Access Control Based Resource Allocation in Cloud Computing Environment

Junshe Wang[1], Jinliang Liu[2], and Hongbin Zhang[1]
(Corresponding author: Jinliang Liu)

School of Information Science and Engineering, Hebei University of Science and Technology[1]
26 Yuxiang Street, Yuhua District, Shijiazhuang City, Hebei Province, China
Communication System and Networks Department[2]
The 54th Research Institute of China Electronics Technology Group Corporation
589 Zhongshan West Street, Qiaoxi District, Shijiazhuang City, Hebei Province, China
(Email: 836251714@qq.com)

(Received Jan. 13, 2016; revised and accepted Apr. 17 & May. 31, 2016)

Abstract

In this paper, we propose a new dynamic resource allocation scheme - Access Control-based Resource Allocation (ACRA) for cloud users in order to address some deficiencies of the current resources allocation mechanisms in some free cloud computing environment. The proposed scheme comprehensively analyses behavior characteristics of cloud users and evaluates user behavior trust using fuzzy analytic hierarchy process (FAHP), and then dynamically adjusts the resources permission of cloud users according to their behavior trust values, thus effectively controlling user resource utilization. Experimental results show that the ACRA scheme can provide basis for allocating resources dynamically and reasonably to cloud users with different behaviors and improve resource utilization in cloud computing systems.

Keywords: Access control, cloud computing, dynamic permission adjustment, resource allocation

1 Introduction

Cloud computing is a new network computing model [16] based on virtualization technology and pay-on-demand business model, which can convert various types of resources (including hardware, platform and software) into services that can be used by cloud users with some special features, such as flexible expansion, dynamic resources allocation, and resource sharing. Dynamic resource allocation and sharing in a cloud computing environment is the common fundamental technology of IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) [5, 7], thus forms a major direction of research on cloud computing technologies.

As an effective mechanism for controlling resource access in systems, access control can restrict resources utilization of access subjects according to their identities and predefined policies, thus effectively ensuring confidentiality, integrity, availability and legal of resources. It is one of the key mechanisms for isolating access behaviors of different users in a system in order to limit security risks. Therefore, access control can be used as a technical solution to the problems of resource allocation in cloud computing [4].

The existing access control technologies are mostly static authorization [2, 18], that is, after the subject receives access permission from the object, the permission can be used without restriction. However, a cloud computing environment, which is different from regular networking environment due to its dynamic and openness features, brings in new challenges to access control for resource allocation.

2 Related Work

This article has researched dynamic allocation and sharing strategies of cloud resources in-depth from the perspective of theory and practice.The authors of reference [6, 11, 22] take proactive measures to the long-term, predictable periodical loads, use statistic and machine learning methods to analyze statistical data about load changes and system logs and built a performance model under long-term load patterns. Although the model provides decision support for global multi-objective optimum making on resources, evaluating the capacity of resources by the average working time required to complete each task exists biggish uncertain. The author of reference [14] starts a research from the angle of resources reliability, considers the failure regularity characteristics of resources in time and space, and uses it as the basis for resources allocation, which shields a lot of fault resource nodes. But there are limits to this strategy. It does not deal with the problem of resource expenditure minimization. In other words, it reduces the availability of resources when a resourceful node assigned to a task that requires very few resources. The author of reference [23] proposes a behavior-based resource provision policy for cloud computing. The policy can forecast the set of submitted task and expectation completing time of task at next time segment from the statistic results, and dynamically adjust the resource provision policy according to the policy table. This resource scheduling scheme does not give detailed analysis of user behavior characteristics.

