A Classified Access Control Model Research for Cloud Computing

Wenyi Shen, Linbo Tao, Bo Liu and Yishen Wang

1 Introduction

Cloud computing forms a huge pool of IT resources by linking a large number of IT resources, which facilitates its use and access to IT resources, together with lower cost to users. It stores user data in the cloud instead of storing them in the local by their owners. So Users do not know where their data is stored, in which server, all these are managed and maintained by the third parties. This framework can properly solve the problems of disaster recovery, sharing and scalability [1], but bring the risk of illegal access and privacy diffusion. There are three reasons, the first, the data of user may be stored together with other users' data in a same physical host with different virtual machine instances which faces the side channel attack, we need to know how to ensure them safely isolated. The second, users store their data in the cloud, facing illegal access by other users or unauthorized internal cloud service providers [2], we need to know how to identify the access identity and permission control. The third, when illegal access to data occured, how to restrict the scope of unauthorized access. All these problems present great challenges to access control.

Based on comparing the advantages and disadvantages of traditional access control and the analysis of cloud computing environment, an access control model based on object sensitivity classification and model T-RBAC is proposed, efficiency

W. Shen (✉)
Department of Computer Science and Technology,
Suzhou College of Information Technology, Suzhou 215000, China
e-mail: shenwenyi0806@163.com

L. Tao · Y. Wang
School of Arts and Sciences, Information Engineering University,
Zhengzhou 450001, China

B. Liu
NanChang High School, Shenyang 110000, China

Z. Deng (ed.), *Proceedings of 2017 Chinese Intelligent Automation Conference*,
Lecture Notes in Electrical Engineering 458,
https://doi.org/10.1007/978-981-10-6445-6_36

and dynamic property are fully considered in this model. It improves the data control ability to users, reduces the scope of illegal access, improves the authorization efficiency of access control.

2 Characteristics Analysis of Access Control

The access control system consists of three main elements: subject, object and control strategy. The subject refers to the access request initiator [3], it could be a user, application or process. The object refers to program called by subject or accessed data. The control strategy refers to a set of rules that subject how to access object. Subject and object are relative, they can be transformed into each other under certain conditions. The nature of access control is to limit the access of users to the resources based on the access control policy, only those authorized subjects allowed to access corresponding resources. Access control intend to prevent objects from invading and destroying.

The traditional access control models have DAC(Discretionary Access Control), MAC(Mandatory Access Control) and RBAC (Role-based Access Control). DAC technology is a kind of common access control technology in multiple users environment, users have absolute control of their data, they may grant other users or groups to access their data, or revoke their permissions, the authorities of each authorized subject controlled by an ACL (Access Control, List) [4]. This kind of access control model fits the small scale systems, but for large distributed systems, it is difficult to maintain the large ACL, flexible task allocation and limiting the malicious operation to authorized users. The MAC model is mainly used in military, government and other high safety requirements areas, it adds the classification to resources security attributes in the network on the basis of DAC, it sets the different subjects access permissions to different attributes. The MAC model has higher security, but less flexibility, so it can not adapt to the frequent switching between subjects and objects in the cloud environment. The role is a collection of a number of rights, refers to the rights set about access resources and operating rights assignment of a task [5]. The RBAC model introduces the concept role into access control, it associates rights with roles. Users get the authority by becoming a member of the proper role instead of getting authority directly, this can greatly simplify the rights management, reduce the complexity of authorization management, improve the flexibility of security policy. As the middle layer between user and rights, role achieves the separation of user and authority, enhances their independence, especially simplifies the large-scale network applications authority. RBAC has relatively fixed roles and corresponding permissions, but it lacks the consideration of the context, so it is not suitable for the distributed environment with complex roles and frequent changes. Due to the lack of dynamic attribute of RBAC model, Thomas et al. proposed TBAC(Task-Based Access Control) model which is a kind of active security model based on task oriented and dynamic authorization [6]. TBAC model considers the implementation of the environment

context, to determine whether to grant access to the subject [7], it considers the implementation of current task and manages authority dynamically according to the tasks state. The TBAC model is very suitable for information processing of distributed computing and multipoint access control, workflow, distributed processing [8], and transaction management system decision making etc., but it does not support passive access.

