Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 17 (2013) 1170 – 1177

Procedia Computer Science

Information Technology and Quantitative Management (ITQM2013)

A trust evaluation model for cloud computing

Xiaonian Wu[a,*], Runlian Zhang[a], Bing Zeng[b], Shengyuan Zhou[a]

[a]*School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China*
[b]*Science and Technology on Communication Security Laboratory, Chengdu 610041, China*

Abstract

Trust has attracted extensive attention in social science and computer science as a solution to enhance the security of the system. This paper proposes a trust evaluation model based on D-S evidence theory and sliding windows for cloud computing. The timeliness of the interaction evidence as the first-hand evidence is reflected by introducing sliding windows. The direct trust of entities is computed based on the interaction evidence by D-S evidence theory. The conflict of the recommendation trust as the second-hand evidence is eliminated with a help of an improved fusion approach as far as possible. Finally, the combination of the recommendation trust exposes the credibility of entities. Experimental results show that the proposed model is effective and extensible.

Selection and peer-review under responsibility of the organizers of the 2013 International Conference on Information Technology and Quantitative Management

Keywords: Cloud computing; Trust evaluation; Evidence theory; Sliding windows

1. Introduction

Cloud computing [1,2] is an emerging information technology that changes the way IT architectural solutions. It is a new pattern of business computing, and it can dynamically provide computing services supported by state-of-the-art data centers that usually employ Virtual Machine (VM) technologies. One of the most critical issues in cloud computing is security [3].

The trust mechanism provides a good way for improving the system security. It is a new and emerging security mode to provide security states, access control, reliability and policies for decision making by identifying and distributing the malicious entities based on converting and extracting the detected results from security mechanisms in different systems and collecting feedback assessments continually. In recent years, many scholars have made a lot of research on trust model. Hwang et al. [4] assessed the security demands of

* Corresponding author. Tel.: +86-13077658295
E-mail address: xnwu@guet.edu.cn.

Selection and peer-review under responsibility of the organizers of the 2013 International Conference on Information Technology and Quantitative Management
doi:10.1016/j.procs.2013.05.149

three cloud service models: IaaS, PaaS and SaaS. Integrated cloud architecture was presented to reinforce the security and privacy in cloud applications. Some security protection mechanisms were suggested, such as fine-gain access control, trust delegation and negotiation, reputation system of resource sites. Zissis et al. [5] pointed out that security in a cloud environment requires a systemic point of view, from which security will be constructed on trust, mitigating protection to a trusted third party. Takabi et al. [6] illustrated the unique issues of cloud computing that exacerbate security and privacy challenges in clouds. Various approaches to address these challenges were discussed. It explores the future work needed to provide a trustworthy cloud computing environment. Tian et al. [7,8] put forward basic criteria about evaluating node behavior trust and evaluation strategy in the cloud computing. Based on the basic criteria of the evaluation, the sliding window was used to carry out the evaluation of node behavior trust. Then a kind of evaluation mechanism on node behavior trust based on sliding windows model was brought forward. Jiang et al. [9] proposed a new evidential trust model for open distributed systems. This model was based on an improved D-S evidence theory by the introduction of time efficiency factor calculation function and the modification of D-S combination rules. It is highly effective in defending attacks on the system for malicious behaviors.

In this paper, we propose a trust evaluation model based on D-S evidence theory and sliding windows to evaluate the credibility of entities and detect the malicious entities for cloud computing. In our model, direct interactions among entities are regard as first-hand evidences. We evaluate the timeliness of the interaction evidence by means of sliding windows. Trust computing of entities is based on D-S theory with the help of the interaction evidences. Recommendation trust values from different entities are regard as second-hand evidences. The combination of the recommendation trust values forms the reputation of entities. Finally, experiments were carried out to estimate the effectiveness and the anti-attack of the proposed model.

The remainder of this paper is organized as follows. Section 2 describes the proposed trust evaluation model. In section 3, the experimental results are shown and discussed. Finally, section 4 provides the conclusion and mentions our future research directions.

2. Trust Evaluation Model

The entities are divided into Cloud Server Provider (CSP) and Cloud User (CU) in cloud computing. Trust evaluation depends on interactions evidences between the CSP and the CU. The interaction evidence is dynamic. And it has fine timeliness. Below we present our trust evaluation model.

2.1. The timeliness of interaction evidence and sliding window

In cloud computing, CUs send service requests to CSPs, and then CSPs provide the corresponding services for CUs. Entities rate each other after each interaction, as in the E-commerce System. Here, we don't consider the cooperation among CSPs and among CUs. For trust evaluating, the interaction and assessment between CSPs and CUs are evidence information.

