International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.321-328
http://dx.doi.org/10.14257/ijsia.2014.8.4.29

Research on the Security based on Utility Theory in Cloud Computing Environment

JieHui Ju[1,2], ZhongYou Wang [3*],WenJuan Li[4,6],WeiZheng Bao[5] and Ya Wang[7]

[1]*Zhejiang University of Science & Technology, Hangzhou 310023, China*
[2]*University of Colorado Boulder, Colorado 80309-0xxx, USA*
[3]*Zhejiang Communications Industry Services Co,Ltd.,Hangzhou 310050, China*
[4]*Key Lab of E-business Market Application Technology of Guangdong Province, Guangzhou 510320, China*
[5]*Surveying and Mapping Management Office, Jinhua Planning Bureau, Jinhua Zhejiang 321000, China*
[6]*Key Lab of E-Business, Hangzhou Normal University, Hangzhou 310036, China*
[7]*The Second Surveying and Mapping Institute of Zhejiang Province, Hangzhou 310012, China*
jjh1mail@163.com, 798026426@qq.com,iellie@163.com, wzbao1970@126.com, hzwywzwy@163.com

Abstract

This paper focuses on the research of optimizing the safety and utility, proposing safety policy optimized model in cloud computing environment based on stochastic programming theory, building mathematical models which are on the basis of ensured data security to enhance the users' utility, model analysis and optimization, and ultimately get the best optimized configuration of security policy in the cloud computing environment to guide the formulation and dynamic adjustment of access control policy in cloud computing environment, and to meet the users' requirements, such as response time, resources availability and other utility requirements.

Keywords: *Cloud Computing, Utility Theory, Security, Access Control, Policy Optimization, Security Analysis*

1. Introduction

Cloud computing is TCP/IP based high development and integrations of computer technologies such as fast micro processor, huge memory, high-speed network and reliable. Cloud Computing emerged as an effective reuse paradigm, where hardware and software resources are delivered as a service through Internet [1]. Nowadays, there are many commercial cloud service providers, offering various kinds of delivered services such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [2]. The cloud computing becomes the host issue in industry and academia with the rapid development of computer hardware and software. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode. It is based on the network and has the format of service for the consumer. The cloud computing system provides the service for the user and has the character of high scalability and reliability. The company must have confidence in the cloud computing if they want to store the private data in the cloud system [3]. Governance and security are crucial to

ISSN: 1738-9976 IJSIA

computing on the cloud, whether the cloud system is in firewall or not. The security of cloud computing is the key import problem in the development of cloud computing [4]. The traditional security mechanism cannot protect the cloud system entirely. The cloud computing application is no boundaries and mobility and can lead many new security problems. The main security problems include data security, user data privacy protection, cloud computing platform stability and cloud computing administration [5-7].

2. The Security Situation in the Cloud Computing Environment

As the representative of the technology revolution, the cloud computing has a great impact on the current information industry and application mode. The personal and business users needn't to learn the server side software and just achieve the wanted service by a few simple clicks on the friendly software windows. Many industrial companies realized the full utility for the invested IT resources by integrating the data centers.

The cloud computing means that the data is stored in the service providers that has a high commercial value such as the user information. And the security and privacy of information become more important. If the security problems happen, the stored data in cloud centers would be forgotten for a long period for individuals or enterprises that rely heavily on cloud computing. Cloud computing is a typical distributed environment which the resources and service are distributed in different service provider and the data owners are also distributed. The access control is required to access several different service providers. This is realized by the interaction operation between the different services. But the heterogeneity, autonomy and dynamism of the distributed environment make the whole cloud computing systems are not absolutely safe. And the cloud security is based on the user utility. Utility computing is a commercial mode that provides with the computing resources. Simply, the utility computing is a payment mode based on the usage amount of the resources. So the problem is discussed in this paper that how to bring the economic benefits to users by considering utility computing.

3. Dynamic Access Control Model based on the Certificate

In the cloud computing environment, there are three kinds of entities which are end user, service provider and data owner. The users request for the access of the cloud computing resources. And the service providers get the data owners that may come from different security domain according to the request from the users. This special organization structure and the dynamic and uncertainty of the environment result in that any access control model can't ensure the absolute safety in the interaction process.

