International Journal of Hybrid Information Technology
Vol.8, No.3 (2015), pp.177-184
http://dx.doi.org/10.14257/ijhit.2015.8.3.17

A New Trust Model in Cloud Computing Environments

Xu Wu[1, 2]

Department of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an, China
Department of Computer Science and Technology, Xian Jiaotong University, Xi'an, China
xrdz2005@163.com

Abstract

Trust management is fundamental to identify malicious, selfish and compromised nodes which have been authenticated. It has been widely studied in many network environments such as peer-to-peer networks, grid and pervasive computing and so on. In the paper, we propose a trust model (TM) based on fuzzy logic inferences, which can better handle uncertainty, fuzziness, and incomplete information in cloud trust reports. The experiments are performed in order to test the accuracy of the TM as compared to a data storage system where no trust model is implemented.

Keywords: *cloud computing, trust model, fuzzy logic*

1. Introduction

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. Trust is an important aspect in the design and analysis of secure distribution systems. It is also one of the most important concepts guiding decision-making. Trust is a critical part of the process by which relationships develop. It is a before-security issue in the ad hoc networks. By clarifying the trust relationship, it will be much easier to take proper security measures, and make correct decision on any security issues. Trust modeling is a technical approach to represent trust for digital processing. Recently, trust modeling is paid more and more attention in cloud computing. In the paper, we propose a trust model (TM) based on fuzzy logic inferences, which can better handle uncertainty, fuzziness, and incomplete information in cloud trust reports.

This paper is organized as follows. Section 2 describes related work. Section 3 gives details on the proposed model. Finally, we conclude with a summary of our results and directions for new research in Section 4.

2. Related Work

This section review some related work about security and trust in the cloud.

2.1. Security in the Cloud

Clouds are dynamic and heterogeneous and are structured in a fundamentally different way from other distributed systems, such as grids, and therefore present new problems for security. To date, there has been minimal research published on cloud computing security. Popovic, *et al.*, [1] discuss security issues, requirements and challenges that Cloud Service Providers (CSP) face during cloud engineering. Recommended security standards and management models to address these are suggested both for the technical and business community.

ISSN: 1738-9968 IJHIT

One of the fundamental problems with adopting cloud computing is providing not only security resources but also assurances that those resources are correctly implemented and maintained within the cloud. Therefore Bret, *et al.*, [2] attempt to provide a level of assurance by some security architectures and models. In this article, they also discuss the need for asking critical questions about the security implications of cloud computing. In the report titled Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, CSA provides its take on some of the security issues related to cloud computing [3]. In the report, security properties are described as essentially the same set of properties that a user expects to see with a self-hosted system. These include the usual: Identification/Authentication, Privacy, Integrity and Provision of Service.

Huan, *et al.*, [4] investigate the different security vulnerability assessment methods for cloud environments. Experiments show that more vulnerabilities are detected if vulnerable tools and servers are in the same LAN. In other word, the hackers can find an easier way to get the target information if it is on the same LAN of compromised systems. Experimental results can be used to analyze the risk in third party compute clouds.

2.1. Trust in the Cloud

Hwang, *et al.*, [5] distinguish among different *service-level agreements* (SLAs) by their variable degree of shared responsibility between cloud providers and users. Critical security issues include data integrity, user confidentiality, and trust among providers, individual users, and user groups. The three most popular cloud service models have varying security demands. SaaS demands all protection functions at all levels. At the other extreme, IaaS demands protection mainly at the networking, trusted computing, and compute/storage levels, whereas PaaS embodies the IaaS support plus additional protection at the resource-management level. In the paper, the authors suggest using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners.

In [6] a trusted cloud computing platform (TCCP) which enables IaaS providers to offer a closed box execution environment that guarantees confidential execution of guest virtual machines (VMs) is proposed. This system allows a customer to verify whether its computation will run securely, before requesting the service to launch a VM. TCCP assumes that there is a trusted coordinator hosted in a trustworthy external entity. The TCCP guarantees the confidentiality and the integrity of a user's VM, and allows a user to determine up front whether or not the IaaS enforces these properties.

