

Stochastic Programming-Based Dynamic Authorization Model for Cloud Services Environments

Kang He, Zhuo Tang, Emmanuel.Gonzalez, Renfa Li

Embedded Systems & Networking Laboratory, Hunan University, Chang Sha, China

hekang0829@163.com

Abstract—Due to the complexity of service resources and the dynamics of application requirements in cloud computing, the objects and subjects of access control model constantly change. Consequently, traditional access control models no longer meet the requirements of cloud security. In this paper, a multi-objective decision-making model based on stochastic programming is proposed. By introducing new variables such as risk and utility, we are able to quantify the current state of the cloud environment. Afterwards, we can use this information to select appropriate safety decision variables to compute the model, taking the minimization of risk and the maximization of utility as the goals. The results obtained by solving the model can be used to allow or deny the user's requests, while considering the dynamic structure of the cloud. In this way, the security of cloud resources can be assured at its core. The experimental results show that, depending on the user requirements and the current cloud environment, solving the model can effectively be used to grant the user the appropriate permissions to access different service resources.

Keywords—Cloud Computing, Access Control, Stochastic Programming, Utility, Risk

I. INTRODUCTION

With the development of virtualization and web services technologies, as well as the advancements made in hardware and software, cloud computing has become a reality [1]. The purpose of cloud computing is to use the Internet as a medium to provide users all kinds of resources, such as processing power, software applications, and storage. These resources can grow larger or smaller on demand, depending on the application needs; and the user is only billed for the resources that have been consumed. Currently there are many large projects, such as Google App Engine [2]. Moreover, cloud computing in China is expected to be a result of the further development of parallel computing, distributed computing and grid computing [3].

A cloud computing system is a distributed system, facing many different users and applications. When a particular user submits a request to the cloud platform, the user first has to go under an authentication process in order to acquire the right permissions to be able to accomplish the task. The cloud computing system needs to be capable of meeting the user's needs, but at the same time should prevent unauthorized users from accessing and operating the system's resources.

Cloud computing's service resources and application requirements are complex and dynamic. Service resources are supplied by different service providers, and since the security levels of each service provider are different, they also need to be taken into account in the model. Similarly, there is large number of users in cloud computing, and the access control requirements of each user, for each one of the various applications, are different. Users have different properties related to system's security, such as the user's safety factor; therefore, we also have to include these in our model.

Because of the nature of the cloud environments, the subjects and objects will change frequently in the security policy. In traditional access control models, such as role-based access control model (RBAC)[4], usually the subject's permissions are granted once and can be used repeatedly; however, these permissions are difficult to adjust within dynamic environments [5], thus making it unsuitable for the accomplish the various cloud computing requirements. In the complex cloud computing environment, it is of great significance to be able to access the needed resources both efficiently and securely.

In this paper, a multi-objective decision-making model based on stochastic programming [6, 7] is proposed, to be used in a cloud computing environment. In a nutshell, when a user requests a resource from service providers, this model attempts to quantify the cloud environment and the current situation of the subject and object of the access control, with the minimization of risk and the maximization of utility as its goals. Solve the model, and we can find the most optimal configuration for implementing system security.

In traditional access control models, the design is often done first, and only then the security is analysed [8]. This approach essentially makes little effort to guarantee security. In this paper, based on the actual cloud computing environment, the appropriate decision variables are selected, and can be used to show the risk and utility functions, as well as constraint conditions. The results obtained by solving the model can be used to elaborate the permission of users that factors risk, utility and security at its core.

This paper is arranged as follows: section 2 presents other related work, section 3 discusses in detail the proposed model, section 4 solves an instance of the model, section 5 concludes the paper.

II. RELATED WORK

In order to protect system resources, an access control model is put in place. The core of the access control model is authorization, that is, a set of criteria that determine if the subject has been granted permission to operate on the object [9].

The typical access control models [9] are discretionary and mandatory access control (DAC and MAC), and RBAC. The classic RBAC model had been introduced in multi-user and multi-application online systems, and was further developed by Sandhu in 1996 [4]. The main idea is this: a group of permissions are assigned to a role, and roles are given to a user. In this way, the user acquires permissions through the roles that have been given. A role associates a user with a permission (or action). It is a convenient and effective way to manage permissions.