The RBAC model is a classical traditional access control model. But the RBAC, the later ARBAC and GTRBAC models are often limited by the characteristic of host-center. These models can't distinguish the common users and the resource owners. This situation results in that the models are hard to adapt to subject-object relationship in the cloud environment. Since the amount of resources in cloud computing is huge, the resource data is required to divided into a lot of small data blocks. The traditional access control model can't involve the all entities in cloud computing. The CARBAC (Cloud Computing Administrative Role-Based Access Control) is proposed in this paper which is role access control management model based on certificate. This model is extension of the RBAC in cloud computing environment. The resources and application programs are accessed by the terminal users in this model. And CARBAC model supports the users' certificates, environment variables and access control strategy.

3.1 User access control management in cloud computing: when an access request is online, the access permission to resources would be checked by the system. If the users have the access permission, the access permission to corresponding resources can be achieved. Otherwise, the users should backup in the data owner side. The users firstly send access request to the data owners. After received by the data owners, the data owners would send the request permission to users. If the authentication information is true and latest, the owners return an encrypted certificate to users. The corresponding access permission will returned to user roles after the users send the encrypted certificate to the service providers. This process is shown in Figure 1.

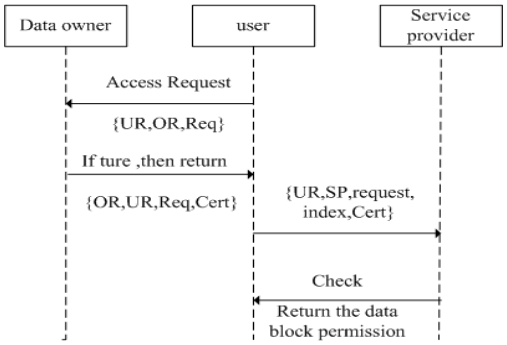

Figure 1. The Authorization Process of User Access Permission

Figure 1 describes the process of the user access permission in CARBAC model. The process can be divided into two parts that are {UR, OR, Req} and {UR, SP, P}. Among them, UR is the user role set. OR is the owner role set. And SP is the service provider. P represents the access rules. Req means the user access request set. And Req is shown in the following equation.

$$\text{Req} = \{UR, OR, ID, request, index, data\ block\ index, op\} \qquad (1)$$

3.2 Simulation experiments: The simulation experiment is based on CloudSim emulator. CloudSim is a kind of cloud computing simulation software which is proposed by the grid lab of Melbourne University in Australia and Gridbus program. It supports the modeling and simulation for the infrastructure of cloud computing. And it is a platform which also supports the data center, service agent and allocation strategy.

Table 1. The Simulation Parameters of TBDAC

Simulation parameter	value	Simulation parameter	value
α	0.8	m	578
σ_s	48	$SI_{eu,do}$	random
σ_U	76	$US_{eu,do}$	random
w_1	45	N_{eu}	random
w_2	55	N_{do}	random

This simulation experiments take TBDAC, ARTrust, EigenRep and PeerTrust into compare based on three different kinds of attack model which are simple malicious nodes, collusion fraud and complex strategy. And the successful transaction rate of the system is analyzed comparatively. The number of simulation nodes is 1000. Among them, the proportion of the simple malicious nodes is from 10% to 50%. The other parameters of the simulation are generated by the random number generator. And these parameters are shown in Table 1.

Among them, $SI_{eu,do}$ and $US_{eu,do}$ represent respectively the number of successful interaction and the number of the fail interaction between eu and do. And σ_s and σ_U are the weights of $SI_{eu,do}$ and $US_{eu,do}$ respectively. Similarly w_1 and w_2 are also the system coefficient.

According to the presentation of the network node, the nodes can be divided into two kinds. The first kind node is simple malicious node which only provides with unreal service. The other kind is collusion fraud node which collaborates with other malicious nodes, denigrates normal nodes and exaggerates the similar nodes. And the comparison of the successful transaction rate between the four modes under the attacking by the simple malicious is shown in Figure 2. The conclusion can be easily gotten that the successful transaction rate is highest with any proportion of the simple malicious nodes.

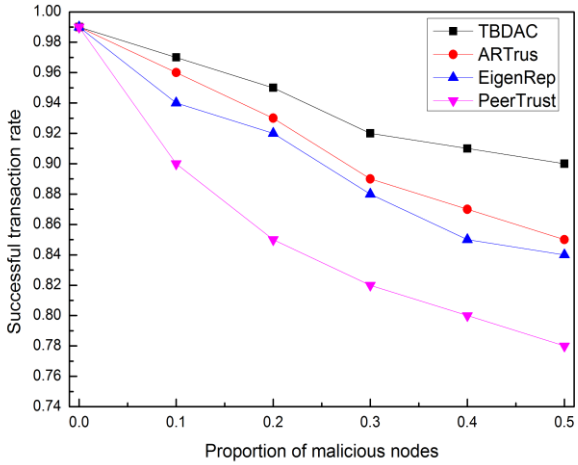

Figure 2. The Successful Transaction Rate under the Attacking by the simple Malicious Nodes

Similarly, the comparison is also diagramed under attacking by the collusion fraud nodes in Figure 3. From the two figures, TBDAC has larger advantage than the other three modes in the respect of the successful transaction rate.

