A Dynamic Multi-domain Access Control Model in Cloud Computing

Dapeng Xiong, Peng Zou(✉), Jun Cai, and Jun He

Science and Technology on Complex Electronic System Simulation Laboratory, Academy of Equipment, Beijing 101416, China
{DapengXiongLNCS, PengZouLNCS, JunCaiLNCS, JunHeLNCS}@Springer.com

Abstract. Access control technology is an important way to ensure the safety of the cloud platform, but the new features of cloud computation environment have brought new challenges to access control technology. Direct at the existing problems of flexibility, timeliness and other aspects in multi-domain access control in the current cloud, on the basis of task driving idea, this paper put forward a dynamic access control policy. New method combined the advantage of RBAC and task driving model, to implement a more flexible and efficient access control model. Through comparative experiment we draw that new policy was improved to be contributory in improving the flexibility and availability of role-based multi-domain access control model .

Keywords: Access control · Dynamic RBAC · Cloud · Multi-domain

1 Introduction

As a new computing model in the initial stage, cloud computation has brought great convenience to people in Internet era with its advantages of large scale, virtualization and high flexibility and so on. However, there is still much room left for improvement of cloud security. As the core technology to guarantee the safety of cloud computing system, access control technology ensures the protection of cloud computing resources to be accessed by legitimate users or programs, avoid unauthorized information leakage, so as to assure the safety and legal use of cloud computing resources. Cloud computing platform is a complex information system, characterized by large scale and distribution according to needs and so forth, these characteristics has brought new challenges to access control technology. Cloud computing environment is a virtual organization composed of various autonomous domains, users and resources are in different autonomous domains, and the relationship between users and resource providers is dynamic. Under these distributed multiple domains, access control mechanisms should be adequately flexible and dynamic in order to ensure the safety access in the multi-domain environment of cloud computing. However, there have been serious deficiencies of each existing product cloud in multi-domain access control. Therefore, the research of multi-domain access control model under cloud computing environment is of important scientific significance and application value.

J.H. Abawajy et al. (Eds): SSCC 2015, CCIS 536, pp. 3–12, 2015.
DOI: 10.1007/978-3-319-22915-7_1

Based on the analysis of requirements and difficulties of multi-domain access control under cloud computing environment, this paper extended and improved role-based multi-domain access control model, which introduced task-based driving mechanism and can dynamically adjust the inter-domain role mapping as needed, thus better solving the problem of inter-domain role mapping. Meanwhile, it solved the problem of policy conflict by the mean of inter-domain policy combination. Finally it completed the experiment on Openstack cloud platform, which proves that this model has advantages in safety and availability.

2 Related Work

2.1 Problem Analysis

Multi domain is one of the important features of the cloud computing environment. Before we discuss the multi-domain access control issues, we need to clarify the definition of domains in the cloud. Autonomous domain refers to "managerial authority of independence and autonomy, users and resources belonging to centralized management, physical organization or logical organization that has independent access control policy space and the only access control decision points" [1]. A typical cloud computing architecture is a distributed network environment made up of multiple autonomous domains. An example of multi-domain is as shown in the following figure (Fig. 1):

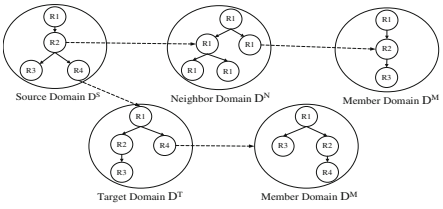

Fig. 1. Structure schematic of multi-domain

Under the cloud computing multi-domain environment, a subject of a security domain should manage access authority of its own domain resource, and meanwhile apply to other security domains for resource access authorization. So, multi-domain access control is divided into intra-domain control and inter-domain control. Intra-domain control manages internal resources via the authority and policy established by itself, inter-domain control manages cross-domain resources operation through authorization control. To solve the multi-domain access control in cloud computation is to achieve inter-domain authorization and access control while ensuring intra-domain autonomy and security.