Traditional distributed access control model protects resources from the system's point of view. The weakness of such a passive safety model is that it cannot dynamically change the permissions of the subject, according to the changes of environment [5]. However, in the cloud computing environment, the complex service resources, and dynamic changes of application requirements cause the subject and object in the security strategy to change very often. As a result, the traditional access control models cannot meet the cloud's application requirements.

In cloud computing, it is hard to ensure the safety of the data in the system, and in such an open distributed environment, it is not enough to only take the most basic safety measures. Other works have introduced an economic security model, where the risk factors are evaluated in distributed environments, and it has been established that the mishandling of even a single operation can create an economic loss [10]. In the meantime, the utility should also be considered to be one of the most important factors in information security [11]. In the security mechanisms of a distributed system, authorization will directly influence the system utility [12, 13]. Other authors have determined that the balance between security and utility can be obtained [14], but their results are not suitable for a cloud computing environment, in which resources and needs are dynamic.

In a real implementation of cloud computing, the user requirements are unknown and unpredictable, and the

resources from the provider are also diverse. The model we created incorporates this uncertainty in the form of randomness, by using stochastic programming. Stochastic programming is used to build mathematical models, and solve math optimization problems with random variables. We try to adopt stochastic programming to quantify the risks and utility in the environment of cloud computing, and then we build and solve a multi-objective mathematical model, to obtain risk minimization and utility optimization. This method based on stochastic programming can pick up the optimal solution, regardless of having several different authorization schemes.

III. SYSTEM MODEL AND ASSUMPTIONS

A. Basic assumptions in cloud computing

The objects are the different resources supplied by cloud providers. The set is $CV = \{cv_1, cv_2, \dots, cv_i, \dots, cv_n\}$ and $cv_i (i=1, 2, 3, \dots, m)$ represents different types of service resources, and the corresponding value of resources is $cv_i.ol$. It is assumed that a user can complete the required task if he has access to these resources.

The set of cloud service providers is $CP = \{cp_1, cp_2, \dots, cp_j, \dots, cp_n\}$, and $cp_j (j=1, 2, 3, \dots, n)$ means a different cloud service provider. The corresponding safety factor is $cp_j.sl$.

Each provider can supply some types of the service resources, and the same service can be offered by many providers.

Generally speaking, a user can access the service resources through the following operations: read, write, execute, modify. In this paper, we will short them as r, w, e and m . The risk of every operation is showed by A_k (k is one of r, w, e and m).

Subject represents an entity such as a person or an application. S_s represents the safety factor of the subject.

The same service can have different costs, depending on the provider that supplies it. Similarly, different services supplied by the same provider all can have different costs. $c_{j,i}^k$ means the cost per unit time of using option k to access the service cv_i supplied by cloud provider cp_j . Also, $t_{j,i}^k$ represents the corresponding time required.

Permission can be showed by $p = \langle O, A, CPI \rangle$, O is the set of objects, A is the set of operations that subject can use to operate on the object, CPI is the set of cloud providers that contain the object. For example, $p = \langle cv_i, k, cp_j \rangle$ means the user can use the operation k to access the service cv_i supplied by cloud provider cp_j .

Decision variable $x_{j,i}^k$ is a binary variable which indicates if a user is able to use the operation k to access the service cv_i supplied by cloud provider cp_j . If $x_{j,i}^k = 1$, the answer is yes, while if $x_{j,i}^k = 0$, the operation is forbidden.

B. Risk model

Different access control permissions have different risks. When a user access the cloud provider's resources, the total risk of the operation can be calculated, and then establish the level of safety of this operation. The definition of risk is

related to the likelihood of the risk happening, and the possible consequences caused by the risk [15].

Risk(permission) = (possibility of an unauthorized access operation) * (value of accessed resources).

$$Risk_p = p_k * a^{cvi_ol} \quad (1)$$

In formula (1), $a > 1$, a is a real number, a^{cvi_ol} is the value of unauthorized accessed resources.

