Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2016, Vol. 8, No. 4

T-RBAC based Multi-domain Access Control Method in Cloud

Dapeng Xiong, Liang Chen

Academy of Equipment，Beijing 101416，China

E-mail: xiongdapeng@outlook.com, 252958524@qq.com

Received: November 6, 2016 Accepted: December 30, 2016 Published: December 31, 2016

DOI: 10.5296/npa.v8i4.10411 URL: http://dx.doi.org/10.5296/npa.v8i4.10411

Abstract

Access control technology protects the cloud from being accessed illegally. However, traditional access control method cannot meet the new demands of the cloud environment. In order to improve the deficiency of the current multi domain access control method in timeliness and flexibility. This paper puts forward a dynamic access control policy on the basis of task driving mechanism. The new method combines the advantage of RBAC and task driving mechanism, introduces in limit aging and real time strategy synthesis. Comparative trials show that the new policy had an advantage in flexibility and availability of multi-domain access control model.

Keywords: Access Control, RBAC, Task driven, Cloud, Multi-domain.

1. Introduction

Access control is one of the core technologies to enhance the safety of cloud computing environment, which protects the cloud resources of legitimates users from unauthorized information leakage. Cloud is a virtual architecture composed of various autonomous domains, where users and resources located in different autonomous domains. The purpose of multi-domain access control is to realize the necessary access of inter domain resources on the premise of ensuring the security of the inner security of domain. In order to achieve this purpose, two tasks should be satisfied: one is to identify and confirm the user who access the system, another is to determine what bound of legal resources the user can access. A motion of cross-domain access is as shown in fig.1.

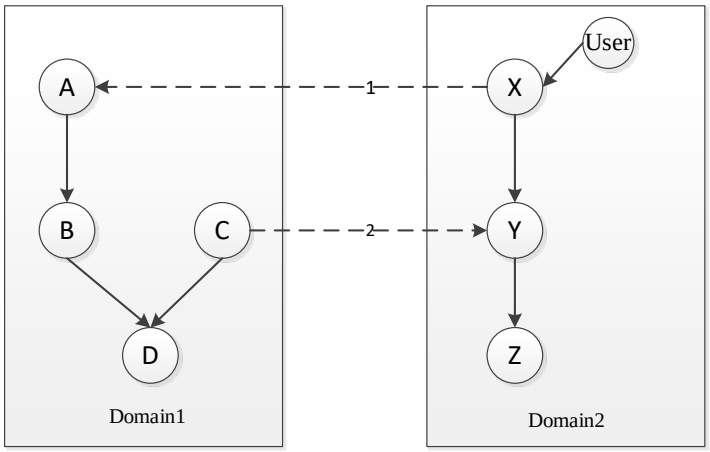

Figure 1. Typical Cross domain Access in Cloud

Each autonomous region runs an independent access control policies. And there is a need for mutual access to resources between domains, which requires a corresponding access control model to coordinate and manage these inter domain interoperability. Multi domain access control technology in cloud is usually based on the RBAC, TRBC, attribute based access control model and other access control model. An example of cross domain access control schematic based on IRBAC2000 [1]is as it is shown in fig.2.

