# Resource and Role Based Access Control Model

Xingdong Li, Zhengping Jin

State Key Laboratory of Networking and Switching Technology

Beijing University of Posts and Telecommunications

Beijing, 100876, China

xingdongli0126@163.com, zhpjin@bupt.edu.cn

**Keywords:** Cloud Computing, Access control model, Resource and Role, self-adaptive.

**Abstract.** Cloud computing's multi-tenancy and virtualization features pose unique security and access control challenges due to resource sharing. Traditional access control models can't meet the needs of the open, network-connected, heterogeneous and highly distributed cloud computing environment. In this paper, we propose the resource and role based access control model (RRBAC), a flexible Resource and Role based Access Control model for the open and dynamic cloud environment. Different from previous work, our model is more extendable, flexible and adaptive due to the following improvements: 1)It is capable of automatically change the corresponding configurations in order to either prevent further misuse or grant further access. 2) User's authorization, role hierarchy and privilege hierarchy are modified to reduce the complexity. 3) Various access strategies are provided for different real-time environment. As a whole, RRBAC model is more extendable, flexible and adaptive. Our theoretical analysis results show that this model can effectively provide dynamic and secure access control.

## Introduction

Recently years, cloud computing has drawn extensive attention from both academia and industry. Cloud computing enable ubiquitous, convenient, on-demand network access to a share pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort. However, due to a great deal of collaboration and resource sharing in cloud computing, unique security becomes an important emerging requirement. Among all security requirements of cloud computing, access control, as one of the fundamental requirements, is concerned with the protection of computational resources and digital information against unauthorized access. And access control models provide methods to regulate users' actions and ensure that only authorized users are given privilege to access certain resources.

There are three main traditional access control models: first, Discretionary Access Control (DAC)[1] which is based on security labels attached to users and resources, but maintenance of the system and verification of security principles is extremely difficult for DAC systems because users control access rights to owned objects; second, Mandatory Access Control (MAC)[2] which is based on the permissions or denials information of each user, however, it is not without serious limitations. The assignment and enforcement of security levels by the system under the MAC model places restrictions on user actions that prevents dynamic alteration of the underlying policies, and requires large parts of the operating system and associated utilities to be "trusted"; thirdly, Role-Based Access Control (RBAC)[3] which is based on the user's role given by the administrator. But, in large systems, memberships, role inheritance, and the need for finer-grained customized privileges make administration potentially unwieldy. Additionally, while RBAC supports data abstraction through transactions, it cannot be used to ensure permissions on sequences of operations need to be controlled[4]. Therefore, these traditional access control models do not respond adequately to new challenges and requirements caused by the open, network-connected, heterogeneous and highly distributed cloud computing systems. In consideration of the new challenges and security requirements of the open and dynamic cloud environment.

 

In this paper, we proposed a flexible Resource and Role Based Access Control (RRBAC) model. Working from the traditional RBAC model, the proposed RRBAC model is more extendable, flexible and adaptive. First, RRBAC can automatically change the corresponding configurations in order to either prevent further misuse or grant further access. Moreover, user's authorization is designed as a three-association authorization and the related role hierarchy and privilege hierarchy are modified to reduce the complexity and help to the system implementation. In addition, various access strategies are provided in RRBAC for different real-time environment. More specifically, we apply self-adaptive techniques[5] in order to monitor, analyze, decide and manage a target authorization infrastructure.

The rest of this paper is organized as follows. Section 2 discusses the related work. We describe our proposed access control model in Section 3. Section 4 provides a practical example to illustrate the effectiveness and applicability of our model. Finally, we conclude with an evaluation of our proposal along with future work in Section 5.

**Related work**

Access control takes charge of the authentication, controls the ability of users to access securable resources and perform various system administration tasks. It's one of the security measures in multi-user shared resource environment. Some works have tried to build access control models for the cloud environment.

The Discretionary Access Control (DAC) model which restricts access to resources based on the identity of subjects a groups to which users belong. The control are discretionary in the sense that a subject with a certain access permission is capable of passing that permission on to any other subject. However, giving all control to the user or group over the files is too dangerous because if an attacker got the control over the account then the attacker will have complete authority on the access. Mandatory Access Control (MAC) refer to a type of access control by which the operating system constrains the ability of a subject to access or generally perform some sort of operation on an object. With MAC, the security policy is centrally controlled by a security policy administrator, and users do not have the ability to override or modify the policy. As the most restrictive access control method, MAC is useful in a highly secured environment and not suited in a fine-grained, persistent, continuous and flexible environment.

