in workflow management systems. ACM Trans. Inf. Syst. Secur. **2**(1), 65–104 (1999)
37. Thomas, R.K., Sandhu, R.: Task-based authorization controls (TBAC): a family of models for active and enterprise oriented authorization management. In: Proceedings of the 11th IFIP WG11.3 Conference on Database Security, pp. 166–181. Lake Tahoe (1997)
38. Li, F.H., Su, M., Shi, G.Z., Ma, J.F.: Research status and development trends of access control model. Chin. J. Electron. **40**(4), 805–813 (2012). (in Chinese with English abstract)
39. Botha, R.A., Eloff, J.H.P.: Designing role hierarchies for access control in workflow system. The 25th Annual International Computer Software and Applications Conference Chicago, pp. 117–122 (2001)
40. Wang, X.W., Zhao, Y.M.: A task-role-based access control model for cloud computing. Comput. Eng. **38**(24), 9–13 (2012)
41. Deng, J.B., Hong, F.: Task-based access control model. J. Softw. **14**(1), 76–96 (2003)

42. Park, S.: Task role based access control: an improved access control model for enterprise environment. The 11th International Conference in Database and Expert Systems Applications. pp. 264–273. London (2000)
43. Androulaki, E., Soriente, C., Malisa, L. et al.: Enforcing location and time based access control on cloud stored data. The 34th International Conference on Distributed Computing systems. pp. 637–648 (2014)
44. Li, F.H., Wang, W., Ma, J.F., et al.: Action based access control model. Chin. J. Electron. **17**(3), 396–401 (2008)
45. Li, F.H., Wang, W., Ma, J.F., et al.: Action based access control model and its behavior management. J. Electron. **36**(10), 1881–1890 (2008)
46. Li, F.H., Wang, W., Ma, J.F., et al.: The access control model of cooperative information system and its application. J. Commun. **29**(9), 116–123 (2008)
47. Li, F.H., Wang, W., Ma, J.F., et al.: Action based access control for web services. The 5th International Conference on Information Assurance and Security, pp. 637-642. Xi'an, (2009)
48. Lin, G.Y., He, S., Huang, H., Wu, J.Y., Chen, W.: Access control security model based on behavior in cloud computing environment. J. Commun. **33**(3), 59–66 (2012)
49. Yuan, E., Tong, J., Zhao, Z.: Attributed based access control (ABAC) for web services. The IEEE International Conference on Web Services, Orlando, Florida. pp. 561–569 (2005)
50. Wang, X.M., Fu, H., Zhang, C.L.: Research progress on properties based access control. J. Electron. **38**(07), 1660–1667 (2010)
51. Ei, E.M., Thinn, T.N.: The privacy-aware access control system using attribute-and role-based access control in private cloud. Proceedings of the 2011 4th IEEE IC-BNMT. pp. 447–451 (2011)
52. Parkark, J., Sandhu, R.: Towards usage control models: Beyond traditional access control. Proceedings of the 7th ACM Symposium on Access Control Models and Technologies, pp. 57–64. ACM press, Monterey California (2002)
53. Chu, X.B., Qin, Y.: A distributed control system based on trusted computing. J. Comput. **33**(1), 93–102 (2010)
54. Tavizi, T., Shajari, M., Dodangeh, P.: A usage control based architecture for cloud environments. Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International. pp. 1534–1539, IEEE (2012)
55. Park, J., Sandhu, R.: The UCON ABC usage control model. ACM Trans. Inf. Syst. Secur. **7**(1), 128–174 (2004)
56. Mounira, M., Rached, A., Ahmed, S.: Access control in probative value cloud. In: Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (2013)
57. Park, J., Zhang, X.W., Sandhu, R.: Attribute mutability in usage control. In: Proceedings of the Annual IFIP WG Working Conference on Data and Applications Security, pp. 15-29 (2004)
58. Zhang, X.W., Nakae, M., Covington, M.J., et al.: Toward a usage-based security framework for collaborative computing systems. ACM Trans. Inf. Syst. Secur. **11**(1), 1–36 (2008)
59. Park, J.: Usage Control: A Unified Framework for Next Generation Access Control. George Mason University, Virginia (2003)
60. Zhang, X.W., Parisi-Presicce, F., Sandhu, R., et al.: Formal model and policy specification of usage control. ACM Trans. Inf. Syst. Secur. **8**(4), 35–87 (2005)
61. Dong, Q.X., Guan, Z., Chen, Z.: An overview of computational cryptography on cryptographic data. Appl. Res. Comput. **33**(09), 2561–2572 (2016)
62. Vipul, G., Amit, S., Omkant, P., Brent, W.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the ACM Conference on Computer and Communications Security. pp. 89-98 (2006)
63. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-Based encryption with non-monotonic access structures. In: Proceedings of the 14th ACM Conference on Computer and Communications Security. pp. 1–17. ACM Press, New York (2007)
64. Attrapadung, N., Imai, H.: Conjunctive broadcast and attribute-based encryption. In: Shacham, H., Waters, B. (eds.) Pairing-Based Cryptography-Pairing 2009, pp. 248–265. Springer-Verlag, Berlin (2009)
65. Shu, J.S., Cao, D., Wang, X.F.: Attribute based encryption mechanism. J. Softw. **22**(6), 1299–1315 (2011)
66. Xiong, J.B., Yao, Z.Q., Ma, J.F., et al.: A portfolio document model and access control scheme in a cloud computing environment. J. Xi'an Jiao Tong Univ. **48**(2), 25–31 (2014)
67. Liu, X., Zhang, Y., Wang, B.: Mona: secure multi-owner data sharing for dynamic groups in the cloud. IEEE Trans. Parallel Distrib. Syst. **24**(6), 1182–1192 (2013)
68. Chen, S.H., Chen, R.J.: Dealer less multi server timed release encryption scheme with privacy preserving encoding. The Second International Conference on Information Security and Digital Forensics, p. 1 (2005)
69. Unruh, D.: Revocable quantum timed release encryption. The 33th Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 129–146. Springer Verlag, Copenhagen, Heidelberg (2014)
70. Zhou, L., Varadharajan, V., Hitchens, M.: Enforcing role based access control for secure data storage in the cloud. Comput. J. **54**(10), 1675–1687 (2011)
71. Zhu, Y., Hu, H.X., et al.: Provably secure role based encryption with revocation mechanism. J. Comput. Sci. Technol. **26**(4), 697–710 (2011)
72. Shamir, A.: Identity Based Crypto Systems and Signature Schemes. CRYPTO 84 on Advances in Cryptology. Springer Verlag, New York (1985)
73. Sahai, A., Waters, B.: Fuzzy identity based encryption. The 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, pp. 457–473. Springer Verlag, Berlin Heidelberg (2005)
74. Wang, Y.D., Yang, J.H., Xu, C., et al.: Survey on access control technologies for cloud computing. J. Softw. **26**(5), 1129–1150 (2015)