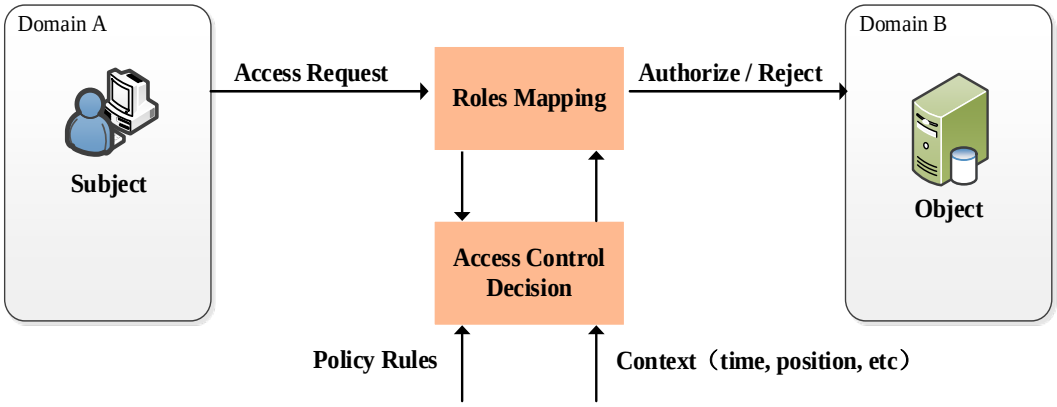

Figure 2. Cross domains Access schematic

A typical cloud computing is described as a distributed architecture consisted of

associated autonomous domains. Where autonomous domain refers to “Physical organization or logical organization that has independent access control policy with centralized, independent and autonomy management”[2]. In the cloud, users can access resources belong to another domain via cross domain authorization.

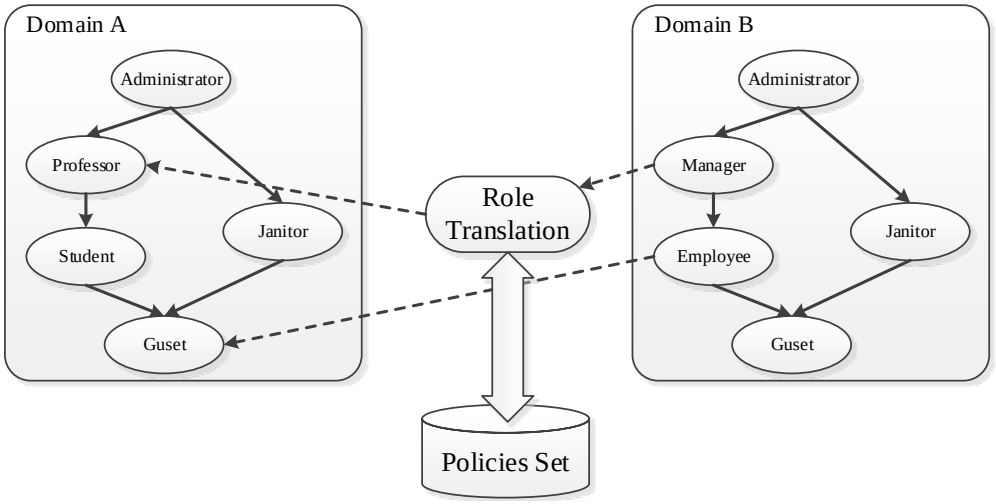

Figure 3. Cross domains Access via Role mapping

RBAC based multi-domain access control model can reach a consensus on security policy via role mapping. As shown in Figure 3, definition role mapping: $Manager_A \rightarrow Professor_B, Employee_A \rightarrow Guest_B$, inter domain roles can be convert to roles which can be understood by local domain. Then inter domain role A can obtain all permissions belong to local domain role B. Though this method meets cross-domain access request by role mapping, a security session should be established between them. The subject of a security domain should manage resources both access authority of its own domain and other neighbor security domains. Each domain runs as its own access control policy, meanwhile a public access control policy should be decided by both parties through consultation agree when sharing theirs resources. So, authorization between domains contains both inner-domain control and inter-domain control. Inter-domain access control manages internal resources via inner authority and policy, inter-domain control manages cross-domain resources operation by authorization control. Therefore, the key issue of multi-domain access control is to achieve cross-domain authorization and access control along with ensuring the security within the local domains.

An ideal access control model of cloud computing should meet the following needs of multi-domain authorization and the characteristics of the cloud. Security interoperation should be able to better fit different security policies of each autonomous domain and to avoid security policy conflict between domains. The model should response in real time according the adjustment of domain and users' access application, and cross-domain authority or rejected should be dynamically allocated or revoking. Should be easy to be implemented, and no extra complex management support is required.

