ICIC Express Letters
Volume **10**, Number **4**, April **2016**

ICIC International ©2016 ISSN 1881-803X
pp. 813–818

A NOVEL DECISION-MAKING MECHANISM FOR CLOUD COMPUTING ENVIRONMENTS

Xu Wu[1] and Feng Li[2]

[1]School of Computer Science
Xi'an University of Posts and Telecommunications
Weiguo Road, Chang'an District, Xi'an 710121, P. R. China
xrdz2006@163.com

[2]School of Engineering and Technology
Indiana University-Purdue University Indianapolis
420 University Blvd., Indianapolis 46202, USA
fengli@iupui.edu

Received October 2015; accepted January 2016

Abstract. *Cloud computing is presently operating under its expected capacity, mainly because of the scarcity of trust between data owners and storage service providers. Therefore, establishing trust for cloud customers and providers has become an important issue in cloud computing environment. We present a novel decision-making mechanism for developing an effective trust management that assists cloud entities (cloud users and cloud service providers) to make good trust decisions. The main idea of our mechanism is to use utility function to express the relationship between benefits and costs of entities, and then make the decision based on expected utility as well as risk attitude in a fully distributed fashion. The unique feature of our mechanism is that it not only helps an entity to select its partners, but also mitigates vulnerabilities in trust-based mechanisms. Through analysis and experiments, we believe our approach is useful for participants to make the decision regarding who to interact with. In addition, it is also a good starting point for exploring tradeoffs among risk, trust and utility.*

Keywords: Trust, Cloud computing, Risk, Decision model, Utility

1. **Introduction.** Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. However, a lack of trust between cloud customers and providers has hindered the universal acceptance of clouds as an increasingly popular approach for the processing of large data sets and computationally expensive programs. In this paper, we propose a novel decision-making mechanism for cloud computing environments based on game theory and relevant trust mechanisms in which the element of trust and risk are incorporated into a single model. The main idea of our mechanism is to use utility function to express the relationship between benefits and costs of entities, and then make the decision based on expected utility as well as risk attitude in a fully distributed fashion. Our mechanism using game theory to model risk provides better protection from malicious service providers, and defines the behavior of entity in cloud computing environments by introducing utility function. The utility function takes into consideration the costs and benefits as perceived by each entity by being connected to the cloud computing system and particular events that occur within the system. The aim of incorporating the element of trust and risk into a single model is to improve security in cloud computing environments. The unique feature of our mechanism is that it not only helps an entity to make a decision, but also mitigates vulnerabilities in

trust-based security that is listed above. This paper is organized as follows. Section 2 describes related work. In Section 3, the proposed decision-making mechanism is discussed. Section 4 describes the test scenario and simulation results. Finally, we conclude with a summary of our results and directions for new research in Section 5.

2. Related Work.

In [2] a distributed reputation based trust management system is presented for hybrid cloud computing system. Trust value storage is distributed at the levels of the clouds in the system, which enables each cloud to make independent local decision for selection about trustworthiness of a cloud. In order to solve privacy and security problems in the IaaS service layer, a model of trustworthy cloud computing which provides a closed execution environment for the confidential execution of virtual machines was proposed [3]. This work has shown how the problem can be solved using a Trusted Platform Module. Yang et al. [4] propose a collaborative trust model for firewalls in cloud computing. A model of domain trust is employed. Trust is measured by a trust value that depends on the entity's context and historical behavior, and is not fixed. Hada et al. [5] propose a trust model for cloud architecture which uses mobile agent as security agents to acquire useful information from the virtual machine which the user and service provider can utilize to keep track of privacy of their data and virtual machines. Edna et al. [6] presented an overview of the cloud computing paradigm, as well as its main features, architectures and deployment models. Moreover, they identified the main issues related to trust and security in cloud computing environments. In order to address these issues, they proposed a trust model to ensure reliable exchange of files among cloud users in public clouds. Li et al. [7] introduced a multitenancy trusted computing environment model (MTCEM). This model was designed for the IaaS layer with the goal of ensuring a trustworthy cloud computing environment to users. Pawar et al. [8] propose an uncertainty model and define an approach to compute opinion for cloud service providers. In [9], the authors propose Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE). The simulation results reveal that DaSCE can be effectively used for security of outsourced data by employing key management, access control, and file assured deletion.

