Chapter 95
A Survey of Extended Role-Based Access Control in Cloud Computing

Hongjiao Li, Shan Wang, Xiuxia Tian, Weimin Wei, and Chaochao Sun

Abstract Access control is one of the key mechanisms for cloud computing security. When it comes to being used in cloud computing environments, RBAC is more scalable and more suitable compared with traditional discretionary and mandatory access control models. A straightforward way is to extend RBAC from traditional fields to cloud computing environments. In this chapter, several extended role-based access control schemes are surveyed from basic extension, A-RBAC, and trust-based RBAC separately. Core techniques of the proposed schemes are detailed. Comparisons around the proposed schemes are analyzed.

Keywords Cloud computing • Access control • RBAC • A-RBAC • Trust

95.1 Introduction

Nowadays, cloud computing is becoming one of the most popular and trendy computing model in the technology world. In cloud computing model, access is performed through network which has the characteristics of ubiquity, convenience, and service-on-demand. The computing resource is a configurable shared pool consisting of networks, servers, storage, applications, and services [1]. There are different slots or sections of a cloud service. Among them, infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) are the three service models. With the cloud computing having more and more deployment, security issues have become important factors restricting its development and application [2].

Access control is the process of limiting access to system resources for only authorized people, programs, processes, or other system components, which plays an important role in the field of information security. Traditionally, there are three kinds of access control models: (1) discretionary, (2) mandatory, and (3) role based [3]. Among the three models, RBAC model is the most scalable, especially in such cases that tracking the users of the services cannot get through a fixed identity.

H. Li (✉) • S. Wang • X. Tian • W. Wei • C. Sun
School of Computer, University of Shanghai Electric Power, 200090 Shanghai, China
e-mail: hjli@shiep.edu.cn

W.E. Wong (ed.), *Proceedings of the 4th International Conference on Computer Engineering and Networks*, Lecture Notes in Electrical Engineering 355,
DOI 10.1007/978-3-319-11104-9_95

Accordingly, when used in cloud computing environments, RBAC models have the superiority.

In this chapter, from the view of the underlying techniques, we survey several extended RBAC schemes for cloud computing. In Sect. 95.2, basic techniques for using RBAC are analyzed. In Sect. 95.3, the core techniques of the proposed schemes and its application in cloud computing are detailed. In Sect. 95.4, we compare the schemes from attaining goals, and technique aspects and future works are listed. And in section Conclusion our conclusions are given.

95.2 Requirement of Using RBAC for Cloud Computing

In RBAC [4–6], the burden of the server is limited by restricting users from accessing the contents out of their zone. RBAC model is formalized by using the following notations: **U**, **R**, **OBS**, **OPS**, and **S**. In turn, they denote user set, role set, protected objects, operations set, and sessions set, respectively. To employ the RBAC model, identifying corresponding entities is the first task. In the SPI model, the identification among the three services (SaaS, PaaS, and IaaS) needs to be separated because each of them has different nature and scope.

Users/agents In SaaS, users can be individual persons, enterprises, or corporations and those web services wishing to access resources. All users identified in SaaS could be included in PaaS. In most cases, the acknowledgment from a virtual machine is received by an IaaS user, who is responsible for fulfilling the system configuration.

The categorization of **Roles** lies in their job functions. In cloud computing, roles can be consumers, tenants, and service providers. The permissions and functions of roles could inherit from a parent role so that the inheritance characteristic of RBAC can embody it.

The definition of **Permissions** is in accordance with the job functions of roles. To perform secure access in cloud computing, permissions are defined on data access, program access, and service access. Disabled and enabled permissions are done through the use of sessions.

From the view of object, resources with the cloud are **protected objects**. Objects, data, programs, and services are representative groups, corresponding to the permissions mentioned earlier. The granularity of the permission definition is consistent with the identification of project objects.

95.3 Extended RBAC Schemes in Cloud Computing

According to the basic components of RBAC model, several extended RBAC models have been proposed from different angles to accommodate to cloud computing environments.