In order to give full play to the advantages of RBAC and TBAC, an access control model T-RBAC (Task-Role Based Access Control) is proposed, such as Wang and Zhao [9] proposed T-RBAC has different access control strategies for different access users, and provides hierarchical security features to improve the accuracy of access control. Huang Yi et al. proposed to improve the accuracy of access control through the classification of roles and permissions [10], all these T-RBAC solve the problem of cloud access control to a certain extent, but these models have the shortcomings of fuzzy classification, lacking the authority interaction between the objects and their owners, especially those sensitive data, privacy information who need fine-grained access control under distributed conditions. A CT-RBAC (Classified Task-Role Based Access Control) model is presented in the paper, the model will give full consideration to the role assignment, task attribute and object sensitivity, through dynamic rights assignment according to object security requirements level, it makes access control more accurate.

3 Design of CT-RBAC Model

3.1 Definitions and Rules

Cloud computing uses the third party data storage and management under distributed environment, it bases on the hypotheses that cloud service providers are believable and they have super user privileges. It is these two hypotheses that may cause potential security risks. So the CT-RBAC model are design based on the following principles.

Principle 1, the cloud service providers are not believable. Most of the T-RBAC model suppose the cloud servers as the believable third party, so it can be used as the middle transfer of authority, but the cloud server is not believable at most time.

Principle 2, the cloud service providers do not have super user privileges. The users' information are stored in the cloud server, their information storage, backup, maintenance and management are all managed by cloud service providers, but users usually do not make any restrictions for cloud service providers on privileges, so cloud service providers actually have the super user privileges on users' data management. This is contrary to the users' security needs.

Principle 3, safety and efficiency. Due to the distributed, concurrency, and dynamic nature of cloud computing, the excessive emphasis on security will affect the efficiency of access control and reduce the user experience. So the right strategy is needed to balance security and efficiency.

Principle 4, flexibility. Some RBAC models are used to group users, which can improve the simplicity of role division, but it limits the flexibility and mobility of user roles. The CT-RBAC model does not block users, it authorize all users uniformly in order to adapt to the dynamic execution of cloud computing and the characteristics of distributed access.

In order to facilitate the expression, the related concepts are expressed as follows.

Users set $U = \{u_1, u_2, \ldots u_m\}$, ($m \in N$, N is natural number set), represents the subjects of the initiate, in cloud computing environment users can be businesses, individuals or other services that apply for the cloud services.

upload() represents the operation of upload.
identity() represents the operation of identification.
grant() represents the operation of authorization.
bool() represents the Boolean function.
$\rightarrow$ represents the process of implementing related operations.
ob represents objects.
ow represents objects owners.
cs represents cloud services servers.

3.2 Architecture of CT-RBAC

The TBAC model is usually divided into high, medium and low three security levels according to the security requirements of the task. The RBAC model is also divided into high, medium and low three grades according to different roles. Whether tasks or roles, their ultimately security requirement is the object security attributes. So in order to make up for this deficiency, it is necessary to give an initial sensitive level to all objects. This value should be set by the owner of the object.

Here we divide the sensitive level of object into four grades, they are open access object, part shared object, limited shared object and the exclusive object, their sensitive level are st_1, st_2, st_3, st_4, let sensitivity set $St = \{st_1, st_2, st_3, st_4\}$, to represent the degree of resource sharing. st_4 corresponds to the open access objects, who can be accessed without the consent of the object owner. st_3 corresponds to the part shared objects, this kind of object is open or shared to certain types of objects, so its access control requires only the consideration of how to define the scope of the group and identify its members. Because this part of the object is large and commonly used, if all them are authorized by the object owner, it will inevitably lead to frequent interaction and low access efficiency, so, this type of object can be authorized by the agency, The access control authority can be done by cloud service provider's proxy servers instead of objects owners, this will reduce the authorized interactions, improve authorization efficiency, the objects owners only need to set the filtering conditions, this strategy can reduce the switching frequency of interaction, improve the efficiency of management. st_2 corresponds to limited shared