What is an ideal multi-domain model of cloud computation? To meet the needs of multi-domain authorization and the characteristics of the cloud, it is necessary to establish a general access control model, which should meet the following requirements:

(1) **Suitability**. Security interoperation should be able to better fit different security policies of each autonomous domain and should not cause security policy conflict or adjustment within each autonomous domain.
(2) **Responsive**. Reasonable response should be made to the request for cross-domain resource access. Under the premise of ensuring two-party security of interoperability, make a response to initiator's request for resource operation ASAP (authorized or rejected)
(3) **Scalable**. The model should be adapted to the characteristics of enormous amount, real-time change of intra-domain users and organization domains, which can flexibly expanded along with the change of the scale and structure of the domain. Here we tend to distributed access management, rather than centralized access decision.
(4) **Real-Time**. The model should have the ability to adjust in real time and can make a quick authorization decision according the adjustment of domain and users' access application, and cross-domain authority should be dynamically allocated and revoking.
(5) **Realizable**. A good security interoperation mechanism should be easily implemented, without introducing complex management support platforms.

2.2 Research Status

The most remarkable characteristic of multi-domain environment is distributed. Multi-domain access control technology in cloud computation has inherited and developed from the distributed multi-domain access control technology, and meanwhile we should also recognize that could computing system has great differences in multi-domain authorization compared to other distributed systems. Thus new characteristics of multi-domain access control under the cloud computing environment should be fully considered, to design access control model suitable for multi domains. At present, the research of multi-domain access control technology in cloud computation mainly focuses on the following aspects:

(1) **Designing of Multi-domain Access Control Model**. Mainly to solve synthesis problem of cross-domain access control strategy, to implement authorization access control of multi-domain coordination.
(2) **Policy Conflict Detection and Elimination.** To solve the problem of inconsistent access control rules introduced because of the synthetic strategies of multi-domain access control, detect and eliminate authentication and authorization that has conflicts.
(3) **Security Analysis of Strategies.** To prove that the designed access control model is safe and reliable and will not bring the authority leakage and other safety hazards.

The traditional multi-domain access control technology has been widely used in distributed information system. The common approaches of multi-domain access control mainly concentrate on the following categories: role-based access control,

attribute-based access control, trust-based access control, or the enhanced combination of the above several strategies [2].

Difficulties in traditional multi-domain access control strategy. The dynamic, distributed, heterogeneous and autonomous multi-domain environment has presented new challenges to computational intra-domain and inter-domain security interoperability. The current multi-domain access control approach still has some deficiencies existing in the application in cloud computing platform in flexibility, security and availability and other aspects; it is mainly reflected in the following aspects:

- **Cross-Domain Interoperability.** How to construct multiple security domains for security policy of inter-domain interoperability, to ensure safe resource interoperability between security domains.
- **Policy Conflict**. How to coordinate and solve the problem of inconsistent security policy between intra domains and extra domains. The policy to assign access object tenant between users and tenants may conflict against each other. The policy decision point (PDP) should use the predefined algorithm, to solve the conflict.
- **Security of Policy**. The synthetic strategy should prevent permission leakage caused by cross-domain access. If the operation is prohibited in autonomous domain, it should also be forbidden in interoperability.
- **Management Mode**. Centralized cross-domain authorization is easy to avoid policy conflict and convenient for implementation, but it has poor expansibility and is easy to cause single point failure. While distributed cross-domain authorization is easy to extend and accord with the support of secure interoperability to local autonomy, but it's difficult to form a global view of strategies, prone to causing security conflict.
- **Moderate Control**. Excessive introducing various control mechanisms bring difficulties to achieve the access control policies, and also may affect the performance.

We took the OpenStack for example to analyze the implementation and existing problems of access control in a typical commercial cloud platform.

2.3 Access Control in OpenStack

OpenStack is the most representative open-source cloud computing platform. OpenStack (JUNO version) contains the following components: Nova, Neutron, Horizon, Swift, Glance, Cinder and Keystone etc., among which Keystone is an authorization control module of OpenStack, responsible for the authorization, service rules and service permission token, which implements Identity API in OpenStack.

Domains represent collections of users, groups, and projects in Keystone. A user, group or item can only belong to one domain, but they can be associated with other domains through authorization. Each domain has a namespace in Identity API, containing some unique attributes only visible to API. In the unique domain attributes of theses definitions, domain name and role name are visible to all domains, while project name, group name and user name can only be visible within the domains [3].