95.3.1 Basic RBAC Extension

95.3.1.1 RBAC Extension Based on PKI and Domain Information

dRBAC (distributed role-based access control) [7] extends standard RBAC by using PKI and domain information in the certificate. If certificates for internal users (role and user in the same domain) and other companies' users (role and user in other domains) are to be authenticated and assigned permissions, the certificate is used to sign and issue. Conditions are written as attributes.

coRBAC (cloud optimized RBAC) [8] model is proposed which aims to achieve services optimization and enhancement of the access control system. Based on coRBAC, the certification process of multilevel cache of establishing secure connection is simplified, and multilevel cache is set up, which greatly improves the user's experience and performance of the access control system. coRBAC extends the dRBACs from two aspects: combing authentication services from different ends and expanding the CAs. Further, the added hierarchical caches make the **coRBAC** more efficient.

95.3.1.2 RBAC Extension Using Restriction Policy

The new advance E-RBAC (efficient RBAC) [9] presents a new extended architecture of RBAC which can resolve the security issues and data loss issues by using restriction policy on the number of roles, users per role, and transaction per day/hour/user. With the help of this new architecture, security level can be enhanced or improved. Another new feature and backup policy helps to reduce the data loss. It means that security level can be enhanced or improved with the help of this new architecture. One new feature is added into this architecture, and that is the backup policy which helps to reduce the data loss. But still there is a point of number of transaction by one ID of one specific role which could be the loop hole of this architecture.

95.3.1.3 RBAC Extension Using Role Ontology

Extended O-RBAC [10] is an extension using role ontology to extend RBAC for multi-tenancy architecture in clouds. For a specific domain, the role hierarchy is built up using ontology. This helps to increase the security by restricting the number of users per role, transaction per user. If the cloud crashes or does not work properly, there is also a concept of backup and restoration to avoid the loss of important data. In this case chances of loss of data are very few. This strategy enhances the security by adding the restraint policy, backup policy, and restore policy.

This extended O-RBAC uses reference ontology to enhance the security and simplify the system design and implementation which is an enhancement in policies in architecture of RBAC. Later, the development of a new back-end database schema for RBAC extension should be taken into account. Another aspect, the scalability of extended RBAC using reference ontology is to be measured.

95.3.1.4 RBAC Incorporating Dynamic Character

In task role-based access control model (task-RBAC) [11], the validation of user access permissions is dynamic because of the assigned roles and its associated task to be performed, which makes it viable for cloud computing environment. TRBAC [12] is a standard RBAC with temporal extension. During running, the role can be enabled and disabled against user requests. It is argued that static roles should always be enabled under some situations, while the assignment of users and permissions is dynamic [12]. The salient feature of this model is that the roles enabled are periodic. But several other important temporal constraints can't be dealt with. Subsequently, James et al. proposed GTRBAC [13]. In this model, the avocation is not role activation but role enabling. In GTRBAC, the constraints can be enabled and disabled. The upper limit of user active duration is within a particular time interval. Also, the number of role activations by a single user is limited. Unfortunately, the problem of trust relation in multi-domains cannot be solved by the model. X-RBAC [14] is a framework which deals with XML-based RBAC policy specification, and it is used to access control enforcement on dynamic XML-based web services. However, trust and context-aware access control is not attained. To solve the above problems, X-GTRBAC [6] is proposed. It combines the X-RBAC with GTRBAC models and the assignment of roles to users is performed by trusted third parties (e.g., any PKI certification authority). The users' trust level (as part of *user profile*) is affected by context information (such as time, location, or environmental state at the time the access requests are made), and it is part of its access control decisions. The users'/roles' access privileges have something to do with the threshold (i.e., the trust level), which is determined by the requestor's access patterns. X-GTRBAC can suit the above real-time requirement.