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 [7]. This work has shown how the problem can be solved using a Trusted Platform Module. The proposed model, called Trusted Cloud Computing Platform (TCCP) is supposed to provide higher levels of reliability, availability and security. In this solution, there is a cluster node that acts as a Trusted Coordinator (TC). In the TCCP model, the private certification authority is involved in each transaction together with the TC.

Zhimin, *et al.*, [8] propose a collaborative trust model for firewalls in cloud computing. The model has three advantages: a) it uses different security policies for different domains; b) it considers the transaction contexts, historic data of entities and their influence in the dynamic measurement of the trust value; and c) the trust model is compatible with the firewall and does not break its local control policies. 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.

Edna, *et al.*, [9] 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. In our model, the trust value of a given node is obtained from a pool of simple parameters related to its suitability for performing storage operations. Nodes with greater trust values are subsequently chosen for further file storage operations.

Cloud service providers (CSP) should guarantee the services they offer, without violating users' privacy and confidentiality rights. Li, *et al.*, [10] 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. MTCEM has two hierarchical levels in the transitive trust model that supports separation of concerns between functionality and security. In MTCEM, the CSP and the users collaborate with each other to build and maintain a trustworthy cloud computing environment.

3. Trust Model

In the section, the trust mode is described in details. Firstly, the scenario is assumed. Without loss of generality, we will adopt the proposed trust model where some customers of the network request certain cloud service (and act, therefore, as clients) and some others provide those services (thus acting as cloud services providers). In such a scenario, a cloud provider could provide a service when this is requested. The trust model is used to select the most trustworthy cloud provider to provide the service for the customer.

3.1. Trust Computation

The steps of the trust model are presented in figure 1. Such steps are as follows.

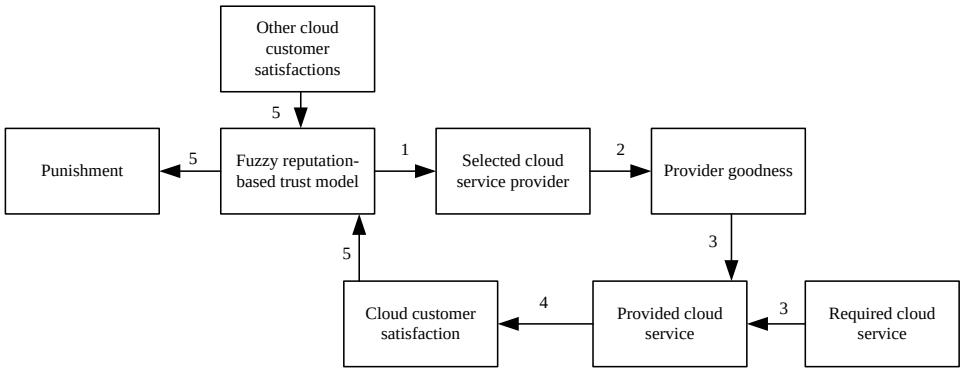

Figure 1. The Steps of the Trust Model

1) The trust model TM selects the cloud service provider to have an interaction with.
2) Such providers has a perceived certain goodness ('very low', 'low', 'medium', *etc.*).
3) According to the required cloud service attributes and the provider goodness, the cloud provider provides a service to the customer.
4) The customer satisfaction is assessed based on the provided service in the previous step.
5) Finally, the punishment level is determined by the customer satisfaction with the received service, together with and other cloud customer satisfactions.

We actually applied linguistic fuzzy sets and fuzzy logic in 1-5 steps.

Trust computing in our scheme has two major steps: trust evidences acquirement and trust aggregation. The trust evidences are considered as the input of the trust model. All evidences form a trust vector, $T=(t_1,t_2,t_3,...,t_n)$ which is the output of the trust model. All trust values are normalized with $\sum_i T_i = 1$, where $i=1,2,...n$ and n is a size of networks. The trust of a user is calculated by the weighted sum of the trust evidence received. In TM, the cloud customer performs fuzzy inference on perceived service properties to generate the customer satisfaction assessment. The local trust scores are computed by customer satisfactions. The fuzzy inference mechanism can capture some uncertainties and is self-adjusting. It can adaptively track the variation of perceived service properties, such as cost, price, quality, delivery time, and so on. The TM system aggregates local trust scores collected from all cloud customers to produce a global reputation for each cloud provider.