This paper summarized the research status of multi-domain access control under cloud computing environment. Then proposed a novel access control model based on RBAC oriented in multi-domain environment. The method combined RBAC with task-driven mechanism, which can gratify the dynamical need of inter-domain role mapping. Meanwhile, it improved the policy conflict digestion problem via real-time global policy synthesis. Finally it realized this model on OpenStack and illustrated it has advantages in safety and availability in two experiments.

2. Related Work

2.1 Research status

The traditional distributed access control technology has been widely used in multi-domain system[3]. 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, and the improvements of these strategies.

Role-Based Approaches. The core idea of RBAC is to introduce the concept of the role to isolate users and permissions, so as to reduce the complexity of authorization management. Role-based access control(RBAC) has role hierarchy, least permission, separation of permission and other flexible features and also has the advantages of convenient management and intra-organizational matching. So it is more suitable for the application in a complex multi-domain environment, to meet the needs of inter-domain secure interoperability.

Attribute-Based Approaches. The core idea of attribute-based access control (ABAC) is not to authorize between subjects and objects directly, but to use the attributes related to security among subject and object and operation (subject attribute, object attribute and resource attribute etc.) as the basis of authorization decision. The advantage of ABAC is that it can fit the dynamic nature, expansibility of network environment.

Trust-Based Approaches. Trust-Based Access Control (TBAC) is mainly triggered from users' access permission, and to determine whether give user the right to access a resource by calculating the user's credibility.

Table1 Analysis of different access control model

Access Control Model	RBAC	TBAC	ABAC
Sample	RBAC96	TRBAC	ARBAC
Security	High	High	High
Flexibility	High	High	Normal
Reliability	Normal	Normal	Hard
Application	Complex scene	Work flow, Distributed system	Large scale, Dynamic expansion

Multi-domain access control in cloud has inherited and developed from traditional distributed multi-domain access control technology. In view of the characteristics of cloud

computing is different from the traditional information systems, cloud computing access control is facing many new problems. When designing multi-domain mechanism suitable for cloud, new characteristics of inner-domain and inter-domain access control under the cloud environment should be fully considered.

2.2 Access Control in Commercial Cloud

OpenStack is the most representative of the open source cloud computing platform. OpenStack access control (Control OSAC, Access) [4]achieves the certification authority via Keystone components, which is responsible for providing authentication and management of users, accounts and role information, authorization services. The core of OSAC is to extend the improved role based access control model. As a role based authorization model, the core part of OSAC is role assignment, including user assignment (UA), group allocation (GA) and privilege allocation (PA). In Keystone, the role represents a set of resources that can be accessed by the user, so that all users can access the authorization by role.

Web Services Amazon (AWS) [5]is an Amazon Co's cloud computing service platform. Access policy of AWS is divided into resource based strategy and user based strategy. Resource based strategy is to associate access authorization with the resources (storage buckets and objects), including the “storage bucket” policy and the access control list (ACL). Both the storage bucket strategy and ACL adopts the XML architecture to describe the corresponding relationship between the authorized person and the granted authority.

Ali cloud was founded in 2009 by the Alibaba group. Ali cloud uses RAM (Resource Access Management)[6] to provide users with the user's identity management and access control services, its core functions focus on user identity management and authorization management. RAM introduces the concept of group (Group) and role (Role) to facilitate the management of permissions and users. Sub - users have all the permissions of the group once join in the group. Role mechanism can solve the problem of one-time authorization of temporary users, users obtain the corresponding authority through the temporary role.

Overall, most of the current commercial cloud platform are adopting the traditional access control technology, the research on the cloud computing environment for access control technology is still in the exploratory stage.

3. A T-RBAC based Multi-domain Access Control Method

In this section we construct and realize a security interoperability model suitable for distributed heterogeneous in multi-domain autonomous environment. Target of this model is to establish a multi-domain access control model based on dynamic real-time role mapping.