Generally speaking, as the safety factor of subjects S_s increases, the probability of the objects accessed in an unauthorized way by the corresponding subject decreases. At the same time, as the safety factor of the service provider increases, the more difficult it is for the service resources supplied by the provider to be accessed in an unauthorized way. The probability of p_k can be calculated by the following formula:

$$P_k = A_k * a^{-(S_s + CPj_sl)} \quad (2)$$

Thus, risk can be calculated by:

$$Risk_p = p_k * a^{cvi_ol} = A_k * a^{cvi_ol - (S_s + CPj_sl)} \quad (3)$$

C. Utility model

The utility is used to represent the satisfaction of a user when permissions to access a resource have been granted. Users do not know the location of the accessed resource, or the cloud service provider that's offering it. The user is concerned with the cost of the accessed resource, the time spent, and whether or not they can complete the task successfully.

A user accesses resources in order to complete a task, and this task can be further divided into many small tasks. We can suppose that the access to a resource can be considered to complete a small task. For simplicity, if a user obtains permissions to access a required resource, we can say that the user finished a task successfully. So the utility can include the following:

Task completion rate ($Rate_t$): During the expected time, the rate of the total number of accesses which were successfully completed and the total number of accesses which were required when the user submitted the task.

Task completion cost ($Cost_t$): The cost that the user should pay off after the task has been successfully completed.

$$Cost_t = \sum_{cp_j \in CP} \sum_{cv_i \in CV} \sum_k (x_{j,i}^k * c_{j,i}^k * t_{j,i}^k) \quad (4)$$

In formula (4), k is one of r, w, e and m .

Task completion time (T_t): the time difference between the moment the task was submitted and the moment the user can successfully access the resources.

$$T_t = Max(t_{j,i}^k * x_{j,i}^k) \quad (5)$$

T_u and $Rate_u$ represent the expected time and task completion rate of a user, respectively.

D. Demand-risk/utility model and Model optimization

In the actual cloud service, the user's demands are uncertain and unpredictable. d_i can be used to express the option that a user will select when he accesses the service cv_i . So the Vector $D = \{d_1, d_2, \dots, d_i, \dots, d_m\}$ represent the user's demand for all kinds of

service. (if $d_i = 0$, it means that the user doesn't access the service. Else, d_i is one of r, w, e and m).

In the Vector $D = \{d_1, d_2, \dots, d_i, \dots, d_m\}$, the value of each element $\overline{d_1}, \overline{d_2}, \overline{d_3}, \dots, \overline{d_n}$ represents the set of values of each element, respectively. So $D = \overline{d_1} \times \overline{d_2} \times \overline{d_3} \times \dots \times \overline{d_n}$ means the Cartesian product of the set. It should meet the constraint:

$$D \in \overline{D} \quad \text{and} \quad \sum_{D \in \overline{D}} p(D) = 1 \quad (6)$$

In the optimization process, the approaches of multiple objective programming and linear programming are used; the minimization of risk and the maximization of utility are the goals. Attributes of subject and object, and authorized conditions are considered to be the optimal requirements. Our model must satisfy the minimum privileges and separation of duties.

If D represents the demand, the Risk/cost/time optimization model can be shown:

Maximize:

$$Rate_t = \sum x_{j,i}^k / (\sum \text{the total number of } (d_i \neq 0)) \quad (7)$$

Minimize:

$$Risk = \left(\sum_{D \in \overline{D}} \sum_{cp_j \in CP} \sum_{cv_i \in CV} \sum_k p(D) (x_{j,i}^k(D) * A_k * a^{cvi_ol - cpj_sl - s_i}) \right) / \sum_{D \in \overline{D}} p(D) \quad (8)$$

$$Cost_t = \left(\sum_{D \in \overline{D}} \sum_{cp_j \in CP} \sum_{cv_i \in CV} \sum_k p(D) (x_{j,i}^k(D) * c_{j,i}^k * t_{j,i}^k) \right) / \sum_{D \in \overline{D}} p(D) \quad (9)$$