The most important problem is how to determine the aggregation weights. Analytic Hierarchy Process (AHP) is a combination of qualitative and quantitative analysis of multi-objective decision, which simplifies the complexity of problem analysis, and can test the consistency of the major Subjective mistakes. However, AHP also has strong disadvantage of subjectivity of depending on the expert's expertise. Weize Wang and Xinwang Liu [11] consider the *t*-norm and *t*-conorm as Einstein operations and develop the intuitionistic fuzzy Einstein weighted averaging ($IFWA^{\varepsilon}$) operator. In the paper, an AIFS (Atanassov's intuitionistic fuzzy set)-based algorithm is proposed to determine the aggregation weights.

Einstein product T_{ε} and Einstein sum S_{ε} are the basic t-norm and t-conorm, respectively, as follows:

$$T_{\varepsilon}(a,b)=\frac{a\cdot b}{1+(1-a)\cdot(1-b)}, \quad (1)$$

$$S_{\varepsilon}(a,b)=\frac{a+b}{1+a\cdot b}, \quad (2)$$

where $\forall(a,b)\in[0,1]^2$.

Einstein product T_{ε} is a prototypical example of the class of strict Archimedean t-norms, which is continuous, strictly monotone, and has the Archimedean property [12, 13]. Therefore, the Einstein product which typically gives the same smooth approximations as the algebraic product could be a good choice for the intersection of IFSs [11]. Equivalently, the Einstein sum S_{ε} could be used for the union of IFSs.

Let *t*-norm and *t*-conorm be Einstein product T_{ε} and Einstein sum S_{ε}, then the generalized intersection and union on two IFSs *A* and *B* become the Einstein product (denoted by $\otimes_{\varepsilon}$) and Einstein sum (denoted by $\oplus_{\varepsilon}$) as follows:

$$A\otimes_{\varepsilon} B=\{(x,T_{\varepsilon}(\mu_A(x),\mu_B(x)),S_{\varepsilon}(v_A(x),v_B(x)))\mid x\in X\} \quad (3)$$

$$A\oplus_{\varepsilon} B=\{(x,S_{\varepsilon}(\mu_A(x),\mu_B(x)),T_{\varepsilon}(v_A(x),v_B(x)))\mid x\in X\} \quad (4)$$

Based on (1) and (2), the intersection and union of two IFSs using Einstein operations in (3) and (4) can be established as follows:

$$A\otimes_{\varepsilon} B=\left\{\left(x,\frac{\mu_A(x)\cdot\mu_B(x)}{1+(1-\mu_A(x))\cdot(1-\mu_B(x))},\frac{v_A(x)+v_B(x)}{1+v_A(x)\cdot v_B(x)}\right)\mid x\in X\right\} \quad (5)$$

$$A \oplus_{\varepsilon} B = \left\{ \left(x, \frac{\mu_A(x) + \mu_B(x)}{1 + \mu_A(x) \cdot \mu_B(x)}, \frac{v_A(x) \cdot v_B(x)}{1 + (1 - v_A(x)) \cdot (1 - v_B(x))} \right) | x \in X \right\}$$

(6)

Weize Wang and Xinwang Liu [11] define the product (denoted by $\cdot_{\varepsilon}$) of the positive real number and an IFS.