However, considering only trust is inadequate when a decision is to be made in order to identify the best set of peers to utilize. Trust and risk have intrinsic relationship, i.e., trust is only meaningful in a risky situation. In the current literature, few trust models proposed taking risk into consideration. In fact, higher risk brings lower success rate of interaction. In this paper, we agree with such a viewpoint, that is to say, risk is one of the important factors that affect the decision making process.

3. The Main Idea of Our Mechanism.

The main idea of our mechanism is that we use utility function to express the relationship between benefits and costs as perceived by each entity by being connected to the cloud computing system and particular events that occur within the system, and then make the interaction decision based on expected utility as well as risk attitude. In traditional Expected Utility theory, the shape of utility function determines the type of personal risk attitude. Utility U_i is related to the personal risk attitude, and it can be defined as

$$U_i = \theta(Benifit - Cost)^{\frac{1}{\theta}} \tag{1}$$

in which the θ value is altered according to the types of personal risk attitude.

$$\theta = \begin{cases} 1 < \theta \leq 2, & \text{if peer } C_i \text{ is risk seeking} \\ 1, & \text{if peer } C_i \text{ is risk neutral} \\ 0 < \theta < 1, & \text{if peer } C_i \text{ is risk averse} \end{cases}$$

We can observe that entity C_i's risk attitude will change the value of utility. Compared to other types of risk attitude, risk seeking entities will tend to expand the utility more.

On the other hand, risk averse entities prefer to reduce some utilities to avoid risk. U_i shows the relationship between benefits and costs as perceived by each entity by being connected to the cloud computing system and particular events that occur within the system. Benefit is the payoff of entity which is gained in a cloud computing system. It is expressed as

$$Benefit = GoodBenefit + MaliciousBenefit \tag{2}$$

Good benefit captures the benefit gained by legitimate participation in a cloud computing system. Malicious benefit captures the benefit gained from acting maliciously. Cost is the expense of entity which is paid in a cloud computing system. It is denoted as

$$Cost = GoodCost + MaliciousCost + CasualtyCost + FoundCost \tag{3}$$

Good cost is the cost of participating in the system. Malicious costs are costs associated with malicious actions, and include bandwidth costs or processing costs. The Casualty cost is a relation that captures the negative effect on a participant when it becomes the casualty of an attack. It allows us to describe an entity's aversion to being attacked and plays a large role in determining how much effort should go into avoiding attacks or whether to participate in a system at all. Also included in the cost is Found cost which is the cost of an attacker being discovered (which may take the form of having to exit and re-enter the system or even just a decrease in available participants to attack). In game theory, the usage of expected utility enables entities to estimate the probability of winning the game. Based on this nature, we introduce the concept of expected utility in cloud computing environments. EU_i denotes the Von Neumann-Morgenstern Expected Utility for entity C_i. For the uncertainty of interacting, the expected utility EU_i of entity C_i is expressed as

$$EU_i = p * U_i - (1-p) * U_i = p * \theta(Benifit - U_i Cost)^{\frac{1}{\theta}} - (1-p) * \theta(Benifit - Cost)^{\frac{1}{\theta}} \tag{4}$$

where U_i is entity C_i's utility, and p is expressed as the probability. We consider that the probability, p, of getting the interaction for the entity C_i is actually reflected by its trustworthiness. Based on this, the trustworthiness of entity can be incorporated into Formula (4). We get

$$EU_i = T_i * U_i - (1-T_i) * U_i = T_i * \theta(Benifit - U_i Cost)^{\frac{1}{\theta}} - (1-T_i) * \theta(Benifit - Cost)^{\frac{1}{\theta}} \tag{5}$$

The trustworthiness of an entity can be derived from its reputation, which is denoted as R_i. The reputation is gotten based on its own experiences or a trust management system. Our decision model can incorporate different methods to computer reputation. The trustworthiness of an entity can be expressed as

$$T_i = \frac{1}{n} \sum_{r=1}^{n} R_i \tag{6}$$

where n denotes the total number of interactions that entity has conducted.