At present, research focuses on the impact of load variation, the physical locations of resources or other factors on dynamic allocation and sharing of cloud resources, rarely involves the source of cloud computing demand and neglects the otherness among cloud users [10]. And in fact, in the process of cloud resource allocation, cloud user behaviors have a direct and significant impact on resource allocation, especially in some free cloud environments where cloud computing resources are only used by internal staff for free [20]. In such environments whether cloud resources are in an idle state becomes an important factor in judging the reasonability of resource utilization. If private cloud users do not undertake related tasks after acquiring cloud resources, it means they have seized these resources, and will affect resource utilization of other cloud users, as well as the resource utilization of the whole cloud computing system. In addition, malicious cloud computing users may utilize cloud resources perform malicious actions [21]. The behavior of some cloud users may change significantly over a period of time. All these factors will make well-behaved cloud users cannot get relevant cloud resources in time, which in turn affect the overall resource utilization of the cloud computing system [15].

The research presented in this paper aims at addressing the problem of degraded resource utilization in a private cloud environment caused by the equal permission granted to all cloud users. We propose a new access control-based scheme for cloud resource allocation that can not only improve the overall utilization of cloud resource, but also enhance security [9] for the cloud computing environment.

3 The ACRA Scheme Design

Inspired by the Role-based Access Control (RBAC) model reported in [1], in this paper we propose a new scheme of cloud resource allocation - Access Control-based Resource Allocation (ACRA). The overall framework of ACRA is shown in Figure 1.

The ACRA scheme consists of three key aspects. First, acquisition of cloud user behavior trust is a key component of the scheme. Both behavior of different users at the same moment and behavior of the same user under different circumstances are prodigiously different. Therefore, behavior trust can reflect behavior of cloud users; and accuracy of behavior trust evaluation directly impacts the subsequent authorization of cloud users [13]. The second key aspect of the scheme lies in, rules in the authorization process. Because the scheme is based on RBAC to solve problems in resource allocation in a cloud computing environment, the authorization rules involved must meet the requirements of the new environment. The third aspect of the ACRA scheme is to handle cloud user authorization required by the various behavior of cloud users in the cloud computing system. In this paper, we propose a dynamic permission adjustment mechanism on the basis of cloud users' behavior trust in order to manage their permission more flexibly, elastically and meticulously.

3.1 Behavior Trust Evaluation

3.1.1 Classification of Behavior Characteristics

The accuracy of behavior classification in a cloud computing environment has a direct impact on that of cloud user behavior trust evaluation, and then determines the reasonability of authorization. The classification of behavior characteristics involved in ACRA, in contrast to operation behavior in traditional access control, is a complex behavior [3] that integrates the utilization of cloud computing resources, network of cloud users, and operation behavior of cloud users. The utilization of cloud computing resources includes the average utilization of hard disks, memories, CPUs, bandwidth and occupied threads. The network of cloud users includes the average exception rate of login, the average propagation delay of IPs, the average time jitter of IPs and the average response time of IPs. The operation behavior of cloud users consists of the average attempt number of unauthorized operations, the average number of attacking other cloud users, the average number of illegal connections, the average number of illegally scanning important ports, the average number of running unsafe programs and the average number of escaping punishments.

3.1.2 Acquisition Methods of Behavior Trust

Analytic Hierarchy Process (AHP) deals with complex problems by breaking them into composing factors, building the hierarchy model according to these factors control relations, determining their relative importance through comparison among them, then setting the order of their relative importance under a people judgement premise. Building the judgement matrix is a key element of AHP to quantify the decision-maker thought for complex systems. However analysis found that is difficult to achieve the consistent standard. In addition, there is a difference between the consistency of judgement matrix and the consistency of human decision-thinking.

To solve the above-mentioned problem, we propose the Fuzzy Analytical Hierarchy Process (FAHP) [17, 19] that employs a Fuzzy Consistent Matrix to improve AHP algorithm.