3.1 Trust measuring based cross domain authority

Related trust measuring method decides the evaluation weight of role according to the role of the role level, then calculates the level of trust on the basis of the role of weight and the evaluation of user role. The basic ideas are as show in fig.4:

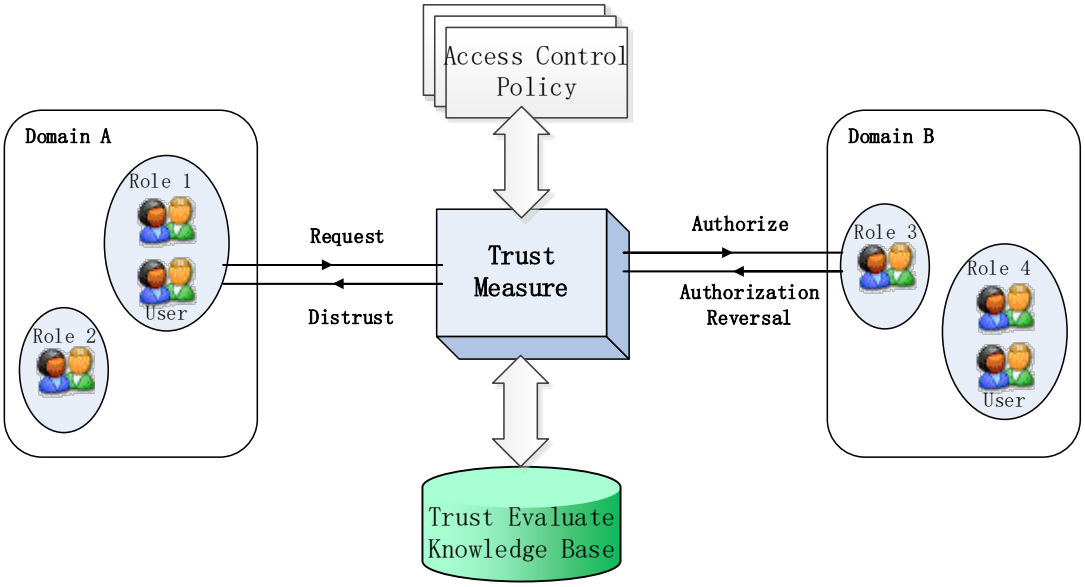

Figure 4. Trust measuring based cross domain authority

(1) Manage of role weight. Assign each role with the corresponding evaluation weights according to importance of the user role in the security domain, the higher the weight, the higher the user's level of authority.

(2) Role trust evaluation. Calculate the degree of trust between entities, represented by "T", the value of T affected with user behavior, context, time attenuation and other factors, the range of $T \in [0,1]$.

3.2 Task-oriented role assignment

Traditional role assignment based on role is fixed once concluded, this way of authorization ignore the dynamic changes of user action, has drawbacks in permission timeliness and distribution on demand. In this paper, we introduce important attribution of task. The task (or activity) is the collections of all cross-domain operating processes. The basic ideas are as show in fig.5

