ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 470-475
doi: 10.18178/wcse.2017.06.081

Access Control Mechanism Based on Role, Attribute and Trust in Multi-tenant Cloud Environment

Cong Wang [1 +], Ronghua Li [2] and Yijie Shi [3 +]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[2] China Mobile Communications Corporation, Beijing, 100032, China.

[3] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

Abstract. In the light of the problem that current access control schemes in multi-tenant cloud envioronment are difficult to adapt to different tenants' requirements of fine-grained division of permissions and can't solve the trust problem among tenants when the user access another tenant's resource. In this paper, we propose an access control mechanism suitable for multi-tenant cloud environment, which combines RBAC, ABAC and trust model. The access control mechanism based on role, attribute and trust meets the needs of cross-tenant access and fine-grained division of permissions. It is easy to check user's permission and solves trust problem between tenants when users access across tenants, improving the security of tenant's data and reducing the complexity of implementation. It is a more fine-grained access control scheme suitable for dynamic cloud environment.

Keywords: Multi-tenant Cloud Environment; Fine-grained Access Control; RBAC; ABAC; Trust Problem.

1. Introduction

With further application of cloud computing, cloud platform data privacy protection has become the focus of the industry and primary consideration for the user to choose a cloud service[1],[2], and access control is an important link of cloud platform privacy protection [3],[4].

In the existing RBAC scheme in multi-tenant cloud environment [5],[6], if we need a fine-grained division of permissions, users must be accurately distinguished, which needs to define a variety of roles[7],[8]. However, it is difficult to solve management and distribution difficulties caused by massive roles, so it's difficult to adapt to different tenants' requirements of fine-grained division of permissions . In addition, RBAC lacks the flexibility to adapt to dynamically changing user, resource, environment and security policies in dynamic multi-tenant cloud environment [9]. The existing access control scheme in multi-tenant cloud environment [10], which is based on RBAC and ABAC, is essentially ABAC with complexity. It is difficult to analyze and change users' permissions. What's more, it does not consider how to isolate tenants effectively, access across tenants, and cooperate between tenants; The existing access control scheme applied in industrial control system [11]and other scenes [12,13,14], which is based on RBAC and ABAC, does not take the problem of cross-tenant access into account. Therefore, it isn't suitable for multi-tenant cloud environment; In the existing role-based trust model, it isn't related to attribute [15],[16], and can not solve the trust problem among tenants when the user access another tenant's resource [8]. So it isn't suitable for multi-tenant cloud environment, either.

+ Corresponding author.
E-mail address: wangcongcherish@gmail.com; yijieshi2000@bupt.edu.cn.

In this paper, we combines RBAC, ABAC and trust model, and apply it in multi-tenant cloud environment. The first chapter introduces the research background and second the related basic knowledge, the third chapter elaborates the proposed access control scheme based on role, attribute and trust in multi-tenant cloud environment. The fourth chapter describes the implementation process of proposed scheme, the fifth chapter summarizes this paper.

2. Basic Knowledge

2.1. Role-based access control（RBAC）

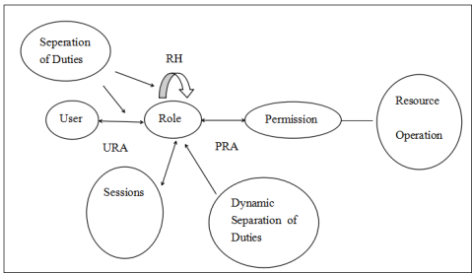

Fig. 1: NISTRBAC reference model

In 2001, the National Institute of Standards and Technology (NIST) proposed the standard RBAC reference model [6], NISTRBAC, as shown above. It is divided into three sub models: Basic RBAC, Level RBAC and Constrained RBAC. It consists of five basic elements: Users, Roles, Sessions, Objects, Operations, Role Permission Assignment(RPA),User Role Assignment(URA). The basic idea is to establish the many-to-many relationships between users and permissions through the roles, so that users obtain the permissions to the resources [17,18,19].

2.2. Attribute-based access control（ABAC）

The basic idea of ABAC is to decide whether to conduct authorization according to whether entities' attributes meet the requirements. It is a kind of dynamic access control mechanism, which does not define authorization policy directly between subject and resource, but according to attributes [4].