95.3.2 Attribute Role-Based Access Control

95.3.2.1 Role-Based Encryption

RBE [15] is a new encryption scheme which solves the encrypted data storage in public cloud with an efficient user revocation. In RBE scheme, the encryption is role based. That is, the data encrypted by data owner can only be decrypt and viewed by the users with appropriate roles specified by A-RBAC policy. The role grants permissions to users who qualify the role. Also, the permissions from existing users of the role can be revoked. Role hierarchies can also be coped with by RBE scheme, that is, one role can inherit another role's permissions. If a user joins a role in which its owner has encrypted the data for, after that, the user can access that data and data re-encryption can be omitted. Whenever a user is evoked, it can no longer access any future encrypted data representing the role. That is, the revocation of the user from its role has nothing to do with other users and roles in the system. By using this approach, the RBE scheme achieves an efficient decryption on the client side. RBE scheme is described by broadcast encryption algorithm.

95.3.2.2 Cloud Infrastructure Based on RBE

Based on the proposed RBE scheme, a secure cloud data storage architecture using a hybrid cloud infrastructure is developed [16], which is illustrated in Fig. 95.1. According to this architecture, the users who wish to access the encrypted data and the data owners who wish to encrypt their data only interact with the public cloud. The role hierarchy and user to role mappings related to the organization are maintained in the private cloud which is only accessible to the administrator of the organization. The administrator specifies the role hierarchy and the role managers who manage the user membership relations.

95.3.2.3 Applying A-RBAC in Cloud Computing

The RBE scheme can achieve efficient user revocation. In the RBE-based cloud storage architecture, an organization is allowed to store data securely in a public cloud, while the sensitive information related to the organization's structure is maintained in a private cloud. The characteristics of constant size ciphertext and decryption key are embodied in the proposed architecture. Also, both encryption and decryption computations are efficient on the client side, and decryption time at the cloud can be reduced by having multiple processors. Accordingly, the proposed system has the potential to be useful in commercial situations.

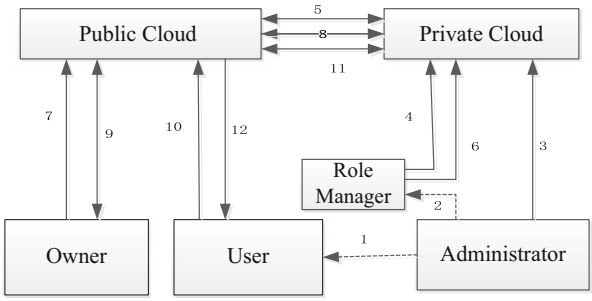

Fig. 95.1 RBE system architecture

95.3.3 Trust-Based RBAC

According to the concepts of trust in social sciences [17, 18], the description of trust in [19] is a mental state. It comprises three aspects: *expectancy*, *belief*, and *willingness to take risk*. In cloud computing environment, the semantics of trust is the same as above; but for cloud entities, the expectancy and the characteristics of cloud entities are still needed to meet competency, integrity, and goodwill.

95.3.3.1 TBDAC Model

TBDAC model [20] is the extension for RBAC. Based on GTRBAC, dynamic access authorization is done by introducing authorization trust factor; in this way, the users' trust-degree and the conditions about constraints can be determined. Accordingly, the information about role and the trust-degree are used to validate the users' legal identities. Also, the privileges for resource access control can be acquired. In TBDAC, a new ticket is proposed to satisfy the dynamic and real-time characters based on a modified Kerberos protocol. The certificate trust-degree is decided by direct trust-degree (**DT**) and recommendation trust-degree (**RT**). To calculate trust-degree, confidence factor (**CF**) and time factor (**TF**) are introduced.

Security theoretic analysis shows that when exchanging information using TBDAC model, security-hidden trouble can be reduced, and the security of overall organization is enhanced. TBDAC is a framework in accordance with the standard of RBAC. Also, it is a dynamic access control model based on trust and the security of resource is ensured.