An entity will make an interaction decision based on (5) and its risk attitude if it has knowledge or correct knowledge of the entity who provides the cloud service in a trust management system, or else it will make the decision based on (1) and its risk attitude. A simplified overview of our decision model expresses the relationships and main determinant factors that affect the decision making process in cloud computing environments as shown in Figure 1.

The risk averse entities prefer to have more protection than the profit. Thus, they will always interact with the entities with the maximum expected utility among the trusted ones only. The risk neutral entities take a balance between two requirements. As a result, they always trade with the entities with maximum expected utility. Yet, risk seeking

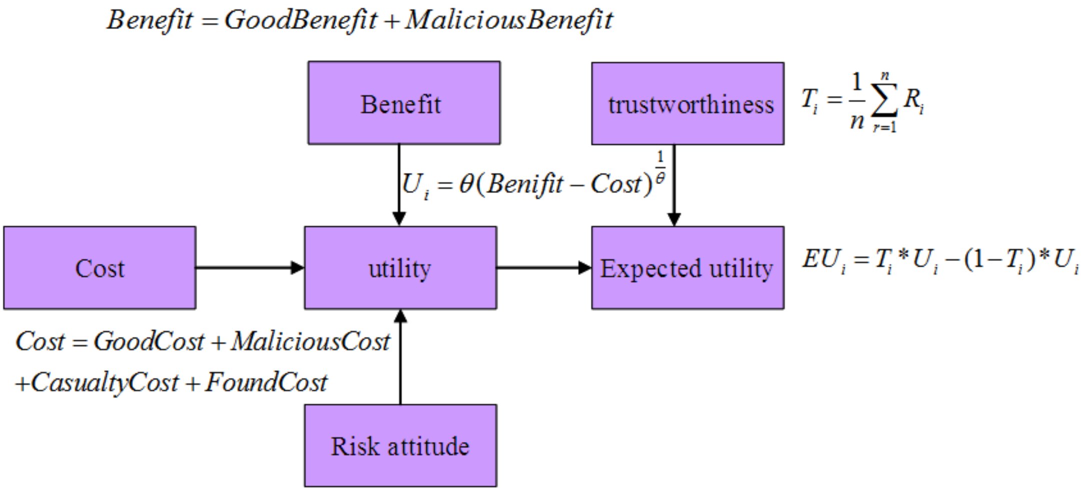
$Benefit = GoodBenefit + MaliciousBenefit$
Benefit
trustworthiness
$T_i = \frac{1}{n}\sum_{r=1}^{n} R_i$
$U_i = \theta(Benifit - Cost)^{\frac{1}{\theta}}$
Cost
utility
Expected utility
$EU_i = T_i * U_i - (1 - T_i) * U_i$
$Cost = GoodCost + MaliciousCost$
$+ CasualtyCost + FoundCost$
Risk attitude

FIGURE 1. Simplified overview of the decision model

entities only focus on the utility gained. As a result, they always interact with the entities with the maximum utility regardless of their trustworthiness. In this case,

$$EU_i = U_i \tag{7}$$

That is to say, for risk seeking participants, the service providers with a high degree of trustworthiness and the deceitful service providers will have an equal interaction chance. Equation (7) shows that trustworthiness becomes meaningless while computing EU_i. After interacting is finished, the entities will use (7) to update the trust value of interaction partners.

4. **Experiment Study.** In the first experiment we evaluate the mechanism in terms of the interacting success rate of participants with different risk attitudes. Through experiments, we can see that during interacting, risk averse entities have the highest success rate (33%), risk seeking entities have the lowest success rate (19%) and risk neutral entities are in the middle (26%). The experimental result expresses that the proposed mechanism can provide entities with more flexibility in the decision-making process, e.g., entities may decrease their benefits to get interaction chance. It is shown in Figure 2. The second experiment shows how risk affects the changes of trustworthiness. As shown in Figures 3, 4 and 5, entities start with a trustworthiness value of 0.5. In Figure 3, risk averse entities build up the trustworthiness by sacrificing part of the benefit due to the nature of personal