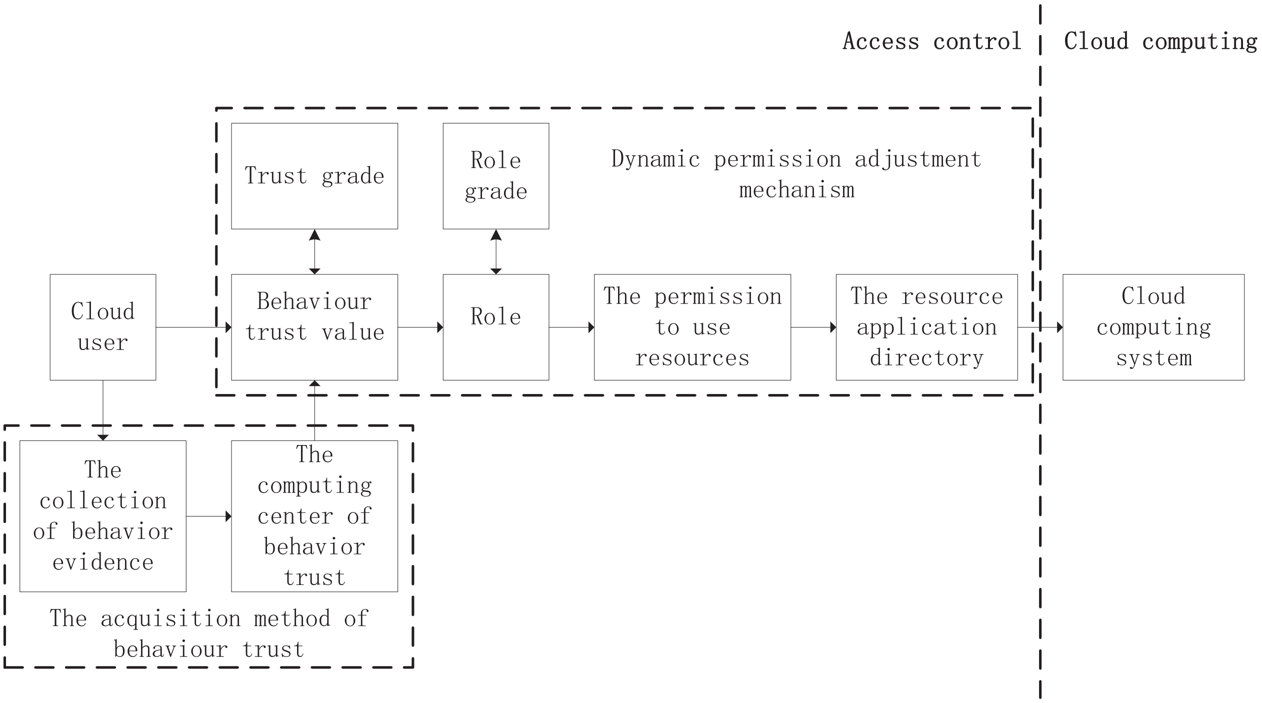
Access control
Cloud computing
Trust grade
Role grade
Dynamic permission adjustment mechanism
Cloud user
Behaviour trust value
Role
The permission to use resources
The resource application directory
Cloud computing system
The collection of behavior evidence
The computing center of behavior trust
The acquisition method of behaviour trust

Figure 1: The overall framework of ACRA

In FAHP, the cloud users' behavior is divided into n characteristics, and each characteristic is further divided into a number of evidence types, which all have been normalized to dimensionless and increasing values on the interval [0, 1] represented with the matrix $E = (e_{ij})_{n\times m}$, where m denotes the maximum term in these characteristics, and the item that doesn't reach m should be substituted with zero.

In order to obtain the initial judgment matrix $EQ = (eq_{ij})_{m\times m}$, there m evidence $E = (e_1, e_2, ..., e_m)$, dualistic comparison of the importance of e_i and e_j in the evidence set is conducted:

$$eq_{ij} = \left\{ \begin{array}{l} 0 \text{ if } \mathrm{e_i} < \mathrm{e_j} \\ 0.5 \text{ if } \mathrm{e_i} = \mathrm{e_j} \\ 1 \text{ otherwise} \end{array} \right\} \tag{1}$$

The initial judgment matrix is transformed into a fuzzy consistent matrix $Q = (q_{ij})_{m\times m}$ [8].