2.3. Trust model [8],[20],[21]

Assuming that $X=\{x_1,x_2,\cdots x_n\}$ is the collection of n feedbacks of the transactions, and has r positive feedbacks and s negative feedbacks. Now set a possible feedback for the next transaction to x_{i+1}, then the possibility that x_{i+1} is positive is as follows:

$$\varepsilon(r,s)=\frac{r+\alpha}{r+\alpha+s+\beta} \tag{1}$$

Most Bayesian trust uses the assumed parameters $\alpha=\beta=1$.

2.4. Symbol specification

Symbol	Meaning	Symbol	Meaning	Symbol	Meaning
R	Role	**URA**	User Role Assignment	**SA**	Subject Attribute
A	Attribute	**RPA**	Role Permission Assignment	**PA**	Permission Attribute
T	Trust	**RBAC**	Role-Based Access Control	**EA**	Environment Attribute
U	User	**ABAC**	Attribute-Based Access Control	**TR**	Trust Relation
Te	Tenant	**DO**	Data Owner	**RH**	Role Hierarchy

3. Access Control Mechanism Based on Role, Attribute and Trust in Multi-tenant Cloud Environment

In this paper, we propose a fine-grained access control mechanism suitable for cloud environment, which combines R, A and T. The combination of R and A refers that based on RBAC, we use A as dynamic factors to judge whether to conduct URA and RPA, where A includes:

Symbol	Meaning
SA	user's attributes, namely the user's ID, Password ,Token etc. returned to the user after registration according to their ID number, mailbox, contact, gender, occupation, degree etc. .
PA	include operating attributes(read, write, update and delete etc.) and resource attributes(type and secret level of data owner's resource).
EA	the time of request, length of access time, address (IP), etc..

The combination of R, A and T refers that by introducing a trust model based on R and A to improve the security of tenant's data and determine whether to conduct URA and RPA. In a word, our scheme combines RBAC, ABAC and trust model, which is suitable for dynamic cloud environment and easy to review user's permissions. Therefore, it is a more fine-grained access control scheme.

There are four entities in multi-tenant cloud environment, including:

Entity Name	Definition
Tenant	The entity who hires cloud services, the provider can provide services for multiple tenants, and the tenant use cloud platform to carry out business.
User	An entity that accesses the busimess in the cloud service hosted by a tenant, the tenant's business can be accessed by multiple users.
Role	A user's identity or job function in a tenant, each tenant can have multiple roles, but each role can only belong to a tenant.
Data Owner	A tenant who has the ownership of accessed data.

Access control scheme controls user's access according to corresponding strategies, preventing data leakage caused by illegal access to data owner's resources: Grant access permission to trusted users; deny access by non-trusted users. In multi-tenant cloud environment, the access control mechanism based on R,A and T is to judge the trust relationship among the four entities according to certain rules. There are three kinds of trust relationship, and the rules are as follows:

1. TR1: The trust of roles to users, refers that R determines whether to conduct URA according to U's trust value. R computes it according to three aspects, respectively: Trust based on attrubutes T_1,Trust based on user's behavior T_2, Trust based on user's reputation T_3.

When the user requests to join a role, the role needs to determine whether SA and corresponding EA meet the requirements firstly, if not, $T_1 = 0$,and then the user's request to join the role is denied, Otherwise, $T_1 = 1$, At this point, the role also needs to compute T_2 and T_3 separately according to the interaction history between the user and the role, between the user and other roles by (1). If the weights of T_2 and T_3 are assigned to $w_2, w_3, w_2 + w_3 = 1$, then the user's trust value $T = w_2 T_2 + w_3 T_3$. If T is greater than or equal to the trust threshold, output 1, accept the request of the user to join the role. Otherwise, output 0, and the user's request is denied.

2. TR2: The trust of DO to R, refers that DO determines whether to conduct RPA according to R's trust value. DO computes it according to four aspects, respectively: Trust based on attrubutes $T_1^{'}$, Trust based on the role $T_2^{'}$, Trust based on role's reputation $T_3^{'}$ and Trust based on RH $T_4^{'}$.

When a role asks DO to have a permission, DO needs to determine whether PA and corresponding EA meet the requirements firstly, if not, $T_1^{'} = 0$, and the role's request is denied. Otherwise, $T_1^{'} = 1$. At this point, DO needs to compute $T_2^{'}$, $T_3^{'}$ and $T_4^{'}$ according to interaction history between DO and R,R and other tenants, interaction history of the role's descendant roles by (1). If their weights are assigned to $w_2^{'}, w_3^{'}, w_4^{'}, w_2^{'} + w_3^{'} + w_4^{'} = 1$, then $T = w_2^{'} T_2^{'} + w_3^{'} T_3^{'} + w_4^{'} T_4^{'}$. If T is greater than or equal to the threshold, output 1, accept the role's request. Otherwise, output 0, the role's request is denied.