Fangbo Cai is currently a Ph.D. candidate in the Faculty of Information Technology at Beijing University of Technology (BJUT), Beijing, China. She received her Master's degree from the same university in 2016. Ms. Cai's research interests include network security and distributed network technology.

Nafei Zhu received her B.S. and M.S. degrees from Central South University, China in 2003 and 2006, respectively, and her Ph.D. degree in computer science and technology from Beijing University of Technology in Beijing, China in 2012. From 2015 to 2017, she was a Postdoc and an Assistant Researcher in the Trusted Computing and Information Assurance Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences in China. She is now on the Faculty of Information Technology in Beijing University of Technology. Dr. Zhu has published over 20 research papers in scholarly journals and international conferences (16 of which have been indexed by SCI/EI/ISTP). Her research interests include information security and privacy, wireless communications and network measurement.

Jingsha He is currently a Professor in the Faculty of Information Technology at Beijing University of Technology (BJUT), Beijing, China. He received his Ph.D. degree from the University of Maryland at College Park in 1990. Prior to joining BJUT in 2003, he worked for IBM, MCI Communications and Fujitsu Laboratories engaging in R&D of advanced networking technologies and computer security. Prof. He's research interests include methods and techniques that can improve the security and performance of the Internet. He has published nearly 260 papers in the above areas.

Pengyu Mu is a currently M.S. candidate in the Faculty of Information Technology at Beijing University of Technology (BJUT), Beijing, China. He received his B.S. degree from Tianjin Polytechnic University in 2015. His research interests include network security, access control and social networking.

Wenxin Li is a Postgraduate in the School of Software Engineering at Beijing University of Technology, Beijing, China. She received her Bachelor's degree in Xi'an Shiyou University. She's interests in research direction mainly for network security, including access control, information protection and distributed network technology.

Yi Yu is a currently M.S. candidate in the Faculty of Information Technology at Beijing University of Technology (BJUT), Beijing, China. She received her B.S. degree from Hubei Polytechnic University in 2016. Her research interests include network security, access control and identity authentication.