Theorem 1. *If fuzzy reciprocal matrix* $Q = (q_{ij})_{m\times m}$*is calculated with the following formulas, then the result is a fuzzy consistent matrix.*

$$eq_{ij} = \left\{ \begin{array}{l} \mathrm{q_i} = \sum_{\mathrm{k=1}}^{\mathrm{m}} \mathrm{eq_{ik}} \ \ \mathrm{i} = 1, 2, ..., \mathrm{m} \\ \mathrm{q_{ij}} = (\mathrm{q_i} - \mathrm{q_j})/2\mathrm{m} + 0.5 \end{array} \right\} \tag{2}$$

Proof.

$$\begin{aligned} q_{ij} + q_{ji} &= \frac{q_i - q_j}{2m} + 0.5 + \frac{q_j - q_i}{2m} + 0.5 \\ &= 1. \end{aligned}$$

So $Q = (q_{ij})_{m\times m}$ is a fuzzy reciprocal matrix:

$$\begin{aligned} q_{ij} &= \frac{q_i - q_j}{2m} + 0.5 \\ &= \frac{(q_i - q_k) - (q_j - q_k)}{2m} + 0.5 \\ &= \frac{q_i - q_k}{2m} + 0.5 - (\frac{q_j - q_k}{2m} + 0.5) + 0.5 \\ &= q_{ik} + q_{jk} + 0.5. \end{aligned}$$

□

Therefore $Q = (q_{ij})_{m\times m}$ is a fuzzy consistent matrix. Because the fuzzy consistent matrix has its special features that make it fit the consistency of human decision-thinking the fuzzy consistent matrix can be applied in AHP.

The weight vector $w = (w_1, w_2, ..., w_m)^T$ of a certain characteristic's evidence is calculated, where:

$$w_i = \frac{1}{m(m-1)/2}[\sum_{k=1}^{m} q_{ik} - 0.5]. \tag{3}$$

Then the assessed value matrix of cloud users' behavioral characteristics is calculated, according to the evidence matrix $E = (e_{ij})_{n\times m}$ and weight matrix $W = (w_{ij})_{n\times m}$, the value on the diagonal of the matrix obtained with $E \times W_T$ is the characteristic assessed value matrix $F = (f_1, f_2, ..., f_m)$.

The initial behavior trust value of a cloud user is defined as follows:

$$\begin{aligned} T_{initial} &= F \times W_f^T \\ &= \sum_{i=1}^{n} f_i w_i, \end{aligned} \tag{4}$$

where $W_f = (w_{f1}, w_{f2}, ..., w_{fn})$ is the weight set of behavior characteristics of cloud users.

It is possible to predict the trend of cloud users' behavior trust according to the sliding window principles and historical behavior trust records. In order to achieve the average effect of historical behavior trust on $T_{initial}$, the time decay value of cloud users' behavior trust with a recording time span z is calculated as follow:

$$T_{average} = \sum_{i=1}^{z} \frac{t_{old}^{(i)}}{t_{new} - t_{old}^{(i)} + 1}, \tag{5}$$

where $\frac{1}{t_{new}-t_{old}^{(i)}+1}$ is the time decay factor of cloud users' behavior trust $t_{old}^{(i)}$ with the recording number i,that is, the effect of historical behavior trust on current cloud users' behavior trust has become weaker with the passage of time.

Finally, according to the initial behavior trust $T_{initial}$ and the average effect of historical behavior trust $T_{average}$, the final value of cloud users' comprehensive behavior trust can be obtained with the following formula:

$$T_{final} = \alpha T_{initial} + (1 - \alpha) T_{average}. \tag{6}$$

3.2 Rules in Authorization

The purpose of obtaining the value of cloud users' behavior trust is to ensure authorization accuracy. Authorization rules involved in ACRA are different from those in traditional access control technologies. The cloud user permission refers to the right that users have to use a certain quantity of cloud resources, and the scope of permission is closely related to the behavior trust of the cloud user.

- The grading of behavior trust: In order to give a more meticulous authorization to cloud users u_i, their behavior trusts are graded into $G = (0, 1, ..., k, ..., , q)$, if $t_k \leq T(u_i) \leq t_{k+1}$ in which t_k, t_{k+1} $0 \leq k \leq q$ respectively represents the minimum and maximum value in a grade interval of behavior trust, and the trust grade of this cloud user is k.