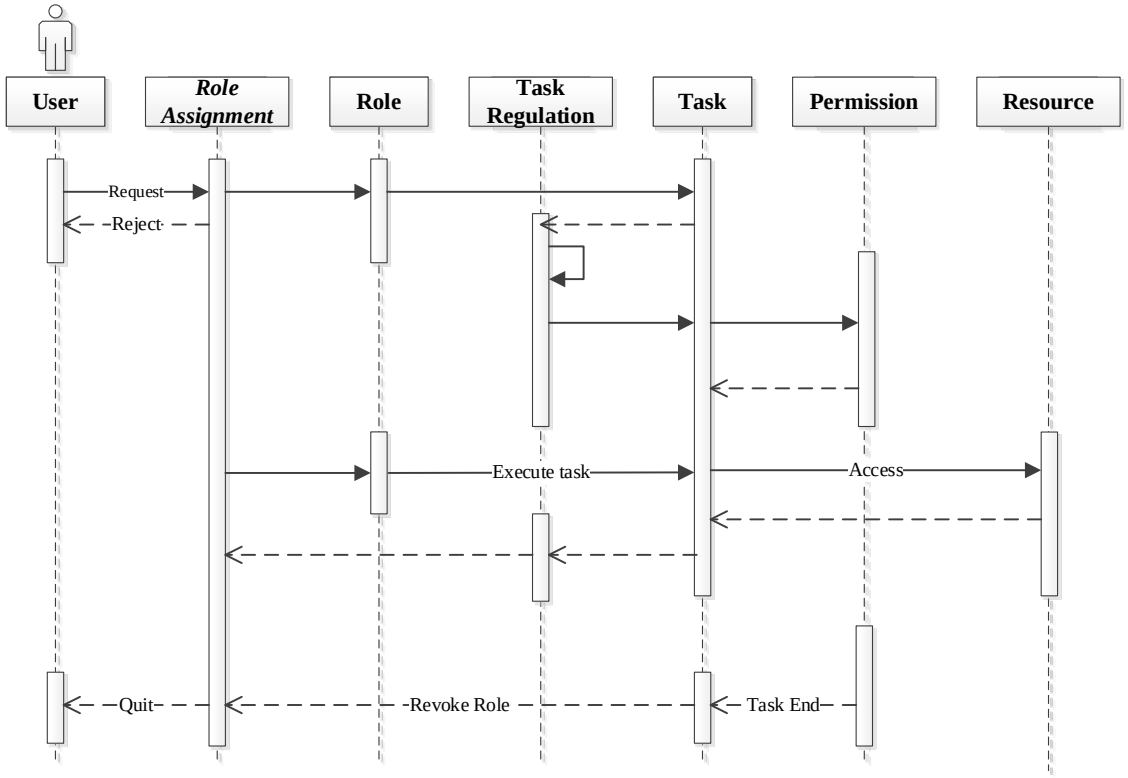

Figure 5. Task-driven role assignment

(1) Assign permissions on the basis of task status. Authorizations start when task request meets the condition. Permissions revoke when task pauses or does not meet the condition. When the task is finished, take back the role and revoke the user's role.

(2) Combine access role with task. Each execution of task is considered as a process that covert a local domain role to a cross domain role. At the end of task execution, the role is revoked, the subject cannot access the object without a given role when the permission is exhausted.

(3) Permission adjusted with the task dynamically. Object's access control permission is not static, but varies along with the process of tasks. Task-role based access control (T-RBAC) solves access control problems from the user needs, permission should be updated and overdue authorization should be revoked in real time according to the needs of current tasks.

3.3 Real-time access control policy synthesis

The dominant ways of RBAC-based access policy synthesis focus on role mapping by establishing an equivalent inter-domain role to realize resource access. The static mapping is a tightly coupled and global role mapping approach with a coordination center[7]. The static role mapping has advantages in large-scale distributed intra-domain policy synthesis, but in less highly interactive conditions. The dynamic mapping is a loosely coupled and distributed approaches based on request act with no coordination center[8]. The dynamic role mapping does well in the policy synthesis in the scene of rapid role updating and frequent interaction among domains, but acts inefficiency for large-scale and heterogeneous scene.

We introduce a role management engine to the management domain, which adopt static and dynamic synthetic policy separately in global policy synthesis and local policy renewal, as shown in the fig.6.