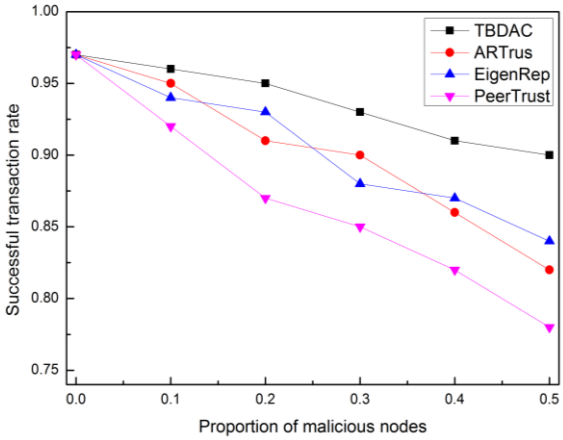

Figure 3. The Successful Transaction Rate under the Attacking by the Collusion Fraud Nodes

4. User Utility Analysis in Cloud Computing Environment based on Risk

User utility means the use value of resources for user which indicates the satisfaction degree is achieved after occupying, using or productively consuming some service. This mainly involves the user expense and the response time of the service request. According to the analysis of the user satisfaction degree, the user utility function in cloud computing environment can be achieved. This function shows the quantitative relation between the utility gotten from the cloud centers and the corresponding service portfolio.

4.1. The user utility function: In the cloud computing environment, the user security is the access risk without the permission in some degree. The expected utility function is proposed to define the degree of risk. This function is defined in a random variable collection. By using the utility function, several service portfolios can be analyzed. The expression is defined as follows. Among them, x, y and z respectively represent different kinds of service portfolios.

$$U = U(x, y, z, \cdots) \qquad (2)$$

Time utility is analyzed with the condition of the task completion rate 100% which means that the task can be completed in the limited time.

T_{U} is defined as the task collection in cloud center by user u. And $TE(T_U)$ is the total time budget of the task collection. $T_{com}(i, S_k)$ is the time that is spent on the service S_k in the task T_i. The time on the task collection T_{U} is also the longest time in the subtask T_i. So the user time utility function is shown in the following equation (3).

$$Ut(Tu) = \ln\left[1 + \frac{TE(Tu) - \max(T_{com}(i, S_k)}{1 + \left|TE(Tu) - \max(T_{com}(i, S_k)\right|}\right] \qquad (3)$$

In the equation (3), $\max(T_{com}(i, \mathrm{S_k}))$ presents the max time spent on the service S_k in the task T_i. And $\left|TE(T_U) - \max(T_{\mathrm{com}}(\mathrm{i}, \mathrm{S_k}))\right|$ means the distance between the subtask time budget and the real expense time.

4.2. Simulation analysis: With the fixed requirement and time budget, the task collection is divided into many subtasks. The research object is the impact on the time

utility with the change of the number x of the subtasks. The price of the unit service resources at the unit time is set c and the requirements of the users are set d which is the total number of basic subtasks needed to complete. The task d is divided into x subtasks T_i. The remaining subtasks which are divisible are equally distributed among the x subtasks to ensure the maximum time of the task execution is the minimal. The values of these variables are shown in Table 2.

Table 2. The Variable Value in the Time Utility Simulation

variable	d	c	x	$TE(T_U)$
value	100	1	1~100	10

The simulation result is illustrated in Figure 4. With the fixed requirements that are involved 100 subtasks, the number x of the subtasks is less than 10, $U_t(T_u)$ is less than zero. When x is 10 or 11, $U_t(T_u)$ is zero. And when x is more than 10, $U_t(T_u)$ is over zero. According to the expression of the time utility function, the closer the value of $U_t(T_u)$ is to zero, the better the time utility is. So the time utility is the best when x is set 10 or 11.