Role-Based Access Control (RBAC) models have gained a great interest in the security community, and figure out the localization and disadvantage of DAC and MAC. In RBAC model, a user owing a role assigned by an administrator can access the corresponding resources and perform specific tasks. However, the RBAC model is not dynamic or scalable because roles must be pre-constructed before using the model; and using RBAC to manage sufficient roles and assign adequate role memberships would become extremely complex in the highly distributed cloud computing system with a heterogeneous IT infrastructure and requirements that span dozens or hundreds of systems and applications. As a variant of RBAC, Attributes-Based Access Control (ABAC) model can change attributes dynamically and provide more fine-grained access control. However, as the dataset and the number of attributes grows larger in ABAC, the size of the policy strategy grows exponentially, which seriously reducing the software performance.

In distributed environment, the dynamic and random of users' behaviors make it more and more difficult to control the resources access and provide effective and adaptive security models. Obviously, traditional access control models do not respond adequately to new challenges and requirements caused by the cloud computing systems. Meanwhile, we note that in any system there is limited number of privileges for users to access resources, such as read, write, modify, and so on. The scale of the permission set (the set of privilege set)[6] is stable and not affected by the scale of roles or attributes[7]. Inspired by this, we propose an extended resource and role based access control (RRBAC) model to mend the imperfection of the famous RBAC model. Meanwhile, the proposed RRBAC model stays isolated from the problem in ABAC that the size of the policy strategy grows exponentially as the number of attributes grows.

## Resource and role based access control model

Traditional Role Based Access Control (RBAC) models and Attribute Based Access Control (ABAC) models are facilitating access to protected resources by defining and assigning permissions to the corresponding roles or attributes. Working from the traditional RBAC model, the Resource and Role Based Access Control (RRBAC) model is proposed in this paper for supporting open and distributed environments. The RRBAC model provides a self-adaptive framework which is flexible enough to be attached to any distributed and dynamic policy and the strategy employed is dynamic, robust, and highly scalable.

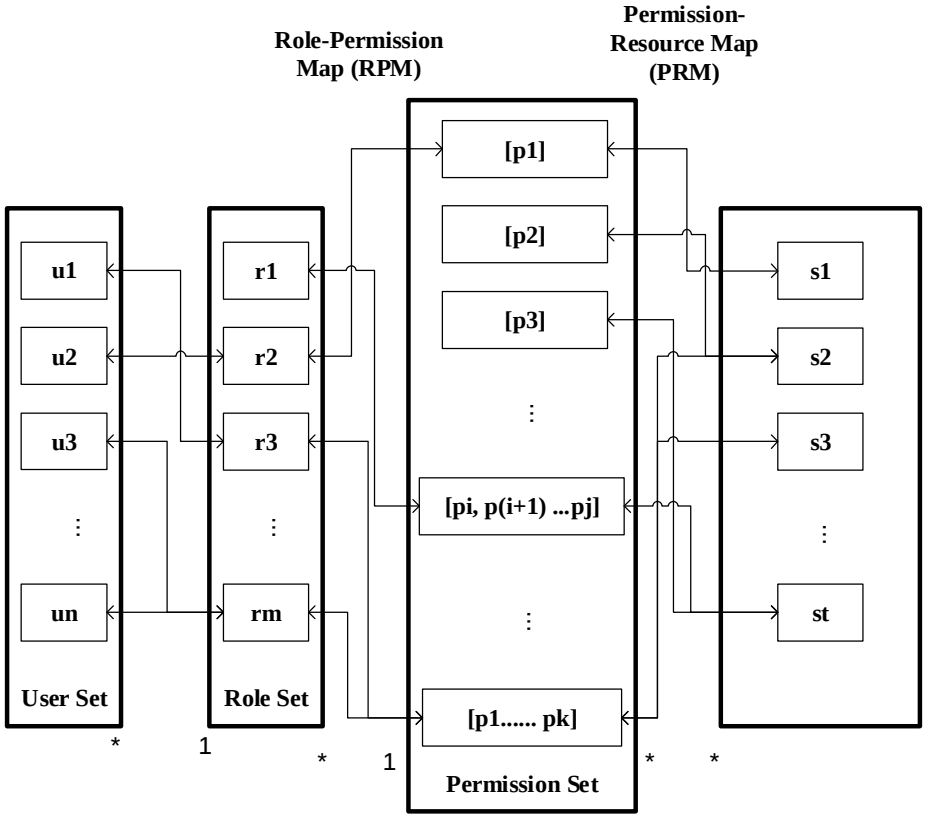


Fig. 1 the Framework of. RRBAC Model

As showed in Fig.1, the framework of RRBAC consists of four sets and two maps, and the related notations are defined as follows:

$\text{user}Set = \{u_1, u_2, ..., u_n\}$ is a set of authorized users where $u_i (1 \le i \le n)$ denotes a user and $n$ is the number of all authorized users.