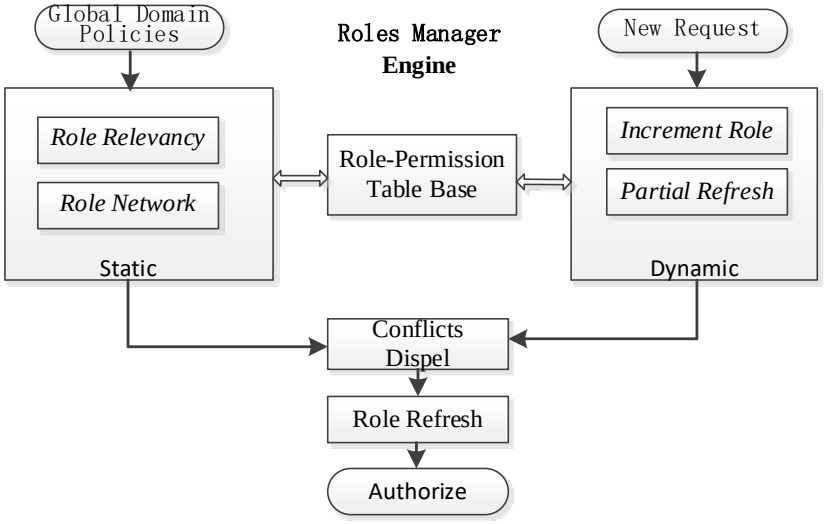

Figure 6. Real-time access control policy synthesis

Combining static and dynamic synthesis method according to the task. We provide a real-time dynamic cross domain strategy synthesis method. The basic idea is as follows:

(1) An engine of Role – Permission manager is set to maintain a role – permission table, which was statically strategized and dynamic updated along with the tasks.

(2) Global synthesis module draws a roles - permission map between domains preliminary, then sorted conflicts uniformly. This process ensured the safety and non - redundancy, but was time-consuming. Suitable for regular maintenance, such as in the stage of access control engine initialization.

(3) Localized strategy updating on the basis of task. Update current task related roles and permissions table to meet the new task request. The accessed domain maps the request from another domain to a partial role set, then incorporate into global table.

4. Simulations and Performance Analysis

Two simulation experiments have been designed in the multi-domain environment. The experimental hardware environment: 4 single CPU (each CPU 4 cores, frequency 1.6GHz, memory 4G) servers. We set up a small cloud computing environment based on OpenStack to simulated a multi-domain environment consisted of 8 domains. Network topology of the experimental environment is as shown in fig.7.

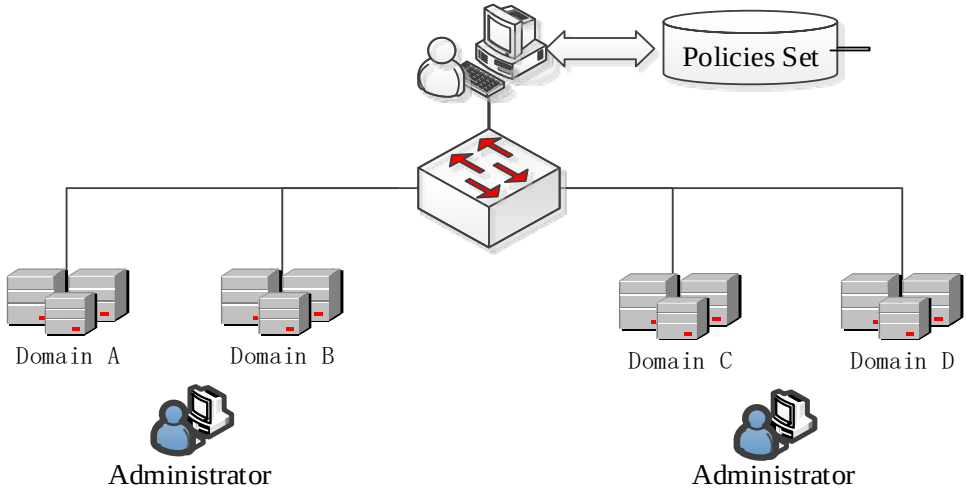

Figure 7. Network topology of the experiment

4.1 Security performance test

The purpose of the security performance test is to examine the ability of RBAC model with Aging Authorization. We compared the trend of policy conflicts along with cross-domain requests, in the case of RBAC bring in aging authorization or not. The experiment simulated the conflict detection process of cloud service. Random construction of a set of 10, 50, 100,150, 300,500, 800 requests to be detected. Experimental results as shown in Fig.8.