- Mapping relationship: There is a one-one mapping relationship among the trust grade $G = (0, 1, ..., k, ..., , q)$ involved in the authorization, role $R = (R_0, R_1, ..., R_k, ..., , R_q)$ and permission $P = (P_0, P_1, ..., P_k, ..., , P_q)$. That is, after determining the trust grade of the cloud user u_i, cloud computing system will assign a grade role to the corresponding trust grade so as to authorize the user.

- Permission setting: The permission in cloud computing environment refers to the permission P of the resources utilization. It is the upper limit for the amounts of cloud resources assigned to cloud users who have applied for resource access. There is a inheritance relationship $P_0 \subseteq P_1 \subseteq ... \subseteq P_k \subseteq ...P_q$ in the permission P of the resources utilization.

  After obtaining a role, the cloud user will be granted permission to use cloud resources. The scope of cloud user's permission depends on the grade of his role. Those who get the high grade roles can utilize more cloud resources, and vice versa. Any cloud user with any role may apply for accessing a certain amount of cloud resources after obtaining permission, and may not necessarily utilize the resources after being granted the access.

3.3 The Dynamic Permission Adjustment Mechanism

Figure 2 is the flow chart of the dynamic adjustment on cloud users permission [12].

In the calculation centre of behavior trust, the FAHP algorithm is adopted to calculate and update the value of behavior trust based on the collected evidence values in real time. The cloud computing system assigns a grade role to the cloud user by judging the trust grade of the behavior trust, so as to achieve the purpose of adjusting the scope of cloud user's permission. The behavior trust value calculated when the cloud user utilizes the resources this time will directly influence his permission next time. This dynamic permission adjustment mechanism can meet the requirements of dynamic permission management in a cloud computing environment.

4 Experimental Verification

We have conducted simulation in order to verify effectiveness of the ACRA scheme.

4.1 Experimental Setup

The experiments were conducted by the use cloud computing software CloudSim, programmed with JAVA language in Eclipse development environment, MySQL database and php Study database management software.

The trust grade vector $G = (0, 1, 2, 3, 4)$ of cloud users was set in the experiment, considering the fact that behaviors of most cloud users are basically dependable or dependable in the actual resource allocation process, and just a minority of them are undependable, the interval between inter zones is respectively set as $(0.05, 0.25, 0.60, 0.80)$ following reference, and the interval between trust values is mapping with the corresponding trust grade. The relationship between the permission and trust grade is shown in Table 1.

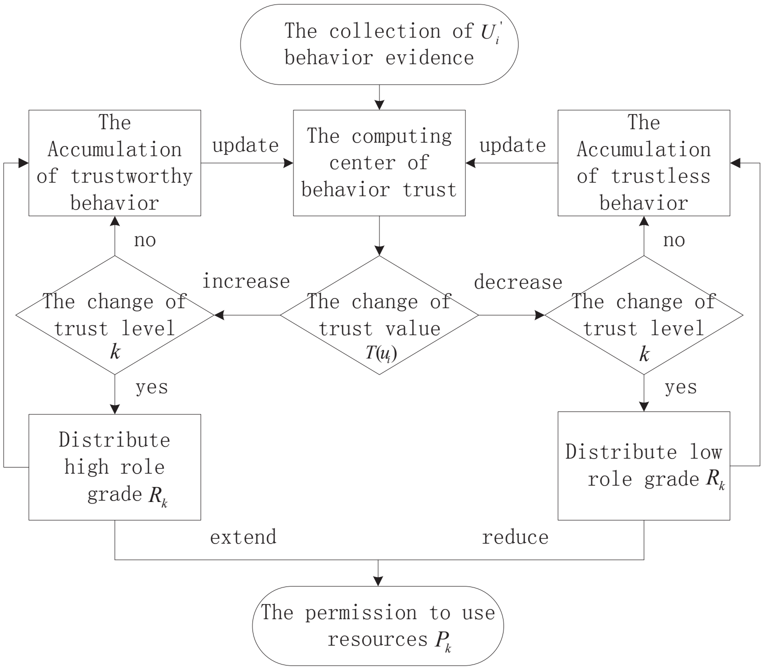
The collection of U_i' behavior evidence
The Accumulation of trustworthy behavior
update
The computing center of behavior trust
update
The Accumulation of trustless behavior
no
no
increase
decrease
The change of trust level k
The change of trust value $T(u_i)$
The change of trust level k
yes
yes
Distribute high role grade R_k
Distribute low role grade R_k
extend
reduce
The permission to use resources P_k

