International Journal of Control and Automation
Vol. 9, No. 11 (2016), pp.363-374
http//dx.doi.org/10.14257/ijca.2016.9.11.31

A Novel Trust Management Method based on Information Visualization for Cloud Computing

Xu Wu

[1]*School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an, China*
xrdz2006@163.com

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. In the paper we present a novel trust management method (TrustSocieties), our attempt at addressing this trust issue through the use of information visualization. TrustSocieties is a visual method for graphical representation of entity trust relationships in cloud computing. The proposed method can assist cloud computing entities to make good trust decisions. The main contribution of this paper is to provide a visualization trust modeling method to user and improve his or her security situational awareness in the cloud computing environments. The experimental analysis shows that the proposed method gives a better understanding of the trust making process, and facilitates accurate and fair assessment of the service reputations. Our analysis shows a significant improvement in trust assignment accuracy for our technique in comparison to manual trust assignment. Our work appears to be the first attempt to research the visualization method of trust management for cloud computing.

Keywords*: cloud computing, trust model, visualization*

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]. Cloud computing brings a shift from heavy IT infrastructure invest for limited resources that are internally managed and owned by a customer to pay per use for IT infrastructure owned by a cloud computing service provider. There are many benefits to cloud computing: lower overall cost of IT ownership, increased flexibility, fault tolerance, locality flexibility ability, and to respond to new business requirements quickly and efficiently. Cloud computing requires that customers trust that a service provider's platforms are secured and provide a sufficient level of integrity for the client's data. Once a client's sensitive data are released into the cloud under the control of a third party, a significant level of risk is placed on the security and privacy of the data. 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.

Cloud customers' risk exposure issues in the cloud differ from those in traditional distributed systems. Cloud customers, who are the information owners, are most concerned about whether data-center owners will abuse the system by randomly using private datasets or releasing sensitive data to a third party without authorization. So, the core security challenge of cloud computing is that the

ISSN: 2005-4297 IJCA

information owner does not control the hardware that is operating on his data. Complicating the situation is that the hardware is multi-tenant with shared resources among many users. However, existing techniques do not satisfactorily solve the problem, a good solution is to leverage trust management technology to build trust into utility cloud computing. 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. 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. Although some trust management approaches are proposed for cloud computing, the problem of how to determine service trustworthiness in cloud computing environments has not been addressed in a satisfactory manner.

In the paper we present a novel trust management method (TrustSocieties), our attempt at addressing this trust issue through the use of information visualization. TrustSocieties is a visual method for graphical representation of entity trust relationships in cloud computing. The proposed method can assist cloud computing participants to make good trust decisions. In reality, trust is a social problem, not a purely technical issue. However, we believe that technology can provide the cloud customers with a way of measuring the claims of the cloud service provider as to how trustworthy their clouds are. The benefits of defining trust with visual approach are threefold: First, it gives a better understanding of the components that can be used in a trust management system. Second, it illustrates that the components contributing to the trust making process can be different from one service environment to another; and third, it shows that the way one person trusts can be different from others.

This paper is organized as follows. Section 2 describes related work. In Section 3, the proposed visualization trust modeling method TrustSocieties is discussed. We also discuss the representation of reputation and how the reputation is built. 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

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*. [2] 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.

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*. [3] 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 [4]. 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*. [6] 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.

2.2. 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 [7] 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. Based on the trust management framework, a mechanism is developed. The mechanism can effectively address strategic feedbacks and mitigate unfairness. The performance of the proposed trust management system has been studied in a simulated environment and due to space limitations this information is not fully provided.

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 [8]. 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*. [9] 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.

Hada *et al*. [10] 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. These agents monitor virtual machine integrity and

authenticity. Security agents can dynamically move in the network, replicate itself according to requirement and perform the assigned tasks like accounting and monitoring of virtual machines.

Edna *et al*. [11] 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*. [12] 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.

Pawar *et al*. [13] propose an uncertainty model and define an approach to compute opinion for cloud service providers. Using subjective logic operators along with the computed opinion values, they propose mechanisms to calculate the reputation of cloud service providers. They also evaluate and compare the proposed model with existing reputation models.

3. TrustSocieties

In this section, we present a brief discussion of the main components of TrustSocieties.