Subject to:

$$Rate_t \approx Rate_u = 1 \quad (10)$$

$$\sum_{cp_j} x_{j,i}^k \leq n \quad (11)$$

$$x_{j,i}^k = 0 \text{ or } 1 \quad cv_i \in CV \quad cp_j \in CP \quad D \in \overline{D} \quad (12)$$

$$Max_{j,i} \{t_{j,i}^k\} \leq T_u \quad (13)$$

$$x_{j1,i1}^{k1} * x_{j2,i2}^{k2} = 0 \quad (14)$$

The cloud service needs to meet the requirement of users. Obviously, the expected task completion rate of a user equals 1. Thus, the actual task completion rate is close to 1. In equation (11), n is the limited number of cloud service providers of a user can access. Normally, it is better that a user access resources supplied by the same cloud service provider. And the equation (14) shows that permission $p_1 = \langle cv_{i1}, k_1, cp_{j1} \rangle$ and $p_2 = \langle cv_{i2}, k_2, cp_{j2} \rangle$ cannot coexist.

IV. ALGORITHM SIMULATION

The experimental data came from The National Supercomputing Center of Changsha, and the used services resources are user identity verification, authorized service, and single point login service respectively.

LINGO was used to complete the simulation [16], and the model was converted into a single target model for simplicity. Regarding access control models, the minimization of risk is usually the most important target. Task completion rate is main reason that drives the user to access the cloud service, and we're going to assume that it always equals 1, for convenience.

For solving the model conveniently, it can be expressed as:

$$a1 * Risk + a2 * Cost$$

And $a_1+a_2=1$, $a_1>a_2$, that is, risk is more important. We suppose $a_1=0.9$, $a_2=0.1$.

In the model, there are several different variables. We will use the following values:

- Cloud service provides: $CP=\{cp_1, cp_2\}$;
- Cloud service resources: $CV=\{cv_1, cv_2, cv_3\}$; the value of resources are 0.8, 0.8 and 0.9, respectively;
- The risk values when a user performs the operation r , w , e and m are 0.2, 0.4, 0.6 and 0.8, respectively.

A. The first simulation

- Experimental conditions: $CP=\{cp_1, cp_2\}$, can provide resources $CV=\{cv_1, cv_2, cv_3\}$; the safety factor of user is $S_s=0.8$, and demand is $D=(r, w, w)$;
- Change conditions: cp_1_ol , cp_2_ol ;
- Results are displayed in the following Table 1:

TABLE 1. THE FIRST SIMULATION RESULTS

	X=1	(Risk) min	(Cost) min	Total
$cp_1_ol=0.8$ $cp_2_ol=0.8$	$x(cp_2, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_2, cv_3, w)$	0.468 2315	2.270 000	0.648 4083
$cp_1_ol=0.8$ $cp_2_ol=0.9$	$x(cp_2, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_2, cv_3, w)$	0.440 7771	2.270 000	0.623 6994
$cp_1_ol=0.85$ $cp_2_ol=0.8$	$x(cp_2, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_1, cv_3, w)$	0.449 7784	2.340 000	0.638 8005
$cp_1_ol=0.85$ $cp_2_ol=0.9$	$x(cp_2, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_2, cv_3, w)$	0.432 0115	2.270 000	0.615 8103
$cp_1_ol=0.9$ $cp_2_ol=0.8$	$x(cp_1, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_1, cv_3, w)$	0.423 6734	2.410 000	0.622 3060

As expected, if the safety factor of the cloud service provider change, the risk values will change. The permissions are adjusted dynamically, and the cost also varies. But the provider which provides the highest utility will be chosen, even if the risk values are the same.

B. The second simulation

- Experimental conditions: $CP=\{cp_1, cp_2\}$, $cp_1_ol=0.8$, $cp_2_ol=0.9$, and the safety factor of user is $S_s=0.8$, demand is $D=(r, w, w)$;
- Change conditions: the provided resources
- Result as the following Table 2:

In clouds, the resources for different providers are not the same, so the authorization is different. Even if users have the same demand, the minimum of the risk and cost may be different because of the different clouds. The proposed multi-objective model can be dynamically created according to the current environment, so the right permission to access the provided resources can be obtained by the user.