Figure 2: The flow chart of the dynamic adjustment on cloud users' permission

The record in the sliding window is $z = 5$, the historical behavior trust records before updating are shown in Table 2.

4.2 Calculation of Behavior Trust

There are three behavioral characteristics of cloud users: the resource utilization of cloud computing R, the network of cloud users N and the operation behavior of cloud users B, after basic evidence values of these three characteristics have been normalized, the average basic evidence value can be obtained as follows:

$$\begin{aligned} R &= (0.74, 0.75, 0.86, 0.63, 0.52, 0) \\ N &= (0.56, 0.49, 0.24, 0.42, 0, 0) \\ B &= (0.64, 0.77, 0.89, 0.86, 0.49, 0.91). \end{aligned}$$

The importance of R, N, B and their corresponding basic evidence in FAHP is shown as follows:

$$\begin{aligned} & R > B > N \\ & R_3 > R_2 > R_1 > R_4 > R_5 \\ & N_1 > N_4 > N_3 > N_2 \\ & B_1 > B_6 > B_2 > B_5 > B_4 > B_3. \end{aligned}$$

The weight values of all basic evidence are:

$$\begin{aligned} w &= (0.5, 0.1667, 0.3333)_T \\ w_r &= (0.2, 0.25, 0.3, 0.15, 0.1)_T \\ w_n &= (0.375, 0.125, 0.2083, 0.2917)_T \\ w_b &= (0.25, 0.1833, 0.0833, 0.1167, 0.15, 0.2167)_T. \end{aligned}$$

The initial behavior trust value $T_{initial}$ is 0.6927 according to the average basic evidence, the percentage of $T_{initial}$ in T_{final} is 0.95. Finally, the final value of comprehensive behavior trust T_{final} is 0.6588. Records of behavior trust values in the sliding window after being updated are shown in Table 3.

4.3 Simulation Analysis

We studied the behavior of a cloud user by setting a series of evidence values. Figure 3 reflects the changing trend of permission with changes in behavior trust values after the user access the cloud computing system for several times. It can be seen from the figure that when his behavior under the condition of poor performance, the number of resources who has the right to use will be decreased, when his behavior under the condition of good performance, the number of resources who has the right to use will be increased. With the change of behavior trust values, user's permission of accessing resources will be adjusted dynamically, as a cloud user utilizes cloud resources to complete computing tasks, his behaviors is closely related to the behavior trust value, which has effectively limited the user's ability in utilizing cloud resources utilization.

5 Scheme Analysis

5.1 The Safe Reliability

The scheme activates the role according to trust grade, which can ensure that a user who has successfully accessed the cloud computing system is trusted. Malicious partic-

Table 1: The classification of trust grade intervals

Trust grade	**Meaning**	**Inter zone**	**Permission**
0	Undependable	[0.00,0.05]	P_0
1	Low dependable	(0.05,0.25]	P_1
2	Basically dependable	(0.25,0.60]	P_2
3	Dependable	(0.60,0.80]	P_3
4	High dependable	(0.80,1.00]	P_4

Table 2: Records of behavior trusts in the sliding window before updating

ID	**6**	**7**	**8**	**9**	**10**
Trust	0.1367	0.3486	0.724	0.2496	0.7231
Time1	2015.01.23	2015.02.03	2015.02.07	2015.03.02	2015.04.08
Time2	18:42:11	02:33:15	05:27:50	14:12:27	15:06:14