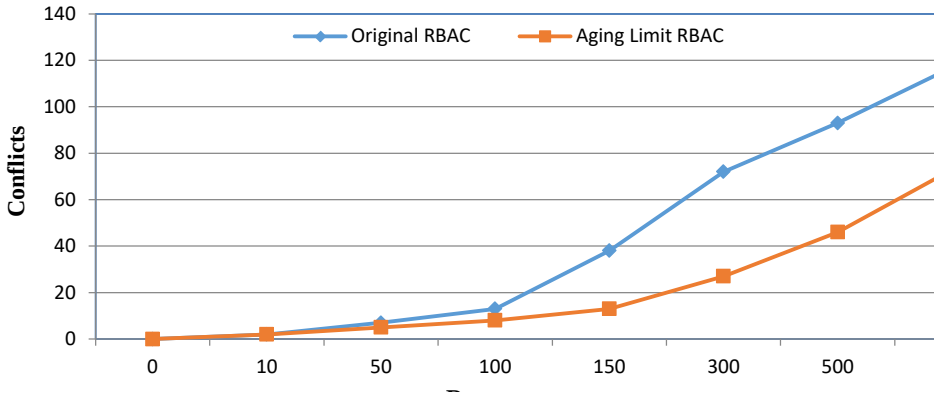

Figure 8. Security performance under different RBAC

The result proved that the task driven RBAC model can keep the risks of policies conflict low via bringing in the authorization mechanism of limited aging. The original RBAC algorithm kept the role authorization, ignoring the task changing, thus lead to conflicts against the existing authorization. While the algorithm based on task driven RBAC bring in the aging control for each authorization, where the manager will revoke the role authorization forwardly in a certain period of time after the session is completed, thus accordingly avoid unnecessary permission leakage due to expired license. Overall, the task-driven method has a certain degree of improvement on the security.

4.2 Efficiency performance test

The purpose of the efficiency performance test is to evaluate the performance of Real-time Global Policies Synthesis, We compared the time consumption of policy synthesis between Static synthesis method, Dynamic synthesis method and the real-time synthesis method. Experiment was implemented in three test bed adopting different policy synthesis to measure the relation between time consumption and real-time request and the scale of domains. Random construction of a set of 50, 100,150, 200,250, 300 requests to be detected. Experimental results as shown in Fig.9, Fig.10 and Fig.11.

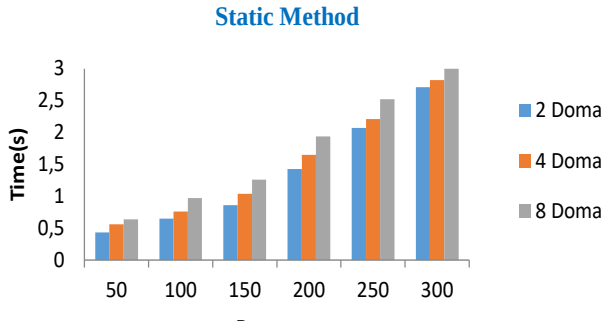

Figure 9. Average time of Static Method

Figure 9 corresponds to the average time of Static Method. The static method has advantages in smaller scale, however costs too much compared with other methods when as the system becomes more complex. It has advantages in primary stage, because the static method spends time on in initialization, but loses the advantage gradually for the lack of flexibility.

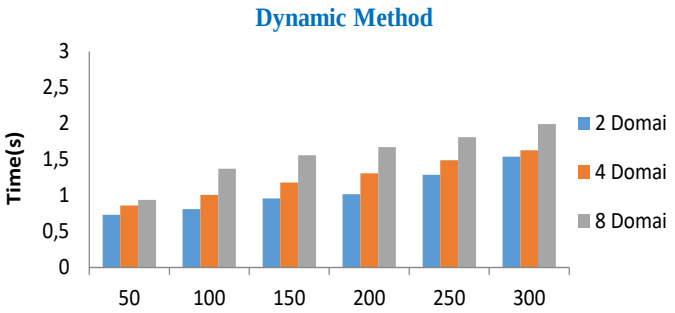

Figure 10. Average time of Dynamic Method

Figure 10 corresponds to the average time of Dynamic Method. The dynamic method has advantages in real-time adaptation, however costs too much compared with other methods in the begging. It has advantages in later stage, because the dynamic method could adjust locally, but costs much time in the primary stage without a global synthesis table.