C. The third simulation

- Experimental conditions: $CP=\{cp_1, cp_2\}$, can provide resources $CV=\{cv_1, cv_2, cv_3\}$, $cp_1_ol=0.8$, $cp_2_ol=0.9$, and the safety factor of user is $S_s=0.8$;
- Change conditions: user demands
- Result as the following Table 3:

As expected, the demands of the user are different, so the criteria for accessing resources are different. According to the needs of users, the model changes dynamically, so the permissions that meet the requirements will be granted the user. Of course, the relative minimum of each case is different.

TABLE 2. THE SECOND SIMULATION RESULTS

	X=1	(Risk) min	(Cost) min	Total
cp_1 : $\{cv_1, cv_2, cv_3\}$ cp_2 : $\{cv_1, cv_2, cv_3\}$	$x(cp_2, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_2, cv_3, w)$	0.440 7771	2.270 000	0.623 6994
cp_1 : $\{cv_1, cv_2, cv_3\}$ cp_2 : $\{0, cv_2, cv_3\}$	$x(cp_1, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_2, cv_3, w)$	0.449 3290	2.340 000	0.638 3961
cp_1 : $\{cv_1, cv_2, 0\}$ cp_2 : $\{cv_1, 0, cv_3\}$	$x(cp_2, cv_1, r)$ $x(cp_1, cv_2, w)$ $x(cp_2, cv_3, w)$	0.440 7771	2.270 000	0.623 6994

TABLE 3. THE THIRD SIMULATION RESULTS

D	X=1	(Risk) min	(Cost) min	Total
(r, r, r)	$x(cp_2, cv_1, r)$ $x(cp_1, cv_2, r)$ $x(cp_2, cv_3, r)$	0.261 0455	0.680 000	0.302 9410
(w, r, w)	$x(cp_1, cv_1, w)$ $x(cp_1, cv_2, r)$ $x(cp_2, cv_3, w)$	0.449 3290	2.010 000	0.605 3961
(w, e, r)	$x(cp_1, cv_1, w)$ $x(cp_2, cv_2, e)$ $x(cp_2, cv_3, r)$	0.513 5392	3.960 000	0.858 1853
(e, e, e)	$x(cp_1, cv_1, e)$ $x(cp_2, cv_2, e)$ $x(cp_2, cv_3, e)$	0.783 1366	7.040 000	1.408 8230
(w, e, m)	$x(cp_1, cv_1, w)$ $x(cp_2, cv_2, e)$ $x(cp_1, cv_3, m)$	0.820 9416	8.890 000	1.869 8470

D. The forth simulation

On the basis of the third simulation, the two cases that the proposed model is used or is not used in the cloud computing system are considered. When the proposed model is not used, the permissions met the needs of users are can be random selected. And the resulted risk, cost, and total value are comparative analyzed. The results are showed in Table 4. At

the same time, the corresponding total value are analyzed and showed in Figure 1.

TABLE 4. THE FORTH SIMULATION RESULTS

D		Risk	Cost	Total
(r,r,r)	optimum	0.261 0455	0.680 000	0.302 9410
	random	0.279 0486	0.810 000	0.332 1438
(w,r,w)	optimum	0.449 3290	2.010 000	0.605 3961
	random	0.423 6734	2.64 000	0.909 3060
(w,e,r)	optimum	0.513 5392	3.960 000	0.858 1853
	random	0.496 4355	4.23 000	1.292 792
(e,e,e)	optimum	0.783 1366	7.040 000	1.408 823
	random	0.757 481	7.94 000	2.269 733
(w,e,m)	optimum	0.820 9416	8.890 000	1.869 847
	random	0.846 5972	12.1699 952	1.978 937

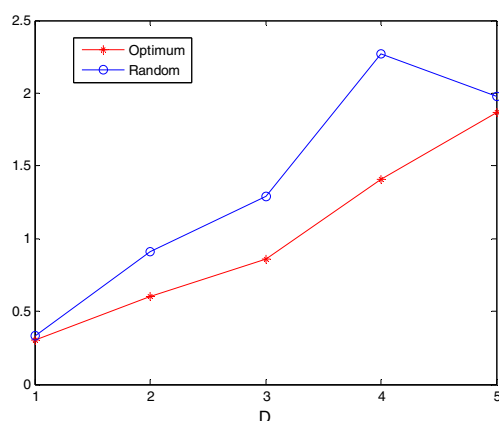


Figure 1. the corresponding total value are analyzed

Obviously, in the same demand, the resulted risk, cost, and total value in the two cases are different. The permissions acquired by the proposed model can meet constraints that the risk and cost are relative minimum.