Table 3: Records of behavior trust values in the sliding window after being updated

ID	**7**	**8**	**9**	**10**	**11**
Trust	0.3486	0.724	0.2496	0.7231	0.6588
Time1	2015.02.03	2015.02.07	2015.03.02	2015.04.08	2015.07.23
Time2	02:33:15	05:27:50	14:12:27	15:06:14	16:25:00

ipants will be locked out of the cloud computing system, therefore intrusion from illegal users can be prevented. By using role grade-based dynamic authorization instead of direct authorization at user registration, the proposed scheme can solve the deficiency of the traditional RBAC model, in which the administrator assigned user role may allow insiders to obtain opportunities to tamper user data. Therefore, the scheme greatly improves the cloud computing system's stability, reliability and security.

5.2 Dynamism

The traditional RBAC model is a static authorization model in which user permission is statically assigned by system administrators. This model includes two static assignment parts: user role assignment and user' role-based authorization. The scheme presented in this paper enables dynamic access control by introducing the concept of a behavior trust value into these assignment parts. The proposed scheme calculates a user behavior trust value by collecting the dynamic data, and dynamically activates the user's role, and authorizes the user's access, which gives a user different level of access permission at different time.

6 Conclusions

In this paper we studied resource allocation in the authorization stage of cloud computing and proposed a new access control-based scheme for cloud resource allocation - ACRA. This scheme first conducts a comprehensive analysis on behavioral characteristics of cloud users, and acquires user behavior trust values using Fuzzy Analytic Hierarchy Process (FAHP). The scheme then decides authorization rules for cloud users and provides a mechanism for dynamic permission adjustment. Experimental results show that ACRA can achieve more flexible and meticulous authorization, effectively restrict the ability of cloud users in resources access, provides the basis for allocating resources to cloud users with different behavior performances, improve overall cloud resource utilization and protect security of the cloud computing environment. The next goal of our research work is to consider performance overhead of the scheme model.

Acknowledgments

This work is supported by College Science and Technology Research Project of Hebei Province (ZD20131016), Natural Science Fund Project of Hebei Province (F2013208137).

References

[1] L. Chang, F. Wang, L. Zhao, Y. Jia, and Z. Cheng, "CT-RBAC: An access control model in cloud com-

puting," *Microelectronics and Computer*, vol. 31, no. 6, pp. 152–157, 2014.

[2] T. Che, J. Ma, N. Li, and C. Wang, "A security quantitative analysis method for access control based on security entropy," *International Journal of Network Security*, vol. 17, no. 5, pp. 517–521, 2015.

[3] K. V. Devi and S. Vetha, "Capacity based resource allocation in cloud," in *Proceedings of 2014 International Conference onCommunication and Network Technologies (ICCNT'14)*, pp. 24–26, Sivakasi, India, Dec. 2014.

[4] Z. Feng, Z. Qin, D. Yuan, and Y. Qing, "Key techniques of access control for cloud computing," *Chinese Journal of Electronics*, vol. 43, no. 2, pp. 312–319, 2015.

[5] W. F. Hsien, C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[6] Q. Li, Q. Hao, L. Xiao, and Z. Li, "Adaptive management and multi-objective optimization for virtual machine placement in cloud computing," *Chinese Journal of Computers*, vol. 34, no. 12, pp. 2253–2266, 2011.

[7] C. Ling, W. F. Hsien, and M. S. Hwang, "A double circular chain intrusion detection for cloud computing based on adjointvm approach," *International Journal of Network Security*, vol. 18, no. 2, pp. 397–400, 2016.

[8] Y. Liu and J. Zhang, "Consistency and scale in fahp," *Journal of Northeast Normal University(Natural Science Edition)*, vol. 42, no. 2, pp. 27–30, 2010.

[9] E. O. Osei and J. B. H. Acquah, "Cloud computing login authentication redesign," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 1–8, 2014.