Definition 1: λ is a positive real number and *A* is an IFS and the scalar multiplication operation $\lambda \cdot_{\varepsilon} A$ is defined as follows:

$$\lambda \cdot_{\varepsilon} A = \left\{ \left(x, \frac{[1 + \mu_A(x)]^{\lambda} - [1 - \mu_A(x)]^{\lambda}}{[1 + \mu_A(x)]^{\lambda} + [1 - \mu_A(x)]^{\lambda}}, \frac{2 \cdot [v_A(x)]^{\lambda}}{[2 - v_A(x)]^{\lambda} + [v_A(x)]^{\lambda}} \right) | x \in X \right\} \quad (7)$$

Deschrijver and Kerre [14] have proposed the concept of a complete lattice. A tradition relation on the lattice $(L, \leq_L)$, $L = \{(a,b) | a,b \in [0,1], a+b \leq 1\}$, defined by

$$(a,b) \leq_L (c,d) \Leftrightarrow a \leq c \text{ and } b \geq d,$$

has also been applied to the operations of IFSs [1,26].The top and bottom elements are $1_L = (1,0)$ and $0_L = (0,1)$.

Definition 2 [15]: $f_L : L^n \to L$ is an aggregation function if it is monotone with respect to $\leq L$ and satisfies $f_L(0_L, ..., 0_L) = 0_L$ and $f_L(1_L, ..., 1_L) = 1_L$.

For brevity, the pair $(\mu_A(x), v_A(x))$ of IFS *A* is simply denoted as $\alpha = (\mu_\alpha, v_\alpha)$. Next Weize Wang and Xinwang Liu investigate the intuitionistic fuzzy Einstein weighted averaging operator and give the computational formula.

Definition 3 [11]: Let $\alpha_j = (\mu_{\alpha_j}, v_{\alpha_j})(j = 1,2,...,n)$ be a collection of IFSs in *L* and $\omega = (\omega_1, \omega_2, ..., \omega_n)^T$ is the weight vector of $\alpha_j (j = 1,...,n)$ such that $\omega_j \in [0,1] (j = 1,...,n)$ and $\sum_{j=1}^{n} \omega_j = 1$; then, an $IFWA^{\varepsilon}$ operator of dimension *n* is a mapping $IFWA^{\varepsilon} : L^n \to L$, and

$$IFWA_{\omega}^{\varepsilon}(\alpha_1, \alpha_2, ..., \alpha_n) = \omega_1 \cdot_{\varepsilon} \alpha_1 \oplus_{\varepsilon} \omega_2 \cdot_{\varepsilon} \alpha_2 \oplus_{\varepsilon} ... \oplus_{\varepsilon} \omega_n \cdot_{\varepsilon} \alpha_n$$

(8)

Theorem 1 [11]: Let $\alpha_j = (\mu_{\alpha_j}, v_{\alpha_j}), (j = 1,...,n)$ be a collection of IFSs in *L*, $\omega = (\omega_1, \omega_2, ..., \omega_n)^T$ is the weight vector of $\alpha_j (j = 1,2,...,n)$ such that $\omega_j \in [0,1] (j = 1,2,...,n)$ and $\sum_{j=1}^{n} \omega_j = 1$. then, their aggregated value by using the $IFWA^{\varepsilon}$ operator is also an IFS, and

$$IFWA_{\omega}^{\varepsilon}(\alpha_1, \alpha_2, ..., \alpha_n) = \left(\frac{\prod_{j=1}^{n} (1 + \mu_{\alpha_j})^{\omega_j} - \prod_{j=1}^{n} (1 - \mu_{\alpha_j})^{\omega_j}}{\prod_{j=1}^{n} (1 + \mu_{\alpha_j})^{\omega_j} + \prod_{j=1}^{n} (1 - \mu_{\alpha_j})^{\omega_j}}, \frac{2 \cdot \prod_{j=1}^{n} v_{\alpha_j}^{\omega_j}}{\prod_{j=1}^{n} (2 - v_{\alpha_j})^{\omega_j} + \prod_{j=1}^{n} v_{\alpha_j}^{\omega_j}} \right)$$

(9)

3.2. Simulated Performance Results

We measure the selection percentage of trustworthy cloud providers in the first experiment. The first result refers to the percentage of trustworthy service providers have been able to achieve. Thus, Figure 2 shows the performance of TM on this respect. As it can be observed, the accuracy of the system where no trust model is used decreases as the percentage of malicious providers and the total number of

customers and providers increases. In the case of a system composed by 400 customers and 25 providers where 30% of the providers are malicious, the system fails and only selects the appropriate service provider in near the 26% of the cases. In Figure 2, the corresponding results for the system which uses TM have been shown. In most of the cases, the accuracy of the model is never below 90%. Only with the biggest networks, this percentage decreases to a minimum of around 85% (when the amount of malicious providers is maximum). This improvement is mainly due to the introduction of the reputation model which makes the good reputation customers' trust score to take a higher weight in the calculation of the global reputation. Therefore, malicious providers are rarely chosen to provider data storage service.