When $c_{j,i}^k$ and $t_{j,i}^k$ changes, the results also are different, because they affect both the cost and the time constraints.

The simulation results show that, based on the needs of users, if you quantify the current cloud system environment, build the model dynamically, consider the minimum risk and the maximum utility as the relative goals, then we can get the decision variables, and the corresponding permissions can be granted to the user. Then, the user can complete the task safely by using the permission to access the resources.

I. CONCLUSIONS

A dynamic access control model based on the stochastic programming in cloud computing is proposed. By quantifying the current cloud system environment and the attributes of subject and object, considering constraints such as time, resources situation, the minimum privileges and separation of duties, a multi-objective model is created. The model regards completing user tasks as the first goal, and makes it possible for a user to access the resources safely on the basis of less cost. And security is enforced by making the minimization of security risks the most important factor in the model. The experimental results show that, according to the user requirements, solving multi-objective model can effectively be used to grant the user the appropriate permissions.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China(61103047), National Postdoctor Science Foundation of China (20100480936), and Hunan Natural Science Foundation(11JJ4052).

REFERENCES

- [1] Won Kim, Soo Dong Kim, Eunseok Lee, and SungYoung Lee, "Adoption issues for cloud computing," *Proceeding of MoMM2009*, 2009: 2-5.
- [2] (2008) Google App Engine [EB/OL], [Online]. Available: <http://appengine.google.com>.
- [3] <http://www.cloudcomputing-china.cn/Article/cloudcomputing/201008/674.html>.
- [4] Ravi S.Sandhu, Edward J.Coyne, Hal L.Feinstein, and Charles E.Youman., "Role-based access control models," *IEEE Computer*, 29(2), pp. 38-47, 1996.
- [5] Xu Feng, Lai Haiguang, Huang Hao, and Xie Li, "Service-oriented role-based access control," *Chinese Journal of Computers*, 28(4), pp. 686-693, 2005.
- [6] Liu Baoding, and Zhao Ruiqing, *Basis of Optimum--Model and Method*, Beijing: Tsinghua University Press, 2005.
- [7] <<Operations Research>> written by materials group, *Operations Research*, 3nd ed., Beijing: Tsinghua University Press, 2005.
- [8] Powers.C.S, Ashley.P, and Schunter.M, "Privacy promises, access control, and privacy management-Enforcing privacy throughout an enterprise by extending access control," *Proceedings of the Third International Symposium on Electronic Commerce*, pp. 13- 21, 2002.
- [9] Shen Haibo, and Hong Fan, "Survey of research on access control model," *Application research of Computer*, pp.9-11, 2005.
- [10] Tang zhuo, Zhao Lin, Li Kenli, and Li Ruixuan, "A dynamic access control model for inter-operation in multi-domain environment based on risk," *Journal of Computer Research and Development*, 46(6), pp.948-955, 2009.
- [11] IEEE, editor. *IEEE Security and Privacy, volume 3 of Economics of Information Security*. IEEE Computer Society, 2005.
- [12] LIN C, and VARADHARAJAN v, "Trust based risk management for distributed system security—a new approach[A]," *Proceedings of the 1st International Conference On Availability, Reliability and Security (ARES'06)*, pp. 6-13, 2006.
- [13] Grandison T, and Sloman M, "A survey of trust in internet applications," *IEEE Communications Surveys*, 3(4), pp. 2-16, 2000.
- [14] ZHANG L, BRODSKY A, and JAJODIA A, "Toward information sharing: benefit and risk access control (BARAC)," *Proceedings of the 7th IEEE International Workshop on Policies for Distributed Systems and Networks(POLICY'06)*, pp. 45-53, 2006.
- [15] P.C.Cheng, P. Rohatgi, C.Keser, et al. "Fuzzy multi-level security: An experiment on quantified risk-adaptive access control", *IBM Research Report RC24190*, 2007.
- [16] (2011) LINGO User's Manual, <http://www.lindo.com>.