3. TR3: The trust between tenants, refers that in multi-tenant cloud environment, if users in tenant A want to access tenant B's resources, B decide whether to assign permissions according to the user's trust value. There are three ways to access cross tenants:

- Way 1: The user in A who wants to access B's resource requests to join corresponding role of B.
- Way 2: The role in A requests to become corresponding role in B, then all users of the role in A can access corresponding resources of role in B.
- Way 3: the role in A requests to become the ancestral role of one or a few roles, then all users of the role in A can access corresponding resources of role in B.

In the first way, corresponding role in B needs to determine whether the user that issued the request is credible, the problem is turned into a expansion of TR1 in multi-tenant environment. In the second and third way, B (DO) needs to determine whether the role in A that issued the request is credible, extending the problem into TR2 in multi-tenant environment. Therefore, the trust relationship between tenants can be classified as TR1 and TR2, which ultimately determines whether to conduct URA and RPA.

In this paper, according to the above trust relationship, we propose an access control mechanism in multi-tenant cloud environment based on role, attribute and trust, which combines RBAC, ABAC and trust model. During URA and RPA process, we use attributes as dynamic factors, and decide whether to assign permissions according to the trust value. This scheme is suitable for dynamic cloud environment, and it is a more fine-grained access control scheme.

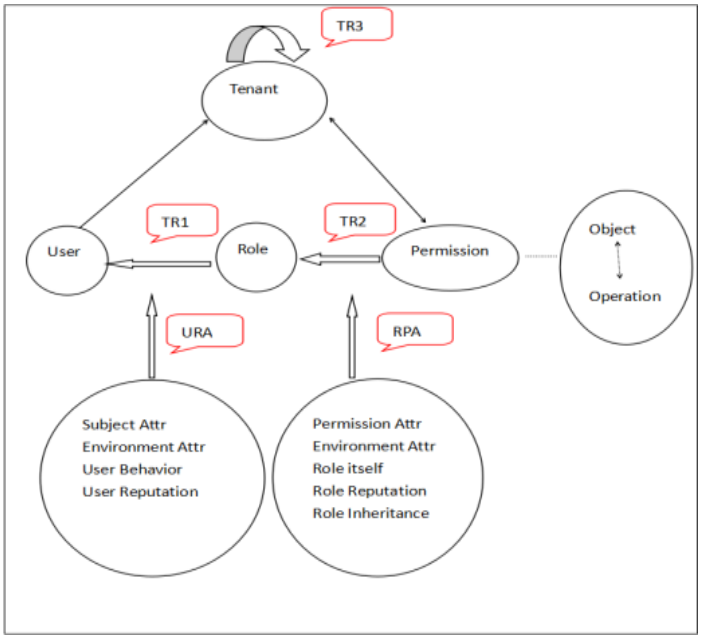

Fig. 2: Access control mechanism based on r, a and t in multi-tenant cloud environment

4. Implementation Process of Proposed Access Control Mechanism

In multi-tenant cloud environment, according to above mentioned, there are three ways to access across tenants. The specific implementation process of proposed access control scheme are as follows:

4.1. Access control process of way 1

1. U sends a request for specific operation on specific resource to the tenant A;

2. Determine whether SA and corresponding EA meet R's requirements, if not, refuse the user's request. Otherwise, go to next step;

3. Compute U's trust value according to SA,EA, user's behavior and user's reputation.

4. Compare it with the pre-set threshold. If it is less than the threshold, the user's request is denied. otherwise, assign the role to the user, and go to the next step;

5. A determines whether PA that the user requested meet the requirements according to U's role and corresponding EA. If not, U's access request is denied. Otherwise, go to the next step;

6. Compute R's trust value according to PA, EA, the role itself and role reputation;

7. Compare it with the pre-set threshold. If it is less than the threshold , the user's access request is denied. Otherwise, grant permission to the role.