5. Conclusion

The paper has presented a new mentality and method for balancing and optimizing resource security and user utility in cloud computing environment, proceeded in-depth research in correlation theory of security policy optimal model in cloud computing environment, solved some scientific problems of cloud computing safety, such as modeling analysis of user access policy security and utility property in cloud computing environment, safety optimalization and verification of access control policy of service process and so on. The outcomes can optimize user utility and resource security in cloud computing center in addition they have significant theoretical significance for the development of access control theory in cloud computing environment.

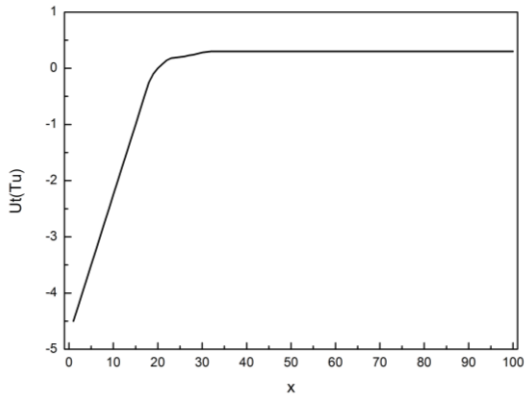

Figure 4. The Time Utility Simulation Result with Fixed Requirements

Acknowledgements

This work is supported by the Scientific Research Fund of Zhejiang Provincial Education Department (No.Y201223199), the open fund for Key Lab of Visual Media Intelligence Handles Technology of Zhejiang Province (NO.2012017), the Natural Science Fund of Zhejiang Province (NO.LQ12G02016,LQ12F02006), the open fund for Key Lab of E-business Market Application Technology of Guangdong Province (2011GDECOF07).

References

[1] D. Kondo, B. Javadi, P. Malecot, F. Cappello and D. Anderson, "Cost-Benefit Analysis of Cloud Computing versus Desktop Grids," Proc. IEEE Int. Symp. on Parallel & Distributed Processing (IPDPS09), IEEE Comp. Soc. Washington, **(2009)** May, pp. 1-12.
[2] A. Dastjerdi and R. Buyya, "A Taxonomy of QoS Management and Service Selection Methodologies for Cloud Computing", Cloud Computing: Methodology, Systems and Applications, L. Wang, R. Ranjan, J. Chen and B. Benatallah (eds), CRC Press, Boca Raton, FL, USA, **(2011)** October.
[3] J. Dean and S. Ghemawat, "Map Reduce: simplified data processing on large clusters", Communication of ACM 51, vol. 1, **(2008)** January, pp. 107-113.
[4] L. Chunlin and L. Layuan, "QoS based resource scheduling by computational economy in computational grid," Information Processing Letters, vol. 98, issue 3, **(2006)** May.
[5] K. Xiong and H. Perros, "Service Performance and Analysis in Cloud Computing," Proc. 2009 Congress on Services – I (SERVICES09), IEEE Computer Society Washington, **(2009)**, pp. 693-700.
[6] W. Jiyi, Z. Jianlin, W. Tong and S. Qianli", Study on Redundant Strategies in Peer to Peer Cloud Storage Systems", Applied Mathematics & Information Sciences, vol. 5, no. 2, **(2011),** pp. 235S-242S.
[7] W. Ji-yi, F. Jian-qing, P. Ling-di and X. Qi, "Study on the P2P Cloud Storage System", Acta Electronica Sinica, vol. 39, no. 5, **(2011),** pp. 1100-1107.

Authors

Jiehui JU, she is a Lecturer at the Zhejiang University of Science and Technology. Currently, she is also a visiting scholar of the University of Colorado Boulder in America (from May 10, 2013 to Jun 5, 2014). Her research interests include Cloud Computing, Data Mining.

ZhongYou WANG, he is the deputy director at Technology R & D Center of Zhejiang Communications Industry Services Co, Ltd. He received Master's Degree in computer science in 2009 at Hangzhou Dianzi University. His research interests include service trust and security, software engineering.

WenJuan LI, she was born in 1978. She is a lecturer at Hangzhou Normal University. She received PhD degree in 2011 from Zhejiang University, Hangzhou China, in computer science. Her research interests include cloud computing, trust and reputation. She has published more than 10 journal articles indexed by SCI, EI.

WeiZheng BAO, he was born in 1970. He is a senior engineer and director of surveying and mapping management office, Jinhua Planning Bureau, Zhejiang Province, China. His research interests include cloud computing and digital city.

Ya WANG, she was born in 1973. She is a senior engineer of surveying and mapping, the second surveying and mapping institute of Zhejiang Province. Her research interests include cloud computing, cadastre and virtual reality.