$roleSet = \{r_1, r_2, ..., r_m\}$ is a set of roles defined according to the practical applications, where $r_i (1 \le i \le m)$ denotes a role and $m$ is the number of all roles.

$permissionSet = \{p_1, p_2, ..., p_k\}$ is a set of privilege sets, where $p_i (1 \le i \le k)$ denotes a privilege set and $k$ is the number of all privilege sets. For instance, in a file system, $p_i$ can be described as {read} or {access, read, write, modify, delete, upload, download}.

$sourceSet = \{s_1, s_2, ..., s_t\}$ is a set of resources which pass the registration, where $s_i (1 \le i \le t)$ denotes a resource and $t$ is the number of all resources.

Role-Permission Map (RPM) is defined for mapping a role to a certain privilege set. Similarily, Permission-Resource Map (PRM) is defined for mapping a resource to a certain privilege set.

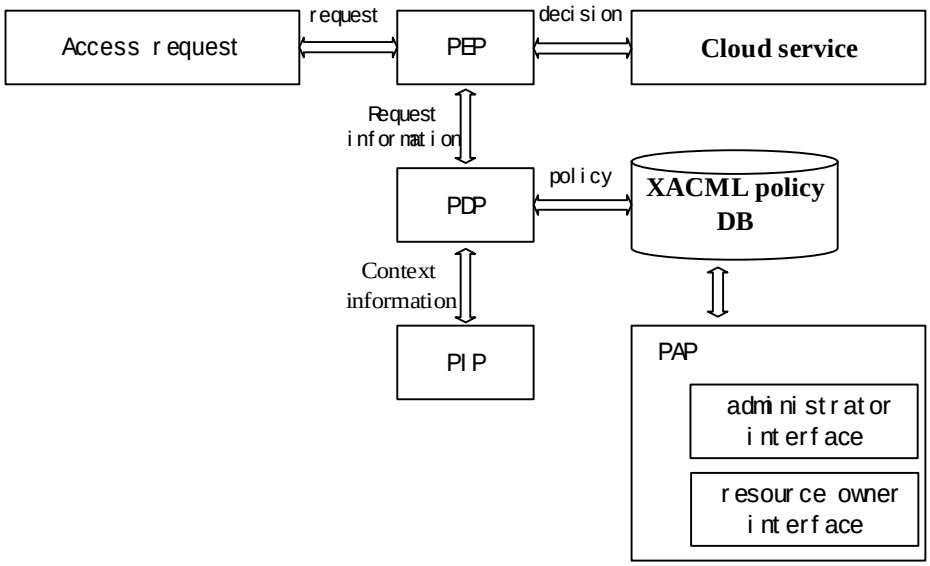


Fig. 2. Work Framework of RRBAC

As showed in Fig.2, the RRBAC model will be developed in the following five modules:

- **the policy decision point (PDP)** is in charge of making authorization decisions based on the RRBAC policies and current environmental conditions.
- **the policy enforcement point (PEP)** accepts a user's request, analyzes and gets the user's information, passes the request information to PDP, and interacts with the Cloud service module according to the decision result returned from PDP.
- **the policy administration point (PAP)** is in charge of policy development and management. It has two outward interfaces, one is for the system administrator to update the RPM and the other is for the resource provider to make a resource regulation, And then the PAP generates the access policy strategy according to certain rules and stores the policy, described by XACML language, into the XACML policy DB. Thus, the PAP provides standard data interfaces for the follow-up system expansion and escalation.
- **the policy information point (PIP)** gets entity environmental conditions and provides them to PDP for making decision.
- **Cloud service** is a set of system resources.

The basic process of RRBAC model is as follows: First, A user sends an access request to the cloud computing system for accessing to one service in the Cloud Service, where the request data is in a format prescribed by XACML. Then, the PEP module accepts the request, analyzes it and gets the user's information, such as user's role, the requested resources and so on. And then the PEP module transmits the request information to the PDP module. Once the PDP module accepts the request information, it sends a request for the access policy strategy to the XACML policy DB, which is generated by the PAP module. Meanwhile, it sends a request to the PIP module for the required context information, such as environmental conditions and resource conditions. Thus, the access control decisions are made based on the policy information and context information of environment, and then the decision result (accept or refuse) is returned to the PEP module. Finally, PEP module is in charge of interacting with the Cloud service module and execute the decision according to the result returned from PDP.