4.2. Access control process of way 2 and 3

1. The user in tenant A sends a request for specific operation on specific resource to tenant B;

2. According to the URA process of way 1 to determine whether U has the role of A;

3. According to the user's role in A and corresponding EA, B judges whether PA that user requested meet requirements. If not, refuse the user's request. Otherwise, go to next step;

4. Compute the trust value of B to user's role in A, according to EA, PA, the role itself, role's reputation and RH.

5. Compare it with the pre-set threshold. If it is less than the threshold, the user's access request is denied. otherwise, the role in A can become corresponding role in B or its ancestor role, then the user joins the role of B, and go to the next step;

6. B determine whether PA that the user requests meet the requirements, according to user's role in B and corresponding EA. If not, the user's access request is denied. Otherwise, go to next step;

7. Compute the trust value of the tenant B to user's role in B, according to PA, EA, the role itself, the role's reputation, and RH;

8. Compare it with pre-set threshold. If it's less than the threshold, the user's access request is denied. Otherwise, grant the permission to the role, that is, the user in A can access tenant B's resources.

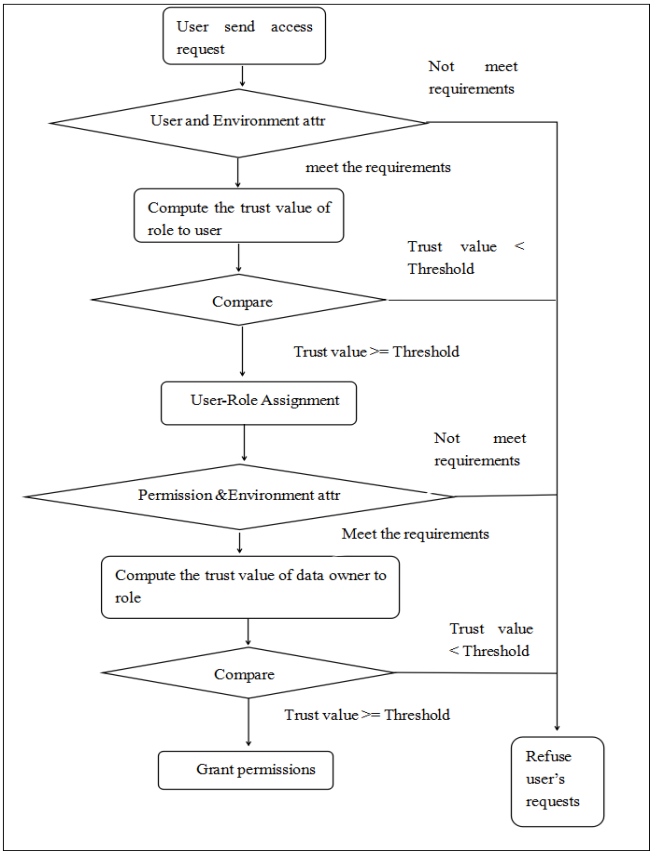

Fig. 3: Access control process of way 1

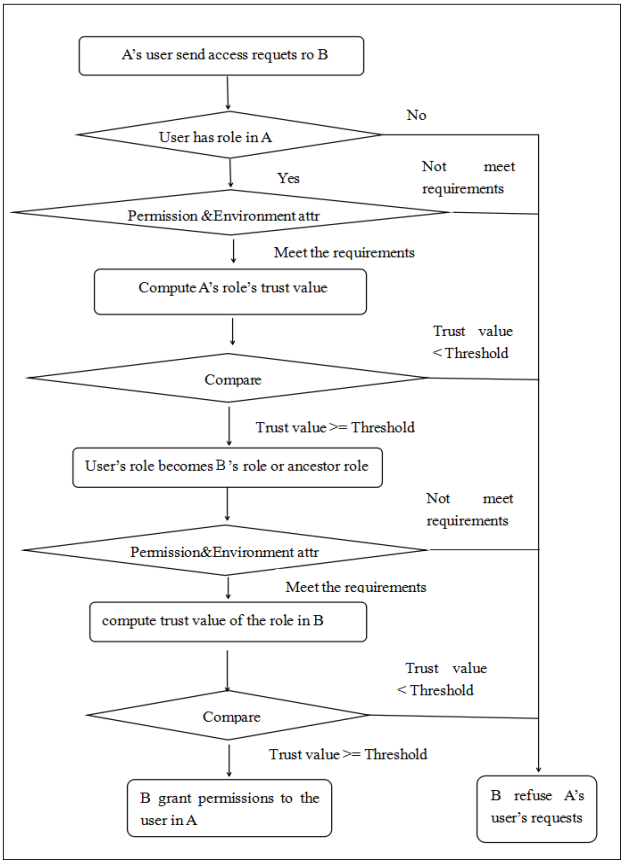

Fig. 4: Access control process of way 2 and 3

5. Conclusion

In this paper, we proposed an access control mechanism suitable for multi-tenant cloud environment, which combines RBAC,ABAC and trust model. The scheme has the advantages of both RBAC and ABAC, which is flexible and easy to review user's permissions, meets the needs of cross-tenant access and fine-grained division of permissions, reducing the complexity of implementation and ensuring security of tenant's data.; And by introducing the trust model based on role and attribute, we resolved the problem that when attributes meet the requirements but users' or roles' credibility is low, URA and RPA will reduce security of tenant's data, and resolved trust problem between tenants when users access across tenants, improving the

security of tenant's data. It is a more fine-grained access control scheme. Our future work is to further improve the computing method of the trust value in the proposed scheme.

6. References

[1] Ching Nung Yang, Jia-Bin Lai. Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing. 2013 International Symposium on Biometrics and Security Technologies:259-266.

[2] Deyan Chen, Hong Zhao.Data Security and Privacy Protection Issues in Cloud Computing .2012 International Conference on Computer Science and Electronics Engineering, 2012:647-651.

[3] Joseph K.Liu, Man Ho Au,Xinyi Huang and Rongxing Lu. Fine-Grained Two Factor Access Control for Web-Based Cloud Computing Services.IEEE Transactions on Information Forensics and Security,2016,11(3):484-497.