In this paper, the evidence set E is defined as follows.

$$E = \{E_1, E_2, \cdots, E_i, \cdots, E_k\}$$

Where, $k \in N$, N is a natural number. $E_i (1 \le i \le k)$ is defined by 5-tuple.

$$E_i = \{time, cspid, cuid, csp\_eva, cu\_eva\}$$

Where, each attribute of evidence E_i is described as follows:

(1) *time* is the emerging time of evidence E_i .

(2) *cspid* is ID of the CSP. It is unique.

(3) *cuid* is ID of the CU. It is unique also.

(4) *csp_eva* is the assessment of the CU to the CSP. The CSP maybe provide good service or denial of service. If the CU is satisfied with services of the CSP, this interaction is positive. So *csp_eva* is 1. Otherwise, if services of the CSP are negative, *csp_eva* is -1. If the CU is unsure for services of the CSP, *csp_eva* is 0.

(5) *cu_eva* is the assessment of the CSP to the CU. The CU's behavior may be normal or fraud. If the CU carries out normal or positive interaction, *cu_eva* is 1; otherwise, if the CU carries out fraud or negative interaction, *cu_eva* is -1. If the system can not decide whether it is normal or fraud for the CU's behavior, *cu_eva* is 0.

The interaction evidence would keep on increasing with the realization of interactions by time. And it is basis for trust computing. In addition, the importance of evidence information would decay over time. The importance of negative evidence would decay more slowly than positive evidence. In order to evaluate reasonably trust of entities based on the evidence information, we employ sliding windows to describe the timeliness of evidence information.

The direct interaction is divided into three categories: positive interaction, negative interaction and uncertain interaction. Accordingly, we set three time windows: positive interaction window(*Wp*), negative interaction window(*Wn*) and uncertain interaction window(*Wu*). *Wp* is used to sift the positive interaction evidence. *Wn* is used to sift the negative interaction evidence. *Wu* is used to sift the uncertain interaction evidence. Sliding window mechanism is shown in Fig 1.

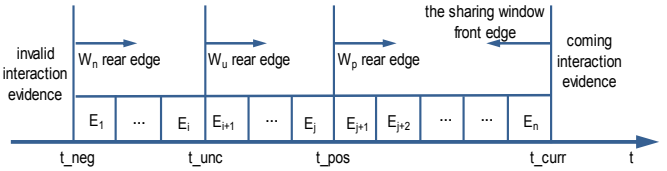


Fig. 1. Sliding window mechanism

Here, t_curr expresses the current time; t_pos, t_neg and t_unc are the critical time. Separately, we denote every time window size as S_p, S_n and S_u($S_p \le S_u \le S_n$) for *Wp* ,*Wn* and *Wu*. There exists follow quantitative relationship:

$$\begin{cases} |t\_curr - t\_pos| = S_p \\ |t\_curr - t\_unc| = S_u \\ |t\_curr - t\_neg| = S_n \end{cases} \quad (1)$$

After introducing Sliding windows, the interaction evidences only inside the windows are valid. Supposed there is positive interaction evidence E_k at time t. If $|t\_curr - t| \le S_p$, E_k is valid; otherwise, it is invalid. This is similar for negative and uncertain interaction evidence. In the process of trust computing, only valid interaction evidences affect the trust degree of entities. In this way, the trust degree of entities would not be increased or decreased by over-ranging interaction evidence. In addition, negative interaction window is bigger than positive interaction window. So negative interaction evidences can affect the trust of entities for longer time. It is in keeping with law of nature.

2.2. Direct Trust

Each interaction is considered as evidence. By querying the evidence set *E*, we can count up the number of valid interactions in time windows. Suppose that positive interaction evidence is marked as α , negative interaction evidence is β , and uncertain interaction evidence is γ . At time *t*, the number of every kind of valid direct interaction between entity *i* and entity *j* can be marked as $\alpha_{i,j}^t$, $\beta_{i,j}^t$, and $\gamma_{i,j}^t$. In $t = t_0$, there is

no interaction between entity *i* and entity *j*, so $\alpha_{i,j}^0 = \beta_{i,j}^0 = \gamma_{i,j}^0 = 0$. Direct trust between entity *i* and entity *j* is computed by direct interactions. Here, we compute direct trust between entities using D-S evidence theory, because D-S evidence theory can express the uncertainty of practical problems with a probability range.