In consideration with the dynamic and distribute cloud environment, a good access control model should be self-adaptive, which means to provide systems with the ability to adapt, manage, repair and update themselves automatically at run-time[8]. For example, in real world, a normal company's opening time is usually fixed. However, the opening time of examination system is always changed. For satisfying the different requirements of various real-world conditions, the RRBAC is designed to be self-adaptive. In RRBAC, there are two table need to be maintained, i.e., RPM and PRM, which are used to define access control policy, authorization request and response messages. And the RPM and

PRM can be provided a maintained by the administrator account and the resource provider maintain, respectively. As part of the self-adaptive RRBAC, the administrator or resource provider can updates the policy model described by XACML in accordance to the required changes. Moreover, we received the RPM and PRM, and integrate them into access control list (ACL)[9], which is a method to restore the access control information. In RRBAC model, we design the format of ACL as follows: $acl = (role): (privilege\ set): (resource)$ where the first part is filled by the role name, such as teacher, student, and so on, and the second part is the operational privilege set, which specifies what actions the requestor can perform towards the resource, and the last part is the name of the requested resource.

The proposed Resource and Role Based Access Control (RRBAC) model is designed fully taking the condition of cloud environment into consideration. RRBAC improves a lot on the basis of traditional RBAC model. First, RRBAC can automatically change the corresponding configurations in order to either prevent further misuse or grant further access. Meanwhile, user's authorization is designed as a three-association authorization and the related role hierarchy and privilege hierarchy are modified. Moreover, various access strategies are provided in RRBAC for different real-time environment. And self-adaptive techniques are applied in order to monitor, analyze, decide and manage a target authorization infrastructure. As a consequence, the RRBAC model is more extendable, flexible, and adaptive.

## Pilot implementation

To illustrate the effectiveness of the proposed RRBAC model, we apply it in the examination system of a university, which is open, network-connected, heterogeneous, dynamic and real-time. The scenario is: an English test is being performed and junior students are allowed to access the examination system from 9:00 am to 11:00 am. The students are only allowed to read authorized documents and answer the questions but not allowed to modify the test paper. In 9:05 am, a student send a request to access the system, the PDP (Policy Decision Point) received the request and make decision whether accept or reject this request according the policy strategy in this system. In addition, visiting students from other university or grade are rejected and those who request before 9:00 am or after 11:00 am in the test day also not be allowed.