95.3.3.2 TOrBAC

In O-RBAC (organization-based access control) [21], the abstract concept of role, purpose, activity group, and structure is for the subjects, objects, and actions. Entities are abstracted by security policy. **TOrBAC** (trust organization-based

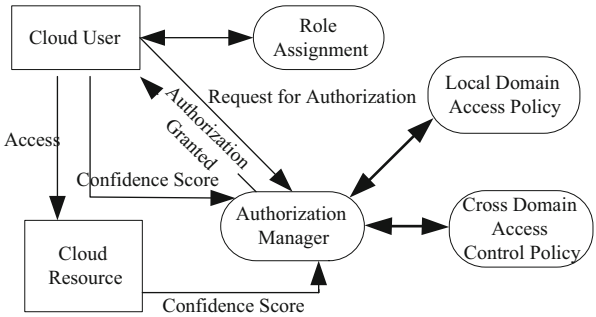

Fig. 95.2 Dynamic access control based on trust

access control) [22] is a new model for specifying such security policies, and a confidence index is calculated recursively using a formula. TTP is a third party which ensures that the interactions between two parties are both trustworthy. In TorBAC model, the cloud computing function of TTP and parameters confidence indicators are taken into account for the trust management. When used in cloud computing, it should be extended to a model which has the deeper mechanisms of detection of rape. In another aspect, the consistency and completeness of the security policy are also to be verified. Also, there is a need to develop more realistic use case and the associated mechanisms.

95.3.3.3 TCloud

Based on trust, a new cross-domain framework, TCloud [23], is proposed to meet the requirements of cloud computing. In multiple domains, access control will be based on the conversion of roles. The role assignment and conversion will take place dynamically. The high-level framework of multiple domain access control is depicted in Fig. 95.2.

First, the cloud user obtains an appropriate role by the role of the management center; then, a user ID, password, role, and resources to be accessed are submitted. After that, the user will interact with the authentication and authorization center to apply for authorization to access. If the resources requested for access are in the local domain, the local access control policies are invoked. Otherwise, cross-domain access control policies of permissions and management will be implemented.

Tcloud is a dynamic model for access control across multiple domains based on the traditional model of role-based access and trust. In single domain, the access is based on the traditional mechanism, while in multiple security domains, the roles are dynamically converted according to the domain of interest. This framework can be more intuitive, effectively protecting cloud users and ensuring the security of the cloud computing platform.

95.3.3.4 CTTM

CTTM (cross-tenant trust models) [24] is formalized based on four potential types of cross-tenant trust relations. In the formalization of CTTM, there are three entity components: **users (U)**, **permissions (P)**, and **tenants (T)**. A novel component **T** is introduced to express accesses in multi-tenant environments in which the other components should fit. **PO** is a many-to-one relation from **P** to **T. UO** may be a many-to-one relation or a many-to-many relation from **U** to **T** depending on implementation. **RB-CTTM** is a role-based extension of CTTM.

To verify the feasibility in the cloud, a cloud-based platform named multi-tenant authorization as a service (MTAaaS) is used. Each tenant has its own access control policy stored in the cloud service and managed through the MTAaaS platform. Also, attribute-based extensions of CTTM and other possible models which are compatible with MTAaaS platform should be investigated.

95.3.3.5 MT-RBAC

MT-RBAC (multi-tenant role-based access control) [25] family aims to provide fine-grained authorization in collaborative cloud environments by building trust relations among tenants. In MT-RBAC, the cross-tenant trust relation is established by the resource owner rather than by the resource requester. MT-RBAC extends the traditional RBAC model with two new built-in entity components: issuers and tenants. Three MT-RBAC models integrate three different trust relations with increasingly finer-grained constraints, respectively, tenant trust (MT-RBAC0), trustee-independent public roles (MT-RBAC1), and trustee-dependent public roles (MT-RBAC).

MT-RBAC models aim to address multi-tenant authorization for collaborative cloud services and enable fine-grained cross-tenant resource access by building tenant-level granularity of trust relations. Performance and scalability results show that the AaaS platform with MT-RBAC incurs an acceptable overhead and is scalable for the cloud storage service.

95.4 Comparisons and Future Work

95.4.1 Comparisons

As illustrated in Table 95.1, we compare these schemes which we have surveyed. We compare these schemes by the criteria of domain (single or multiple), dynamic (supported or not), multi-tenant (supported or not), goal (performance, security level, data loss, etc.), core techniques, etc.