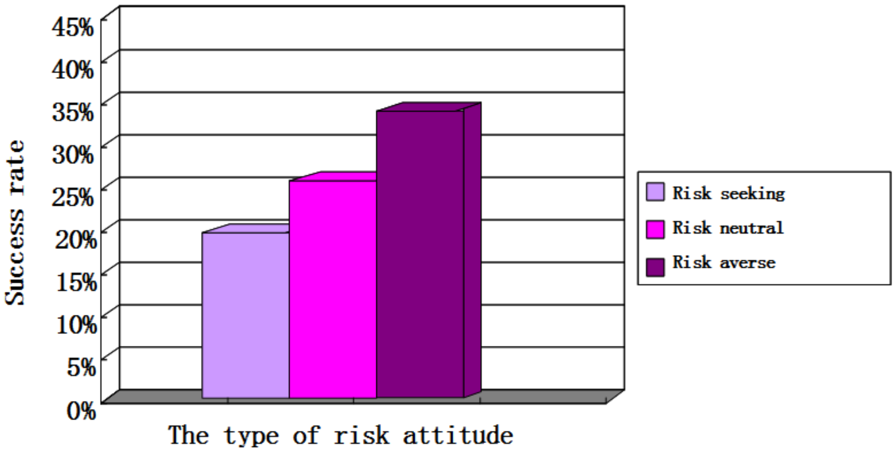

FIGURE 2. The result of success rate

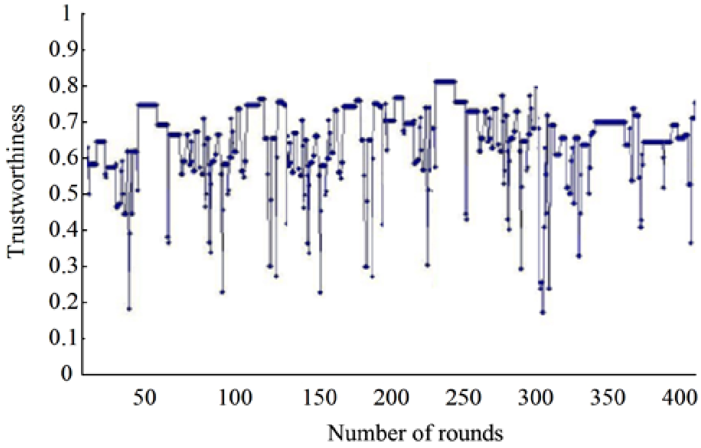

Figure 3. Simulation results of entities with risk averse attitude

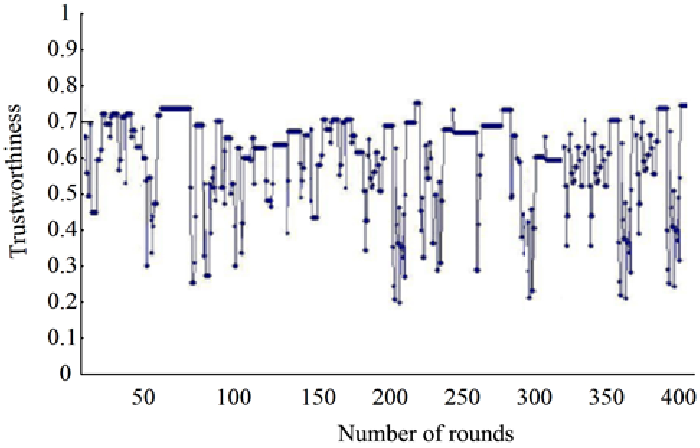

Figure 4. Simulation results of entities with risk neutral attitude

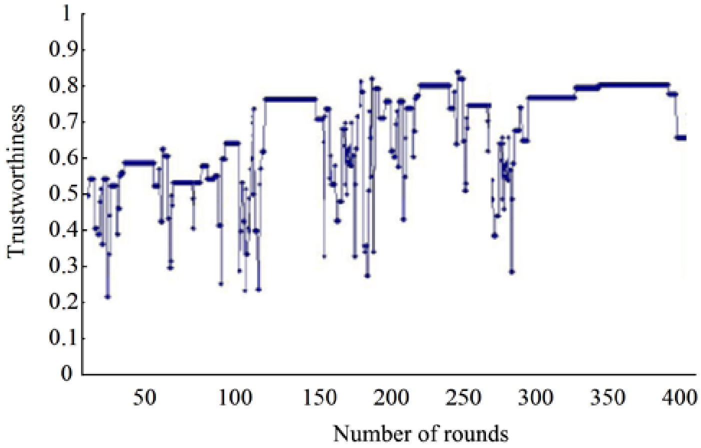

Figure 5. Simulation results of entities with risk seeking attitude

risk attitude. In this sense, risk averse entities with poor trustworthiness will have chance to build up the trust. The same findings can be found in other entities with different risk attitudes, Figures 4 and 5. This finding contradicts the traditional trust-based mechanisms where entities only interact with those that are known to be trustworthy. Since entities now consider the risk in partner selection, an entity with a low trustworthiness can make sacrifices of its benefit to get the chance of dealing with other entities. In the case the entity would not find it beneficial to attack the other entity based on our decision mechanism, so the malicious behavior of entities is restrained in a certain degree. In addition, entities can interact with more than one entity in each round; therefore, it is normal to see that there are some "big jump" from high trustworthiness to low trustworthiness in Figures 3, 4 and 5.

5. **Conclusions.** In this paper we propose a novel decision mechanism, and analyze its usefulness based on utility functions of cloud entities (cloud users and cloud service providers). The proposed unique approach is applicable to cloud computing system where entities roam into uncertain and unfamiliar environments. Our mechanism can be implemented individually without the cooperation of other entities in a system. As a result, it mitigates the problems inherent and often unaddressed by trust-based mechanisms. Furthermore, the proposed mechanism can provide participants with more flexibility in the decision-making process, e.g., service providers may decrease their benefits to get interaction chance. We also discussed in this paper that entities with different personal risk attitudes can make decisions differently. In the near future, we would like to test our mechanism into more real cloud computing environments and analyze the system performances.