We set the trust distinguish framework $\Omega = \{T, -T\}$, so $2^\Omega = \{f, \{T\}, \{-T\}, \{T, -T\}\}$. Here, $\{T\}, \{-T\}, \{T, -T\}, f$ respectively represent trust, distrust, uncertain and impossibility. We denote the direct trust as dt. In time *t*, entity *i* evaluates the direct trust degree on the entity *j*, which is expressed as $dt_{i,j}^t = (dm_{i,j}^t(\{T\}), dm_{i,j}^t(\{-T\}), dm_{i,j}^t(\{T, -T\}))$.

Where, if $t = t_0$, $dt_{i,j}^0 = (0,0,1)$. And the BPA (basic probability assignment) function $dm_{i,j}^t(\{\cdot\})$ is defined as follows:

$$\begin{cases} dm_{i,j}^t(\{T\}) = u \times dm_{i,j}^{t-1}(\{T\}) + (1-u) \times \dfrac{\alpha_{i,j}^t}{\alpha_{i,j}^t + \beta_{i,j}^t + \gamma_{i,j}^t} \\ dm_{i,j}^t(\{-T\}) = u \times dm_{i,j}^{t-1}(\{-T\}) + (1-u) \times \dfrac{\beta_{i,j}^t}{\alpha_{i,j}^t + \beta_{i,j}^t + \gamma_{i,j}^t} \\ dm_{i,j}^t(\{T, -T\}) = 1 - dm_{i,j}^t(\{T\}) - dm_{i,j}^t(\{-T\}) \end{cases} \tag{2}$$

Here, $u \in [0,1]$ is a weight factor. After setting the sliding windows as Figure 2, interactions beyond the window size are regarded as invalid evidence. And the invalid evidence would not be cited in trust computing. However, the invalid evidence still is behavior of entities ever, and the effect of the invalid evidence can not be dispelled suddenly, but rather gradually. By introducing the weight factor u and $dm_{i,j}^{t-1}(\{\cdot\})$, the past interactions can affect the trust degree of entities to some extent. Of course, its effect will disappear gradually. We can control the influence of the past interactions by adjusting the weight factor *u*.

2.3. Reputation

The entity obtains the recommendation information from other entities which have ever interacted with the evaluated entity. If the entity has no direct interaction with the evaluated entity, its recommendation information will not be considered. And we do not consider recommendation's iteration. So it avoids large recommendation chains.

Suppose entity s has direct interaction with entity *j*. Entity *i* can gain the recommendation information about entity *j* from entity *s* according to direct trust from entity *s* to entity *j*, which is denoted as $rt_{s,j}^t = (rm_{s,j}^t(\{T\}), rm_{s,j}^t(\{-T\}), rm_{s,j}^t(\{T, -T\}))$. Here, $rm_{s,j}^t(\cdot)$ is the corresponding BPA function. And we take the direct trust value $dt_{s,j}^t$ as the recommendation trust value $rt_{s,j}^t$ for entity *i*, so $rt_{s,j}^t = dt_{s,j}^t$ and $rm_{s,j}^t(\cdot) = dm_{s,j}^t(\cdot)$.

In the trust network, there exists more than one recommendation information from different entities. Based on Dempster rule, we can combine these recommendations. However, the conclusion may be inconsistent with the evidence if there is serious conflict among recommendations. Referring to fusion approach for conflicting evidence in reference [9], we compute the weight of every recommendation, which is denoted as ω_s. According to ω_s, the BPA function $rm_{i,j}^t(\{\cdot\})$ of the recommendation trust $rt_{s,j}^t$ is revised as follows.

$$\begin{cases} rm_{s,j}^t(\{T\}) = \omega_s \times rm_{s,j}^t(\{T\}) = \omega_s \times dm_{s,j}^t(\{T\}) \\ rm_{s,j}^t(\{-T\}) = \omega_s \times rm_{s,j}^t(\{-T\}) = \omega_s \times dm_{s,j}^t(\{-T\}) \\ rm_{s,j}^t(\{T, -T\}) = 1 - rm_{s,j}^t(\{T\}) - rm_{s,j}^t(\{-T\}) \end{cases} \tag{3}$$

Finally, the combination of the all recommendation trusts form reputation of entities. Reputation of the entity j is represented by rt_j^t at time t. It is calculated as follows according to Dempster's rule.

$$rt_j^t(A) = rt_{1,j}^t(A) \oplus rt_{2,j}^t(A) \oplus \cdots \oplus rt_{q,j}^t(A), q = 1,2,\cdots,m; \quad A \neq f, A \in 2^{\Omega} \tag{4}$$

3. Experimental Evaluation

3.1. Simulation setup

To evaluate the performance of above model, we performed simulation experiments in Netlogo. In the simulation experiments, the CSPs and the CUs are independent.