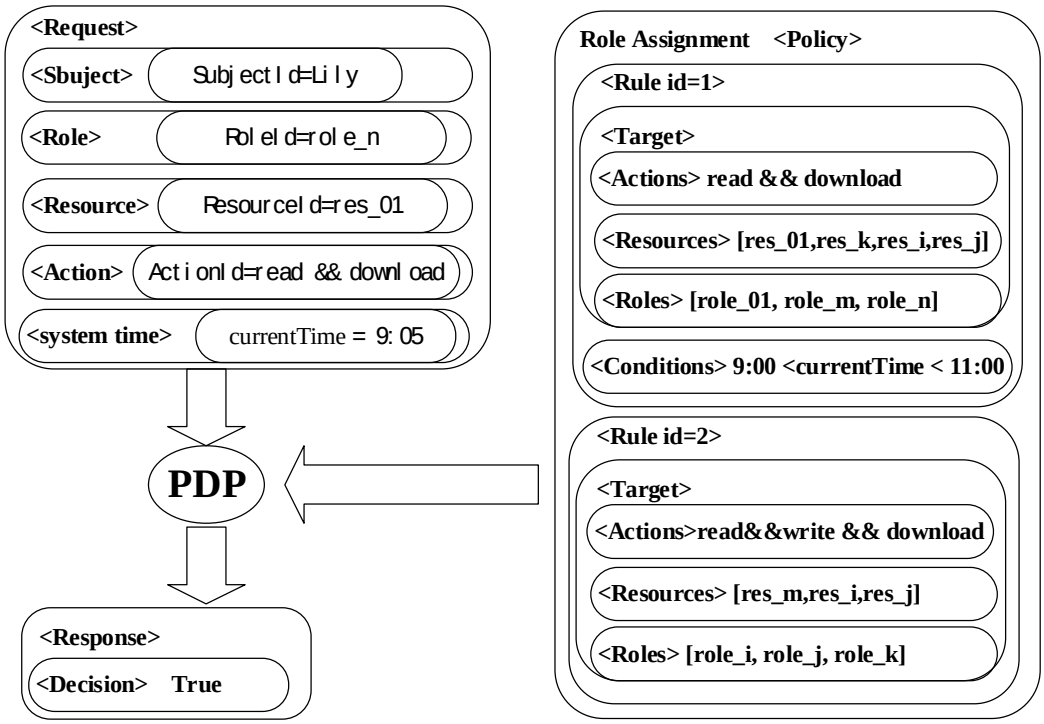


Fig. 3. the Proposed XACML Profile in RRBAC

Fig.3 gives a example of the proposed XACML Profile in the RRBAC model. In this example, RRBAC model works as follows: first, the PDP module gets and analyzed the request information. Obviously, the request permissions set is [read, download], the role is $r_n$, and the resource of the request is $s_1$. Then the PDP get the system's policy strategy from the database and find out the rule which permission set is [read, download]. And then the PDP checks in sequence if the role (i.e , $r_n$) can be found in the role set of the rule and the resource (i.e., $s_1$) can be found in the resource set [$s_1$, $s_k$, $s_i$, $s_j$]. When, and only when the check result is true, the user's request can be satisfied. And the policy strategy XACML used in the decision-making process is as showed in Fig.4. In order to cope with the condition that the strategy of a system's access control changes frequently, we designed two interfaces for the resource provider and the administrator to update the policy XACML, and the RRBAC model will analysis the sub-strategy and then these update activities can be combined into the latest access policy strategy used for the RRBAC model, result in high flexibility.

The case above illustrates the effectiveness of the proposed RRBAC model for the real-time environment. And it is clearly that the RRBAC model is more extendable, flexible, and adaptive based on mass improvements in configurations self-adaption, user's authorization adjustment, the related role hierarchy and privilege hierarchy, various access strategies provision and self-adaptive techniques application.

## Conclusion

The main contribution of this paper is to propose a flexible Resource and Role Based Access Control (RRBAC) model for the open and dynamic cloud environment. Working from the traditional RBAC model, the proposed RRBAC model is more extendable, flexible and adaptive, and stays isolated from the problem in the ABAC model that the size of the policy strategy grows exponentially as the number of attributes grows. More specifically, the RRBAC model can automatically change the corresponding configurations in order to either prevent further misuse or grant further access. Meanwhile, user's authorization is designed as a three-association authorization and the related role hierarchy and privilege hierarchy are modified to reduce the complexity and help to the system implementation. Moreover, various access strategies are provided in RRBAC for different real-time environment. In addition, we apply self-adaptive techniques in order to monitor, analyze, decide and manage a target authorization infrastructure. As a consequence, the RRBAC model provides a self-adaptive framework which is flexible enough to be attached to any distributed and dynamic policy and the strategy employed is dynamic, robust and highly scalable.

There are a few directions we would like to work on in the future. For instance, we could analyze the tradeoffs between roles and resources to obtain practically useful insights and results. Another work we want to do is to extend the policy strategy for leveraging the power of XACML.

## Acknowledgements

This work is supported by NSFC (Grant Nos. 61300181, 61502044), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

## References

[1] D. D. Downs, J. R. Rub, K. C. Kung, and C. S. Jordan, Issues in discretionary access control, Security and Privacy, 1985 IEEE Symposium on. pp. 208-208, 1985.

[2] D. Gros, M. Blanc, J. Briffaut, and C. Toinard, Advanced MAC in HPC systems: performance improvement, Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on. pp. 699-702, 2012.

[3] W. Li, H. Wan, X. Ren, and S. Li, A refined RBAC model for cloud computing, Computer and Information Science (ICIS), 2012 IEEE/ACIS 11th International Conference on. pp. 43-48, 2012.

[4] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, Role-based access control models, Computer, no. 2, pp. 38-47, 1996.

[5] C. Bailey, D. W. Chadwick, and R. De Lemos, Self-adaptive authorization framework for policy based RBAC/ABAC models, Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. pp. 37-44, 2011.

[6] E. T. Ueda, and W. V. Ruggiero, A Systematic Mapping on the Role-Permission Relationship in Role Based Access Control Models, Latin America Transactions, IEEE (Revista IEEE America Latina), vol. 10, no. 1, pp. 1243-1250, 2012.

[7] R. Abdunabi, M. Al-Lail, I. Ray, and R. B. France, Specification, validation, and enforcement of a generalized spatio-temporal role-based access control model, Systems Journal, IEEE, vol. 7, no. 3, pp. 501-515, 2013.

[8] G. Hains, Efficient static checking of dynamic access control in shared multiprocessor environments, Collaborative Technologies and Systems, 2007. CTS 2007. International Symposium on. pp. 33-36, 2007.

[9] W. Jinfei, and L. Hai, The access control research of management information system, Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on. pp. 190-192, 2010.