Table 95.1 Comparisons of extended RBAC models

		Domain	Dynamic	Multi-tenant	Goal	Core technique
Basic RBAC extension	dRBAC	Single			Identify different enterprises and organizations	PKI and domain information contained in the certificate are taken advantage of
	CoRBAC	Multiple respectively			Improve overall efficiency	Reduce the established secure connection and set up multilevel cache
	E-RBAC	Single			Improve security level and reduce data loss	Restriction policy
	O-RBAC	Single		√	Security level enhanced and data loss reduced	Role ontology
	GTRBAC		√		Advocate for activation of roles	The dependencies relation among roles is temporal, which is enabled periodically
	X-GTRBAC		√		Trust level of a user is affected	Trusted third party provides the certification, the context is consider
A-RBAC	A-RBAC	Single	√		Reduce the attack surface, overcome collusion attacks	Cloud data storage architecture based on RBE
Trust-based RBAC	TBDAC	Single	√		Reduce security-hidden trouble, enhance security of overall organization	Authorization trust factor
	TorBAC	Multiple respectively			The external connection of users with different accesses are better controlled, the confidence of business operators cloud is strengthened	A confidence index is calculated using a recursive formula
	TCloud	Multiple respectively	√		The degree of trust in single as well as multiple domains are established and calculated	Trust concept
	CTTM	Multiple respectively	√	√	Bridge authorization domains of each tenant	Cross-tenant trust relations
	MT-RBAC	Single		√	Provide fine-grained authorization	Build trust relations among tenants

Remark: √ denotes that the criteria is supported
Do domain, *Dy* dynamic, *Mt* multi-tenant, *S* single, *M* multiple respectively

95.4.2 Future Work

The extended RBAC model above proposed different mechanisms for accommodating cloud computing environment, but still there are more issues to be resolved for the RABC model to be deployed.

If the users, roles, objects, and attributes of the environment are to be applied, it is necessary to develop property-driven RBAC model. Also, permission assignment for the real-time application needs to be developed to implement access control decisions. Based on the properties of the user to roles, the rules being used in assigning permission for the real-time application need to be developed to implement access control decisions.

Development of position-sensitive role-based access control model incorporated into PEP prevents user identity, role or position in the cloud from leaking to the remote server (may not be fully trusted), and only when the user is in a logical location within the boundaries of space enable/activate characters (calculated from the true position by the particular mapping function).

In cloud computing, there is the need of more formal definitions for different entities in RBAC. Also, more efforts on industrial standards, best practices, and large-scale experiments need to be put into.

At present, there is not much research going on for solving the access control problem involving multi-domain in industry and academia of cloud applications, but this problem cannot be ignored and new solutions are needed. Dynamic access control and multi-tenant architecture support also need further enhanced research efforts.

Conclusion

In this chapter, extended RBAC mechanisms for cloud computing are discussed elaborately. Basic RBAC extension is based on PKI and domain information, using restriction policy, role ontology, or incorporating dynamic characteristic separately. A-RBAC enforces RBAC policies on encrypted data using a hybrid cloud infrastructure. Trust-based RBAC models incorporate the trust concept into RBAC. It can be concluded that as the RBAC model gradually improves and combines with other security mechanism, RABC model will play a more and more important role in cloud computing security. We believe that the more successful on RBAC, the more maturity of the cloud computing platform.

Acknowledgments This paper was funded by the Innovation Program of Shanghai City Board of Education No. 11YZ194 and No. 12YZ146, No. 12YZ147, the founding Program of Shanghai Natural Science No. 11ZR1414300 and 12ZR1411900, and the founding Program of National Natural Science No. 61202020.