The CSPs are classified into 3 types: good CSP, bad CSP and random CSP. Their respective proportions in all CSPs are 80%, 10% and 10%, and they provide different services are as follows.

(1) The good CSP always provides reliable services.
(2) The bad CSP always provides unreliable services.
(3) The random CSP provides reliable or unreliable services randomly.

The CUs are classified into 3 types: honest CU, malicious CU and random CU. The proportional distribution of each kind of the CUs is similar to the CSPs.

(1) The honest CU always takes legal actions.
(2) The malicious CU always takes illegal actions.
(3) The random CU takes legal or illegal actions randomly.

For all CSPs and CUs, the initial trust degree follows (0,0,1). This is to say, they are all unknown for the system at first. New interactions are continuously generated with an arrival rate 80 interaction per simulation-time step, between a random CSP and a random CU.

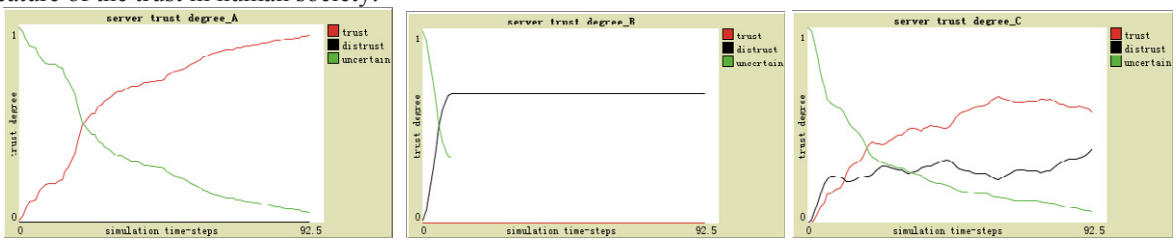
Table 1. Summarizes the parameters used in simulation experiments

Parameter	Description	value
n	number of CSPs	50
m	number of CUs	200
u	weight factor	0.2
S_p	positive interaction window size	50
S_u	uncertain interaction window size	80
S_n	negative interaction window size	150

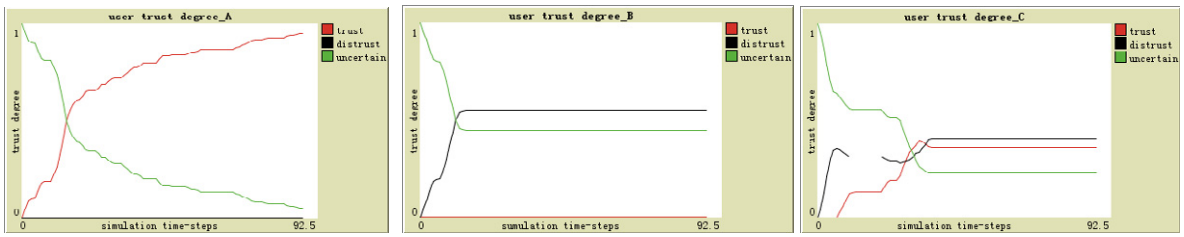
3.2. The effectiveness of proposed model

At first, we evaluate the effectiveness of our model. The experimental result is as follows. Fig 2 reveals the changing of the trust degree for three kinds of entities. The credibility of the good/honest entities continues to grow as the steady accumulation of positive interactions. On the contrary, the credibility of the bad/malicious entities decreases as negative interactions. And the trust degree of the malicious entities has no changing when the distrust degree reaches a certain degree. The reason is that the entities would be considered to be malicious if its distrust degree is greater than the assumed threshold value. The entities would not be permitted to interact with any other entities. So the trust degree of the malicious entities would not change any more. For random entities, the change in behavior results in the change of the credibility of random entities. Besides, we can notice that the credibility of entities increases slowly and the incredibility of entities increase quickly. This is contributed to the feature of sliding windows. In sliding window mechanism, positive interactions are valid for a short period of time and negative interactions are valid for a long period of time. So the credibility of entities can increase by recent positive interactions slowly. But early negative interactions continue to have bad effects

on the trust degree of entities so that the distrust degree of entities would increase quickly. It is accord with the feature of the trust in human society.