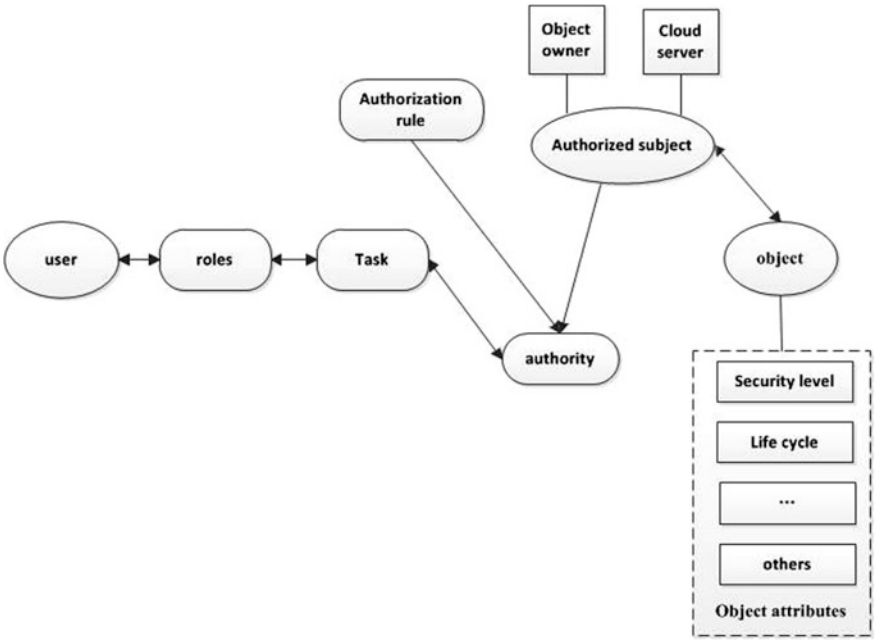

Fig. 1 CT-RBAC model structure diagram

objects which occupied by their owners only at first, not shared by a group, any applying for sharing must get the owner's authority, and the authority can not be transmitted by the authorized users, the authorization is not transitive. st_1 corresponds to the exclusive object, the object is a private information that is only required to be exclusive and will not be authorized to anyone. So any shared request is illegal except its owner.

CT-RBAC model adds the initial object security level and the authorization policy of authorized agent on the basis of the T-RBAC model, the model structure is shown in Fig. 1.

The implementation of the CT-RBAC model can be described as:

Step 1 the user sends an access request.
Step 2 the cloud server identifies the highest security level of the object in the requested task and matches the request role level, if matched, authorizes the request by the authorization policy, otherwise, submits the request to the object owner to determine whether authorized.
Step 3 create tasks, allocate resources.
Step 4 record the life cycle of the task, realize the object access.
Step 5 determine whether the task is over and recycle related resources and permissions.

There are two issues that need to be focused on in the model, one is the classification of the security level of the object and the proxy authorization strategy, and the other is the authorization transfer problem.

First, we discuss the classification of the security level of the object and the proxy authorization strategy.

The process can be described as:

1. The object owner uploads resources to the cloud server.

$$upload(ob_{ow}) \rightarrow cs$$

2. The cloud server identifies whether the object owner has marked the object sensitivity.

$$identify(ob) = value_{st}, (value_{st} \in \{st_1, st_2, st_3, st_4, \phi\})$$

3. If $value_{st} \neq \phi$, According to the value of $st_i, i = \{1, 2, 3, 4\}$ cloud server stores them correspondingly, those high sensitivity data should be blocked, marked, and encrypted.
4. If $value_{st} = \phi$, the cloud server asks the object owner to give a sensitivity level to the object, and then jump to step 2 to rejudge, if the sensitivity level has been given, process it in accordance with step 3, otherwise skip to step 5.
5. If the object owner ignores the hint and continues to upload the object to the cloud server, then assign a default value st_3 to the object. The reason is that the object owner ignore the reminder shows that there is not much sensitive information contained in the object, but from the view of resource protection, we should limit the scope of access. If a user access request is higher than the cloud server authorization level, the cloud server can submit the request to the object owner to determine whether to authorize. The object owner has the rights to change the sensitivity level of the object.

Now, the object has the original sensitivity attributes, then the user involves an efficiency issues in the following authorization strategy. The authorization strategy is as following.

The object with sensitivity level st_1 does not set other user access rights, its permissions can not be passed.

$$bool(grant(ob)) = false, \text{if } u_{ob} \neq ow_{ob}, u \in U$$

The object with sensitivity level st_2 is authorized by the object owner, and the authorization is not transitive

$$bool(ow \rightarrow grant(u_i)) = true$$
$$bool(u_i \rightarrow grant(u_j)) = false, u_i, u_j \in U, (i \neq j)$$

The object with sensitivity level st_3 is authorized by the cloud server agent, and the members of the group can pass the authorization.

$$
\begin{aligned}
&bool(ow \rightarrow grant(u_i)) = false,\\
&bool(ow \rightarrow grant(cs)) = true,\\
&bool(cs \rightarrow grant(u_i)) = true\\
&bool(u_i \rightarrow grant(u_j)) = false, u_i, u_j \in U, (i \neq j),
\end{aligned}
$$

The object with sensitivity level st_4 is authorized by the cloud server agent and the authorization can be passed.

$$
\begin{aligned}
&bool(ow \rightarrow grant(u_i)) = false,\\
&bool(ow \rightarrow grant(cs)) = true,\\
&bool(cs \rightarrow grant(u_i)) = true\\
&bool(u_i \rightarrow grant(u_j)) = true, u_i, u_j \in U, (i \neq j),
\end{aligned}
$$

This process is shown in Fig. 2.