References

1. Mell P. The NIST definition of cloud computing. Int J Eng Technol. 2009;4(5):284.
2. Feng DG, Zhangetc M. Research on cloud computing security. J Softw. 2011;22(1):71–82. In Chinese.
3. Meghanathan N. Review of access control models for cloud computing. In: ICCSEA, SPPR, CSIA, WimoA – Computer Science & Information Technology (CS & IT). 2013. p. 77–85.
4. Ferraiolo D, Kuhn DR. Role-based access control. In: Proceedings of the 15th national computer security conference. 1992. p. 554–63.
5. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chadramouli R. Proposed NIST standard for role-based access control. ACM Trans Inform Syst Secur. 2001;4(3):224–74.
6. Shin ME, Ahn G. UML-based representation of role-based access control. In: IEEE 9th international workshops on enabling technologies: infrastructure for collaborative enterprises (WET ICE'00). 2010. p. 195–200.
7. Freudenthal E, Pesin T, Port L, Keenan E, Karamcheti V. dRBAC: distributed role-based access control for dynamic coalition environments. In: 22nd IEEE international conference on distributed computing systems (ICDCS'02). 2002. p. 411–20.
8. Zhu TY, Liu WD, Song JX. An efficient role based access control system for cloud computing. In: 11th IEEE international conference on computer and information technology. 2011. p. 97–102.
9. Parminder S, Sarpreet S. A new advanced efficient RBAC to enhance the security in cloud computing. Int J Adv Res Comput Sci Softw Eng. 2013;3(6):1136–42.
10. Parminder S, Sarpreet S. Towards novel and efficient architecture for extended-RBAC in cloud computing. Int J Comput Sci Inform Technol. 2013;4(3):515–8.
11. Sejong O, Park S. Task-role-based access control model. J Inform Syst. 2003;28(6):533–62.
12. Bertino E, Bonatti PA, Ferrari E. TRBAC: a temporal role-based access control model. ACM Trans Inform Syst Secur. 2001;4(3):191–233.
13. Joshi JBD, Bertino E, Latif U, Ghafoor A. A generalized temporal role-based access control model. IEEE Trans Knowl Data Eng. 2005;17(1):4–23.
14. Bhatti R, Joshi JBD, Bertino E, Ghafoor A. Access control in dynamic XML-based web-services with XRBAC. In: Proceedings of the 1st international conference on web services. 2003. p. 243–9.
15. Zhou L, Varadharajan V, Hitchens M. Enforcing role-based access control for secure data storage in the cloud. Comput J. 2011;54(10):1–143.
16. Zhou L, Varadharajan V, Hitchens M. Achieving secure role-based access control on encrypted data in cloud storage. IEEE Trans Inform Forensic Secur. 2013;8(12):1947–60.
17. Blomqvist K. The many faces of trust. Scand J Manage. 1997;13(3):271–86.
18. Mayer R, Davis J, Schoorman F. An integrative model of organizational trust: past, present and future. Acad Manage Rev. 1995;20(3):709–34.
19. Huang J, Nicol D. A formal-semantics-based calculus of trust. IEEE Internet Comput. 2010;14 (5):38–46.
20. Tan ZJ, Tang Z, Renfa L, Ahmed Sallam, Yang L. Research on trust-based access control model in cloud computing. In: IEEE 6th joint international information technology and artificial intelligence conference (ITAIC). 2011. p. 339–44.
21. Cuppens F, Cuppens-Boulahia N, Mie GE A. Inheritance hierarchies in the Or-BAC model and application in a network environment. In: Second foundations of computer security workshop (FCS'04). 2004. p. 1–10.
22. Saidi MB, Elkalametc AA. TOrBAC: a trust organization based access control model for cloud computing systems. Int J Soft Comput Eng. 2012;2(4):122–30.
23. Ullah S, Zheng XF, Zhou F. TCloud: a dynamic framework and policies for access control across multiple domains in cloud computing. Int J Comput Appl. 2013;62(2):1–7.
24. Tang B, Sandhu R. Cross-tenant trust models in cloud computing. In: ieee 14th international conference on information reuse and integration (IRI). 2013. p. 129–36.
25. Tang B, Li Q, Sandhu R. A multi-tenant RBAC model for collaborative cloud services. In: 11th annual international conference on privacy, security and trust (PST). 2013. p. 229–38.