(a) the trust degree of the good CSP (b) the trust degree of the bad CSP (c) the trust degree of the random CSP



(d) the trust degree of the honest CU (e) the trust degree of the malicous CU (f) the trust degree of the random CU

Fig. 2. The changing of trust degree for different entities

3.3. Anti-attack of the system

Success interaction rate is the ratio of successful interactions to overall interactions in the simulation time. It can reflect the anti-attack of the system in a certain extent. Thus we measure anti-attack of the system by success interaction rate. With a help of the trust computing based on evidence theory and sliding windows, we can identify the malicious entities efficiently. Thank to it, we can restrict the interaction of malicious entities further. It can help to increase the success interaction rate of the system. The experiment results are shown in Fig 3. Results show that the success interaction rate with trust computing is higher than that without trust computing. From Figure 3, we can see that the changing of success interaction rate is divided into two stages: decline stage and rise stage. The success interaction rate declines with malicious interactions at the beginning. After a time, the success interaction rate keeps rising. It is because that the system with trust computing has begun to identify the malicious entities and refuse to provide service for them. The result shows that trust computing can enhance the anti-attack of the system because it can help to the system correctly identifying the malicious entities.

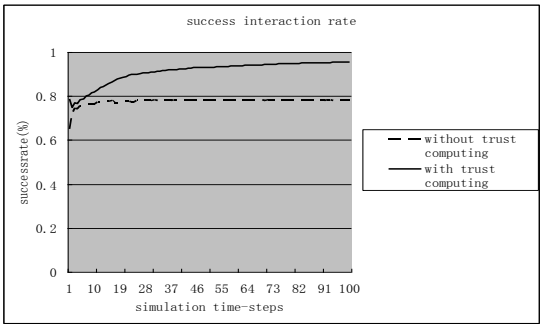


Fig. 3. Success interaction rate

4. Conclusions

Trust evaluation model is of importance to supporting system security. This paper has presented a trust evaluation model based on evidence theory and sliding windows for cloud computing. The proposed model has a number of advantages as follows. Firstly, it is simple to be executed. The time complexity of our algorithm is $O(n \times m)$ if there are n CSPs and m CUs in the system. Secondly, the timeliness of interactions is reflected by introducing sliding windows. In sliding window mechanism, interactions are divided into valid interactions and invalid interactions. Only valid interactions can affect the trust degree of entities. So it improved the extensibility of the system. Thirdly, the trust degree of entities changes dynamically according to the behavior of entities based on D-S evidence theory. We evaluate the trust of both the CSPs and the CUs. In this way, we can provide security protection for the CSPs and the CUs. Finally, it can help the system identifying malicious entities to some extent and improve the success interaction rate. It enhances the anti-attack of the system. Simulation experiments show that the trust degree of entities increases slowly and decreases quickly using our model. It can effectively identify malicious entities, and provide reliable information to correctly make the security decisions for the system. Future, we will look for ways to overcome the collusive deception behaviors. And the data mining and knowledge discovery method [10] will be combined with our trust evaluation model to evaluate the changes of CUs and CSPs.

Acknowledgements

The authors would like to thank the support by the Foundation of Science and Technology on Communication Security Laboratory (9140C110404110C1106), the GuangXi National Natural Science Foundation of China (2012GXNSFAA053224), the Guangxi Graduate Education Innovation project of China (2010105950810M18), and the Foundation of Guangxi Department of Education (201010LX156,CD10066X).

References

[1] M. Armbrust, et al., "A view of cloud computing," Communications of the ACM, 2010, 53, p. 50-58.
[2] R. Buyya, et al., "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, 2009, 25, p. 599-616.
[3] D.-G. Feng, et al., "Study on Cloud Computing security," Ruan Jian Xue Bao/Journal of Software, 2011, 22, p. 71-83.
[4] K. Hwang, et al., "Cloud security with virtualized defense and reputation-based trust management," in 8th IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2009, December 12, 2009 - December 14, 2009, Chengdu, China, 2009, p. 717-722.

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, 2012, 28, p. 583-592.
[6] H. Takabi, et al., "Security and privacy challenges in cloud computing environments," IEEE Security and Privacy, 2010, 8, p. 24-31.
[7] L.-Q. Tian, et al., "Node behavior trust evaluation based on behavior evidence in WSNs," in 2010 2nd International Conference on Future Computer and Communication, ICFCC 2010, May 21, 2010 - May 24, 2010, Wuhan, China, 2010, p. 1312-1317.
[8] L.-q. Tian, et al., "Evaluation of user behavior trust in cloud computing," in 2010 International Conference on Computer Application and System Modeling, ICCASM 2010, October 22, 2010 - October 24, 2010, Shanxi, Taiyuan, China, 2010, p. 7567-7572.
[9] L. Jiang, et al., "A new evidential trust model for open distributed systems," Expert Systems with Applications, 2012, 39, p. 3772-3782.
[10] Y. Peng, G. Kou, et al., "A Descriptive Framework for the Field of Data Mining and Knowledge Discovery," International Journal of Information Technology & Decision Making, 2008, 7, p. 639–682.