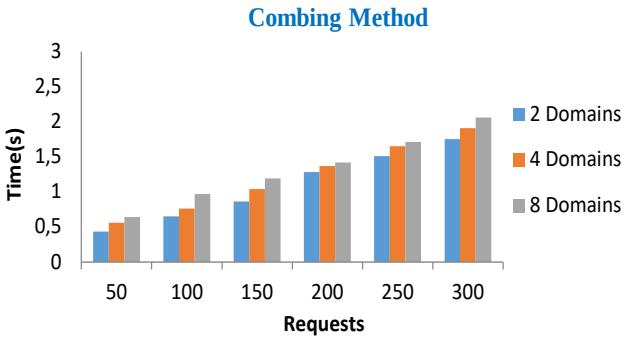

Figure 11. Average time of Combing Method

Figure 11 corresponds to the average time of Combing Method. In the preliminary stage from 50 to 100, the dynamic method cost the longest time. While in the later stage from 200 to 300, the static method cost the longest time. Combing method adopt global synthetic strategy in large-scale initialization, and using local dynamic update to meet the real-time request. It proves 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. We did not test its effect of our method in a much larger domain limited to environmental conditions.

5 Conclusion

This paper improved the Role-based multi-domain access control model by bringing in aging control and associative policy synthesis to the cloud. Compared with the common RBAC algorithm, this method can revoke permissions at the end of the task, thereby reduce the possibility of permission leakage. And the dynamic updating role - access tables according to requests, to reduce the calculation time of global strategy of synthetic, and improve the efficiency of authorization. And the experiment showed that, this model has a better performance in certain conditions. Furthermore works will be done in two aspects: How to determine the appropriate trust weight suit for each role; and More types of conflicts should be tested.

Acknowledgement

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] Kapadia, Apu Chandrasen. “I-Rbac 2000: A Dynamic Role Translation Model for Secure Interoperability.” (2001). Available at https://www.researchgate.net/publication/23

61743_I-Rbac_2000_A_Dynamic_Role_Translation_Model_For_Secure_Interoperability
[2] Chen Xiangran, “Research on Key Technologies of Role-based Secure Interoperation in Multi-domain Environments”. For the Degree of Master of Military Science, 2010.
[3] Punithasurya, K, and P. S. Jeba. “Analysis of Different Access Control Mechanism in Cloud.” International Journal of Applied Information Systems 4.2(2012):34-39. Available at http://research.ijais.org/volume4/number2/ijais12-450660.pdf
[4] OpenStack API Complete Reference, http://developer.openstack.org/(last accessed December 12, 2016)
[5] Overview of Managing Access - Amazon Simple Storage Service. http://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-overview.html(last accessed December 12, 2016)
[6] 阿里云- 访问控制.https://help.aliyun.com/product/28625.html?spm=5176.doc28645.3.1.DKFz1e(last accessed December 12, 2016)
[7] Shafiq, Basit, et al. “Secure Interoperation in a Multidomain Environment Employing RBAC Policies.” IEEE Transactions on Knowledge & Data Engineering 17.11(2005):1557-1577. https://doi.org/10.1109/TKDE.2005.185
[8] Piromruen, S., and J. B. D. Joshi. “An RBAC framework for time constrained secure interoperation in multi-domain environments.” IEEE International Workshop on Object-Oriented Real-Time Dependable Systems IEEE Computer Society, 2005:36-48. https://doi.org/10.1109/WORDS.2005.18