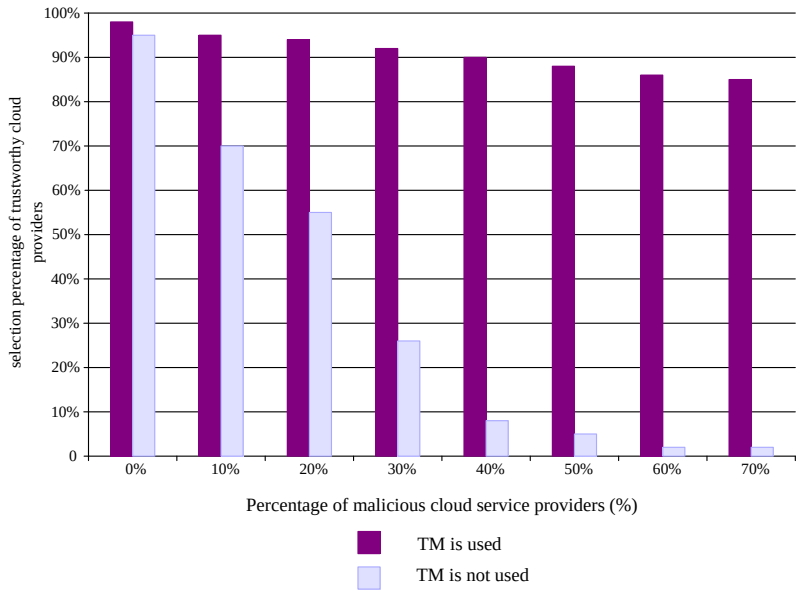

Figure 2. Selection Percentage of Trustworthy Cloud Service Providers

The second experiment measures the length of the path leading to trustworthy cloud providers. With respect to path length (see Figure 3), a similar effect with the selection of trustworthy providers happens. The system which uses TM obtains better results as the number of good providers available decreases. The average number of hops needed to reach the most trustworthy cloud provider was 3.95.

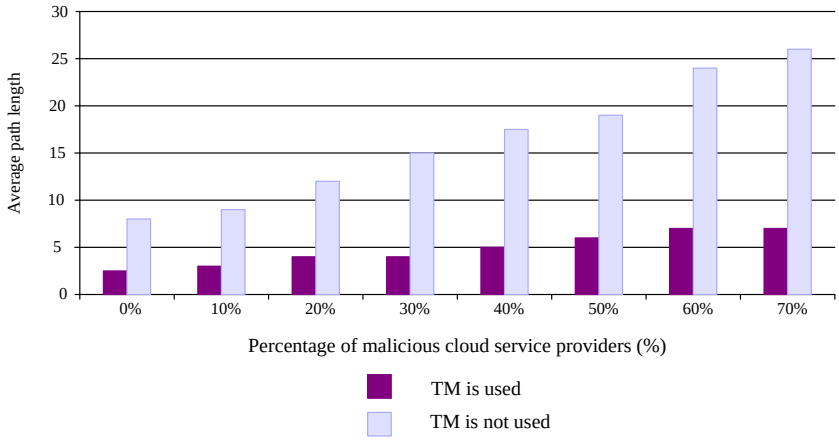

Figure 3. Average Path Leading to Trustworthy Cloud Providers

4. Conclusion

Trust is a critical part of the process by which relationships develop. It is a before-security issue in the ad hoc networks. By clarifying the trust relationship, it will be much easier to take proper security measures, and make correct decision on any security issues. Trust modeling is a technical approach to represent trust for digital processing. Recently, trust modeling is paid more and more attention in cloud computing. In the paper, we propose a trust model (TM) based on fuzzy logic inferences, which can better handle uncertainty, fuzziness, and incomplete information in cloud trust reports. As a future work, we plan to test our model into more real cloud computing environment and analyze the system performances.