[10] S. Parikh, "A survey on cloud computing resource allocation techniques," in *Proceedings of 2013 Nirma University International Conference on Engineering (NUiCONE'13)*, pp. 397–404, Taipei, Taiwan, Nov. 2013.

[11] M. Risch, G. Li, and C. Courcoubetis, "The gridecon platform: A business scenario tested for commercial cloud services," in *Proceedings of the 9th Int Conf on Cluster Computing and the Grid*, pp. 46–59, Berlin, Germany, Aug. 2009.

[12] N. Sklavos and O. Koufopavlou, "Access control in networks hierarchy: Implementation of key management protocol," *International Journal of Network Security*, vol. 1, no. 2, pp. 103–109, 2005.

[13] Y. Tan and C. Wang, "Trust evaluation based on user behavior in cloud computing," *Microelectronics and Computer*, vol. 32, no. 11, pp. 148–151, 2015.

[14] G. Tian and D. An, "Failure rules based node resource provision policy for cloud computing," in *Proceedings of 2010 IEEE International Symposiums on Intelligent Signal Processing*, pp. 397–404, Taipei, Taiwan, Sept. 2010.

[15] P. Varalakshmi, T. H. Judgi, and M. Fareen, "Local trust based resource allocation in cloud," in *Proceedings of 2013 Fifth International Conference on Advanced Computing (ICoAC'13)*, pp. 591–596, Chennai, India, Dec. 2013.

[16] Y. Wang, J. Yang, C. Xu, X. Ling, and Y. Yang, "Survey on access control technologies for cloud computing," *Journal of Software*, vol. 26, no. 5, pp. 1129–1150, 2015.

[17] C. Xiao and M. Chen, "Research on user behavior trust model based on ifahp in cloud computing environment," *Netinfo Security*, vol. 12, no. 0, pp. 14–20, 2015.

[18] H. Xiong, X. Chen, X. Fei, and H. Gui, "Attribute and rbac-based hybrid access control model," *Application Research of Computers*, vol. 33, no. 7, pp. 1–10, 2015.

[19] T. Yang, Y. Yuan, and M. Zhang, "Research of site selection of housing industrialization base based on fuzzy analytic hierarchy process," *Journal of Engineering Management*, vol. 29, no. 2, pp. 43–48, 2015.

[20] B. Yin, Y. Zhang, B. Fang, and W. Feng, "Cloud resource allocation method based on elastic resource adjustment," *Telecommunications Science*, vol. 11, no. 4, pp. 22–27, 2014.

[21] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, "Establishing safe cloud: Ensuring data security and performance evaluation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 88–99, 2014.

[22] W. Zhang, H. Zhang, D. Zhang, and T. Cheng, "Memory cooperation optimization strategies of multiple virtual machines in cloud computing environment," *Chinese Journal of Computers*, vol. 34, no. 12, pp. 2266–2277, 2011.

[23] J. Zhou, W. Zha, Y. Chen, and H. Zhang, "User-aware resource provision policy for cloud computing," *Journal of Computer Research and Development*, vol. 51, no. 5, pp. 1108–1119, 2014.

Junshe Wang received her B.S. degree from the Department of automation at Hebei Institute of Mechano-Electric Engineering in 1982. Now, she is a professor in School of Information Science and Engineering at HEBUST, located in Shijiazhuang, China. Her current research interests include management of network and management of computer information, etc.

Jinliang Liu is an assistant Engineer of Communication system and networks department at The 54th Research Institute of China Electronics Technology Group Corporation, he received his B.S. degree and M.S. degree from the Department of School of Information Science and Engineering at HEBUST, located in Shijiazhuang, China. His current research areas include management of network, access control technology and its applications in cloud computing environment, etc.

Hongbin Zhang is an associate professor of School of Information Science and Engineering at HEBUST, he received his B.S. degree from the Department of automation at HEBUST in 1998, received his MS, and Ph.D. degrees from the School of Computer Science and Technology at Xidian University in 2005, 2009. His current research interests include management of network, insider threat analysis, etc.