OpenStack Access Control (OSAC) module realizes the access control through the certification authority in Keystone; its core is the extension of typical role-based access

control model. A brief description of OSAC' mechanism is as follows. As a role-based authorization model, the core part of OSAC is the role assignment. The user, group and item have a corresponding role, and permission is only related to the role, so all the items can get the authorization through the role. The user can be associated with item belonging to other domain by being authorized a user role of another item. The role-based access control model modifies the role of cross-domain users according to the permission of extra-domain resources in the service to achieve cross-domain authorization control, with great flexibility. The disadvantage of OpenStack authorization control is too coarse granularity of access control.

3 A Role-Based Multi-domain Access Control Policy in Cloud

In this section we focused on the features of cloud computing environment to construct and realize a security interoperability model suitable for distributed heterogeneous multi-domain environment. The design purpose of this model is to establish a multi-domain access control model based on dynamic role mapping, by means of role mapping, that is to realize resource access by constructing an inter-domain equivalence relation.

3.1 Task-Driving Dynamic Role Assignment

As role assignment based on role mapping is unchanged upon consultation, this way of authorization has disadvantages in permission timeliness and distribution on demand and other aspects. In RBAC model, another important concept, task, was introduced in this paper. The task (or activity) herein is the joint name of all cross-domain operating processes initiated by users. Task-role based access control (T-RBAC) solves security problems from the perspective of the user needs, which is an active security model based on task and using dynamic authorization. By adopting the viewpoint of task oriented, security model was established and security mechanism was implemented from the angle of tasks, and real-time security management was provided during the task processing, whose basic ideas are as follows (Fig. 2):

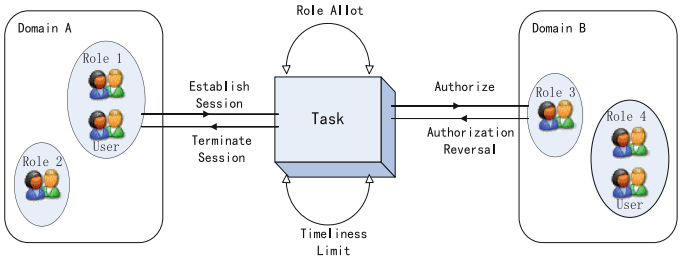

Fig. 2. Task-driving dynamic role assignment

(1) Combine access permission with task, the execution of each task is considered as a process that subject uses relevant access permission to access the object. During the task execution, the permission is consumed. The subject cannot access the object any more when the permission is exhausted,
(2) The access permission that the system grants to users is not only related to subject and object, but also associated with the current tasks of subject and task status. Object's access control permission is not stationary, but varies along with the change of tasks in this context. Due to the active, dynamic and other characteristics of T-RBAC, it has been widely used in decision making of information processing and transaction management system of workflow, distributed processing and multipoint access control.

This paper introduced task-driving mechanism, permission could be updated and overdue authorization should be revoked in real time according to the needs of current tasks. By combining the timeliness of task model and the flexibility of role model, it proposed a task-driving multi-domain access control model based on role mapping.

3.2 Real-Time Multi-domain Access Control Policy Synthesis

The main approach of RBAC-based multi-domain policy synthesis is the role mapping, which is to realize resource access by establishing an inter-domain role equivalence relation. The current role-based cross-domain policy synthesis approach can be divided into static mapping and dynamic mapping according to the question whether it can realize dynamic role mapping. The static mapping is a tightly coupled, global role mapping approach with a coordination center. One of the most classical frameworks of static mapping approach is the global role mapping method proposed by Shafiq [4]. The dynamic mapping is a loosely coupled approach based on request act with no coordination center. Smithi Piromruen et al. [5] proposed a dynamic interoperability framework between domains stand for Dynamic policy synthesis.

Two traditional synthesis methods have some limitations when applied in cloud computing environment. With the global efficiency, the static role mapping has an advantage in large-scale distributed intra-domain policy synthesis, but acts inefficiency in highly interactive conditions. With local flexibility, the dynamic role mapping has advantage in the policy synthesis in the scene of rapid role updating and frequent interaction among domains, but is incapable of action for large-scale and heterogeneous scene.

In the real multi-domain cloud computing scenario, the virtual domain has large scale, complex structure, and strong instantaneity, the use of single static or dynamic synthetic policy cannot meet the demand. This paper introduced role management engine in the management domain, by combining the advantages of these two role mapping approaches, it adopted static and dynamic synthetic policy separately in global policy synthesis and local policy renewal, as shown in the following figure (Fig. 3).