[4] S.Yu,C.Wang, K.Ren,and W.Lou. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. proceedings of IEEE, 2010.

[5] Mohamed Amine Madani, Mohammed Erradi, Yahya Benkaouz. Access Control in a Collaborative Session in Multi Tenant Environment. 2015 11th International Conference on Information Assurance and Security,2015.

[6] B.Tang and R. Sandhu. A Multi-Tenant RBAC Model for Collaborative Cloud Services. Eleventh Annual Conference on Privacy, Security and Trust, 2013:229-238.

[7] Lan Zhou, Vijay Varadharajan, Michael Hitchens .Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage .IEEE Transactions on Information Forensics and Security, 2013(12) :1947-1958.

[8] Lan Zhou,Vijay Varadharajan and Michael Hitchens. Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage. IEEE Transactions on Information Forensics and Security,2015(10):2381-2395.

[9] D.Richard Kuhn,Edward J. Adding Attributes to Role-Based Access Control. IEEE Computer,2010(6):79-81.

[10] Nai Wei Lo,Ta Chih Yang and Ming Huang Guo. An Attribute-Role Based Access Control Mechanism for Multi-tenancy Cloud Environment. Wireless Pers Commun,2015(84):2119-2134.

[11] Jingwei Huang,David M,Nicol,Rokesh Bobba and Jun Ho Huh. A Framework Integrating Attribute-based Policies into Role-Based Access Control. Proceedings of the 17th ACM Symposium on Access Control Models and Technologies,2012:187-196.

[12] The Privacy-Aware Access Control System Using Attribute and Role-Based Access Control in Private Cloud. Proceedings of IEEE,2011:447-451.

[13] Alshaimma Abo-alian,Nagwa L.Badr and M.F.Tolba. Hierachical Attribute-Role Based Access Control for Cloud Comput ing. Advances in Intelligent Systems and Computing,2015:381-389.

[14] Vijay Varadharajan,Alon Amid and Sudhanshu Rai. Policy Based Role Centric Attribute Based Access Control Model. International Conference on Computing and Network Communications,2015,12:427-432.

[15] R.K. Banyal,V.K. Jain, Pragya Jain. Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment. Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies,2014.

[16] Tang B,Sandhu R. Cross Tenant trust models in cloud computing. Proceedings of 14th IEEE Conference on Information Reuse and Integration(IRI),2013:129-136.

[17] DAVID F, Sandhu R and Richard D. Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001: Pages 224–274.

[18] David F. Ferraiolo and D. Richard Kuhn.Role-Based Access Controls .15th National Computer Security Conference,1992:554 - 563.

[19] Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink and Charles E. Youmank. Role-Based Access Control Model. IEEE Computer, 1996(2): 38-47.

[20] Lik Mui,Mojdeh Mohtashemi, Ari Halberstadt. A Computational Model of Trust and Reputation for E-businesses. Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.

[21] Audun Josang . The Beta Reputation System. 15th Bled Electronic Commerce Conference eReality: Constructing the eEconomy Bled, 2002: 324-337.