Acknowledgements

The work in this paper has been supported by Scientific Research Program Funded by Natural Science Basis Research Plan in Shaanxi Province of China (Program No.2011JQ8006) and Shanxi Provincial Education Department (Program No.11JK1060 and 2013JK1132) and National Natural Science Foundation of China (Program No. 61373116) and and China Postdoctoral Science Foundation (Program No.2014M560796) and special funding for key discipline construction of general institutions of higher learning from Shanxi province and special funding for course development from Xi'an University of Posts and Telecommunications.

References

[1] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," MIPRO, 2010 Proceedings of the 33rd International Convention, **(2010)**, pp. 344-349.
[2] M. Bret and D. Georeg, "Establishing trust in cloud computing," IAnewsletter, vol. 13, no. 2, **(2010)**, pp. 4-8.
[3] http://www.cloudsecurityalliance.org/csaguide.pdf.
[4] H.-C. Li, P.-H. Liang, J.-M. Yang and S.-J. Chen, "Analysis on Cloud-Based Security Vulnerability Assessment," Proceedings of the IEEE 7th International Conference on e-Business Engineering (ICEBE), **(2010)**, pp. 490-494.
[5] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, **(2010)**, pp. 14-22.
[6] J. Abawajy, "Establishing Trust in Hybrid Cloud Computing Environments", In: Proc. of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), **(2011),** pp. 118−125.
[7] W. Han-zhang and H. Liu-sheng, "An improved trusted cloud computing platform model based on DAA and Privacy CA scheme," Proceedings of the IEEE International Conference on Computer Application and System Modeling (ICCASM 2010), **(2010)**.
[8] Z. Yang, L. Qiao, C. Liu, C. Yang and G. Wan, "A collaborative trust model of firewall through based on Cloud Computing," Proceedings of the 14th International Conference on Computer Supported Cooperative Work in Design. Shanghai, China, **(2010)**, pp. 329-334.
[9] D. C. Edna, O. A. Robson and T. S. J. Rafael, "Trust Model for File Sharing in Cloud Computing," Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization, **(2011)**, pp. 66-73.
[10] X.-Y. Li, L.-T. Zhou, Y. Shi and Y. Guo, "A Trusted Computing Environment Model in Cloud Architecture," Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, **(2010)**, pp. 11-14.
[11] W. Wang and X. Liu, "Intuitionistic Fuzzy Information Aggregation Using Einstein Operations," IEEE Trans. Fuzzy Syst., vol. 20, no. 5, **(2012)**, pp. 923-938.
[12] E. P. Klement, R. Mesiar and E. Pap, "Triangular norms, position paper I: Basic analytical and algebraic properties," Fuzzy sets and Systems, vol. 143, no. 1, **(2004)**, pp. 5-26.
[13] B. Hu, "Fuzzy Set Theory", Wuhan, China: Wuhan Univ. Press, **(2004).**
[14] G. Deschrijver and E. Kerre, "On the relationship between some extensions of fuzzy set theory," Fuzzy sets and Systems, vol. 133, no. 2, **(2003)**, pp. 227-235.
[15] G. Beliakov, H. Bustince, D. P. Goswami, *et al.*, "On averaging operators for Atanassov's intuitionistic," fuzzy sets. Inf. Sci., vol. 181, no. 6, **(2011)**, pp. 1116–1124.

Authors

Xu Wu received her Ph.D. degree in Computer Science, from the Beijing University of Technology, in 2010. She is an associate professor of Xi'an University of Posts and Telecommunications. She is currently doing postdoctoral research at the MOEKLINNS Lab, Department of Computer Science and Technology of Xian Jiaotong University. Her research interests include trusted computing, pervasive computing, mobile computing, and software engineering. She has published more than 30 technical papers and books/chapters in the above areas.