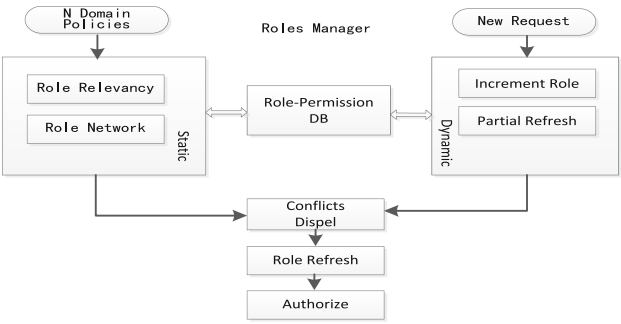

Fig. 3. Real-time multi-domain access control policy synthesis

Extending the idea of task-oriented, we combine static and dynamic synthesis method according to the task. Then provide real-time dynamic cross domain strategy synthesis to meet new request. The basic idea is as follows:

(1) Static strategy and dynamic policy updating models are managed by the engine of Role - permission manager, the two works together to maintain a role - permission Table
(2) Global synthesis module draw roles - permission map between domains in advance, then resolute conflicts uniformly. This process is time-consuming, but to ensure the safety and non - redundancy. Suitable for regular maintenance, such as in the access control engine initialization stage, take a long time to generate a global role authorization table, then to calculate and update it in the system idle time.
(3) Local strategy updating is task driving. Update related roles and permissions table in order to meet the new request. The domain map authorization requests from other domains to a part role set, which will be processed with permission mapping and conflicts resolution, so as to achieve the inter domain access.

The combined method can not only adapt to the global strategy for synthesis of large scale, heterogeneous multi domain environment, meanwhile to fulfill local strategy aroused by task. The synthetic methods have advantages in flexibility and availability compared with traditional multi-domain strategy.

4 Simulations and Performance Analysis

The experimental environment: 4 single CPU (each CPU4, frequency 1.6 GHz, memory 4G) servers. We set up a small cloud computing environment, which simulates a multi-domain environment consisted of 8 domains. Network topology of the cloud environment is as shown in Fig. 4.

Two simulation experiments have been designed in the multi-domain environment. One purposed to inspect the ability of Task driving RBAC model. Another aimed to observe the effect of the real-time multi-domain access control policies combination.

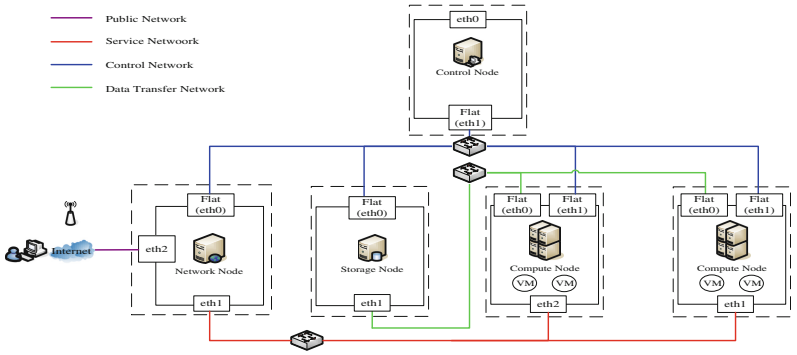

Fig. 4. Network topology of the experiment cloud

4.1 Task Driving RBAC Model

The purpose of the first experiment is to prove that, the task driving RBAC model which bring in the authorization mechanism of limited aging, will keep the risks of policies conflict low.

In order to illustrate the effect of Task driving and Aging Authorization, a contrast experiment was designed as follows. The experiment compared the history of policy conflicts along with cross-domain requests, in the case of RBAC bring in aging authorization or not. Experimental results as shown in Fig. 5.

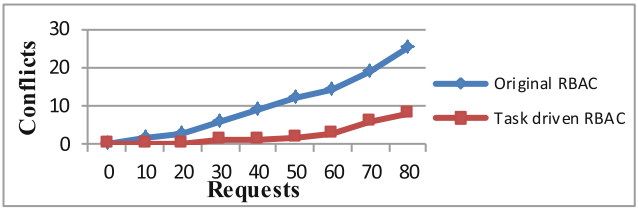

Fig. 5. Experiment result of task driving RBAC model

By analyzing the experimental results, we can get the following conclusion. The original design of RBAC algorithm maintained in the given user role authorization, thus with the passage of time, newcomer of role authorization may cause conflicts against the existing authorization. While the new algorithm based on task driving RBAC bring in the aging control for each authorization, in which the manager will revoke the role authorization forwardly in a certain period of time after the session is completed, accordingly avoid unnecessary permission leakage due to expired license.