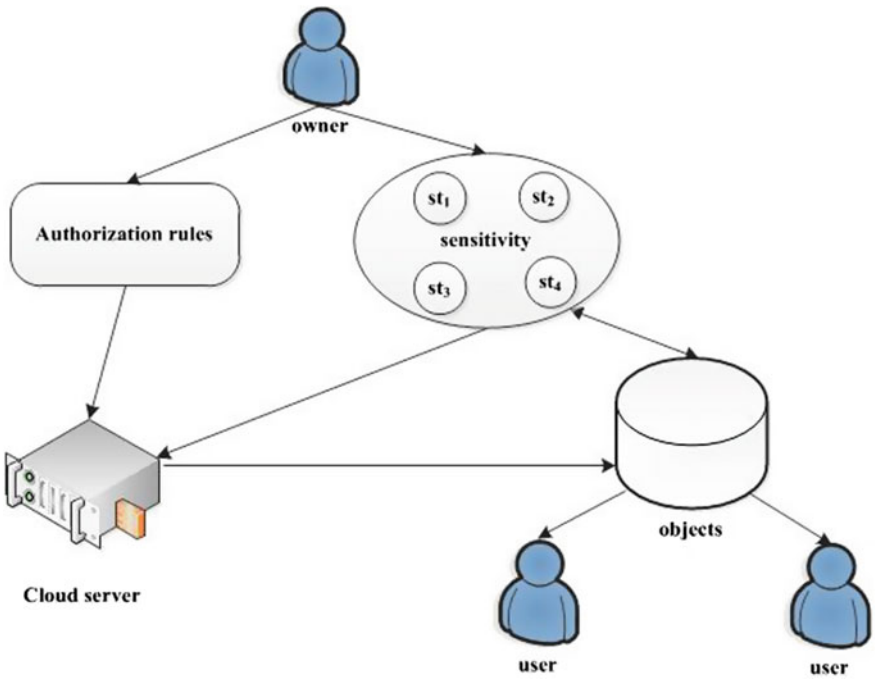

Fig. 2 Authorization policy diagram

4 Conclusion

Based on the T-RBAC model, the object owner has divided the sensitivity level related to the object, in order to avoid the security level change caused by data transfer or storage location change, the CT-RBAC formulates the authorization rules between the object owner and the cloud server. It realizes the combination of cloud server proxy authorization and the object owner authorization to those high sensitivity information. It also improves the efficiency and security of access control, realizes the fine grained access control.

References

1. Jiang Z-W, Zhao W-R, Liu Y, Liu B-X (2013) Model for cloud computing security assessment based on classified protection. Comput Sci 40(8):151–156 (in Chinese)
2. Xin Chen, Wang X-H, Huang H (2009) Research on multi-attribute information security risk assessment method based on threat analysis. Comput Eng Design 30(1):38–41 (in Chinese)
3. Fan J, Xue Y (2010) Information security risk assessment method based on traffic and classified protection. Comput Digital Eng 38(3):112–115 (in Chinese)
4. Yang H, Fong S (2013) Countering the Concept-drift Problem in Big Data Using iOVFDT. IEEE Int Congr Big Data 2013:126–132
5. Wang Y-D, Yang J-H, Xu C, Ling X, Yang Y (2015) Survey on access control technologies for cloud computing. Journal of Software 26(5):1129–1150 (in Chinese)
6. Hong C, Zhang M, Feng DG (2010) AB-ACCS: a cryptographic access control scheme for cloud storage. J Comput Res Dev 47:259–265
7. Li W-G, Zhao F-Yu (2013) RBAC permission access control model with attribute policy. J Chin Comput Syst 34(2):328–331
8. Li F-H, Su M, Shi G-Z, Ma J-F (2012) Research status and development trends of access control model. Acta Electronica Sinica 40(4):805–813 (in Chinese)
9. Wang X-W, Zhao Y-M (2012) A task-role-based access control model for cloud computing. Comput Eng 38(24):9–13 (in Chinese)
10. Yi H, Li K-L (2013) Model of cloud computing oriented T-RBAC. Application Research of Computers 30(12):3735–3737 (in Chinese)