Acknowledgment. The work in this paper has been supported by National Natural Science Foundation of China (Program No. 71501156) and China Postdoctoral Science Foundation (Program No. 2014M560796) and Shaanxi Provincial Education Department (Program No. 15JK1656).

REFERENCES

[1] M. A. Imad and L. John, Challenges for provenance in cloud computing, *Proc. of the 3rd USENIX Workshop on the Theory and Practice of Provenance*, pp.1-6, 2011.

[2] N. Santos, K. Gummadi and R. Rodrigues, Towards trusted cloud computing, *Proc. of HotCloud*, 2009.

[3] H. Wang and L. Huang, An improved trusted cloud computing platform model based on DAA and privacy CA scheme, *Proc. of the IEEE International Conference on Computer Application and System Modeling*, 2010.

[4] Z. Yang, L. Qiao, C. Liu, C. Yang and G. Wan, A collaborative trust model of firewall-through based on cloud computing, *Proc. of the 14th International Conference on Computer Supported Cooperative Work in Design*, Shanghai, China, pp.329-334, 2010.

[5] P. S. Hada, R. Singh and M. M. Meghwal, Security agents: A mobile agent based trust model for cloud computing, *International Journal of Computer Applications*, pp.12-15, 2011.

[6] D. C. Edna, O. A. Robson and T. S. J. Rafael, Trust model for file sharing in cloud computing, *Proc.of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization*, pp.66-73, 2011.

[7] X. Li, L. Zhou, Y. Shi and Y. Guo, A trusted computing environment model in cloud architecture, *Proc. of the 9th International Conference on Machine Learning and Cybernetics*, pp.11-14, 2010.

[8] P. S. Pawar, M. Rajarajan, S. K. Nair and A. Zisman, Trust model for optimized cloud services, *Proc. of the 6th IFTP International Conference on Trust Management*, pp.99-112, 2012.

[9] M. Ali, S. U. R. Malik and S. U. Khan, DaSCE: Data security for cloud environment with semi-trusted third party, *IEEE Trans. Cloud Computing*, pp.1-13, 2015.