4.2 Real-Time Global Policy Synthesis

The purpose of the second experiment is to prove that, the real-time fusion method of global static synthesis and partial dynamic synthesis can improve the abilities of multi-domain access control policy synthesis.

In order to illustrate the effect of Real-time Global Policies Synthesis, a contrast experiment was designed as follows. The experiment compared the time consumption of policy synthesis, between Static synthesis method, Dynamic synthesis method and the new real-time synthesis method. We measured the relation between time consumption and real-time request and the scale of domains, in three test bed adopting different policy synthesis. Experimental results as shown in Fig. 6.

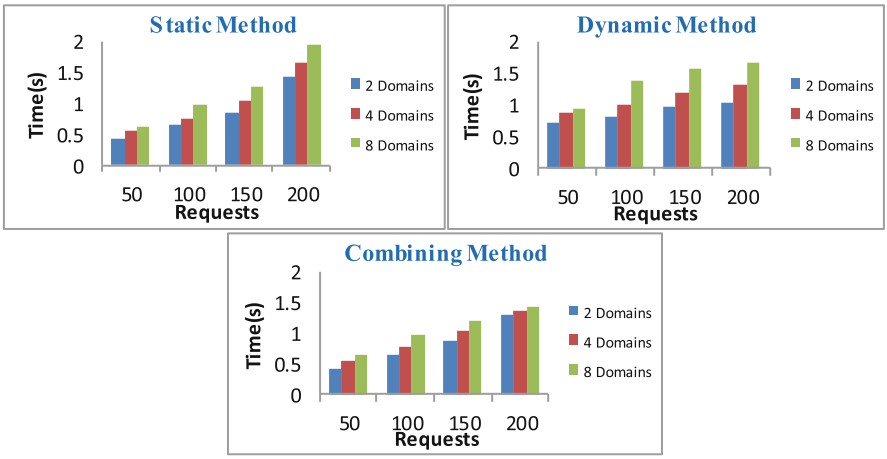

Fig. 6. Average time of policy synthesis

By analyzing the experimental results, we can get the following conclusion. Integrating real-time strategy synthesis method combines the advantages of two methods, using global synthetic strategy in large-scale initialization, using local dynamic update to meet the real-time request. Overall, the real-time strategy synthesis method saves synthetic time, has a certain degree of improvement on the flexibility and usability. We did not test its effect of our method in a much larger domain limited to environmental conditions.

5 Conclusion

On the basis of the analysis of technical defects existing in multi-domain access control in the current cloud computing platform, this paper improved the Role-based multi-domain access control model by bringing in aging control and policy synthesis manager, and the experiment showed that, this model has superiorities in certain conditions. (1) Compared with the general RBAC algorithm, this method can update the permissions according to task requirement timely, and revoke permissions at the end of the task, thereby reduce the possibility of permission leakage. (2) Dynamic updating role - access tables according to requests, to reduce the calculation time of global strategy of synthetic, and improve the efficiency of authorization. This paper

also has some shortages in the following aspects worth further research. (1) How to determine the appropriate aging time. (2) A larger scale multi-domain test.

Acknowledgments. This research has been supported by National High Technology Research and Development Application of China (2012AA012902) and "HGJ" National Major Technological Projects (2013ZX01045-004).

References

1. Xiangran, C.: Research on key technologies of role-based secure interoperation in multi-domain environments. In: For the Degree of Master of Military Science (2010)
2. Punithasurya, K.: Jeba Priya S: Analysis of Different Access Control Mechanism in Cloud. Int. J. Appl. Inf. Syst. **4**(2), 34–39 (2012)
3. OpenStack API Complete Reference. http://developer.openstack.org/
4. Shafiq, B., Joshi, J.B.D., Ghafoor, B.E.: A secure interoperation in a multi-domain environment employing RBAC policies. IEEE Trans. Knowl. Data Eng. **17**, 1557–1577 (2005)
5. Piromruen, S., Joshi, J.B.D.: An RBAC framework for time constrained secure interoperation in multi-domain environment. In: IEEE Workshop on Object-oriented Real-time Databases (WORDS-2005) (2005)