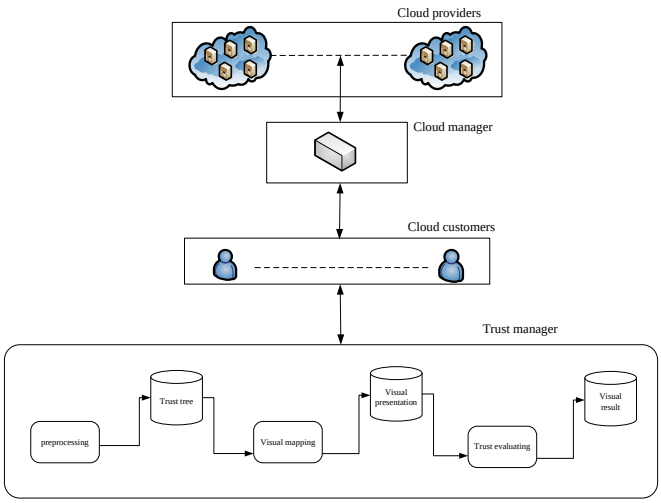

Figure 1. Main Components of TrustSocieties

Figure 1 shows the basic components of TrustSocieties that allows cloud users to deploy applications and scientific workflows that require resources beyond the capacity of their clouds. TrustSocieties is layered in that services are provisioned to cloud users based on cloud-level by the cloud manager. Cloud users require resources to deploy services and run applications. Cloud providers provide resources and services to potential users for fee or following another economic model such as

bartering. Resource providers have their cost structures and policies that govern how their resources are provisioned to a user.

3.1. Cloud Manager

Users submit their resource allocation requests to their local Cloud Manager (CM). CM is responsible for selecting suitable clouds that are able to provide the required resources to users. It is also responsible for managing requests for resources and services from other CM. Resources sharing between multiple clouds to meet cloud user requirements are enabled by peering arrangements established between the participating clouds. The peering agreement describes the information that is to be exchanged under the terms stated in contracts such as SLA. The peering policy also describes the desired level of access control as well as mechanisms to protect data both in storage and transmission. In addition, CM is also responsible for monitoring the execution of applications across multiple clouds. The CM also interacts with other entities including accounting systems that provide information on shares consumed by peering clouds.

3.2. Trust Manager

Trust manager enables cloud customers to select the best resources in the CM settings. It is responsible for computing the reputation value of the cloud service providers. We define the reputation of a cloud service provider as a measure of confidence in ability of that provider to provide a safe platform and sufficient level of integrity for the customer's data. Each cloud customer uses reputation values to determine whether it can trust a certain cloud service provider or not. The trust is represented as a binary value. The visual trust making process consists in the following three phases:

1) Preprocessing:

A cloud customer sends the data packet with a given trust context to other customers. The customers with similar trust context re-broadcast it in order to reach the whole network. Every customer stores the address of the customer from which it has received the first data packet. This customer will be called the parent. This way, a trust tree overlay with similar trust context will be constructed.

2) Visual mapping

The phases provide a visualization representation of trust, its components and the trusting process by using user requirements notation for trust modeling. By way of illustration we will refer to the visual method.

The Figure 2 shows the trust's visual definition. First, there are always two participants in the Figure– cloud customer and cloud service provider – involved in the process of trust. The customers use the cloud service offered by the providers. As shown in the Figure, the customer, in the trust decision-making process, decides whether he should trust the provider. The trust decision making process is illustrated by using user requirements notation [14]. This process can be detailed to show how exactly one decides about trust or distrust. Finally, the trust process can end in the good result or bad result, based on the behaviors of the provider. As showed in Figure 2, the behavior of the provider is out of the boundary of the customer and therefore is not controllable and predictable. In this case, the previous direct observation and experience (*i.e.,* first-hand information) and indirectly by sharing observations and experience measures with other entities (*i.e.,* second-hand information) can help the customer to reduce the risk of trust and the complexity of trust decision making process.

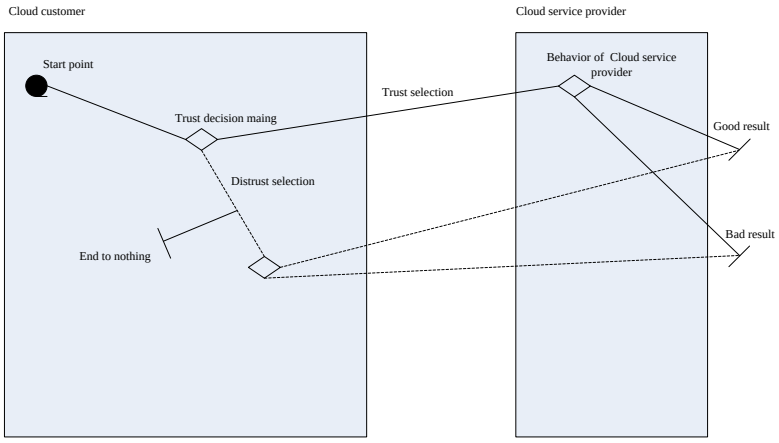

Figure 2. Trust's Visual Definition

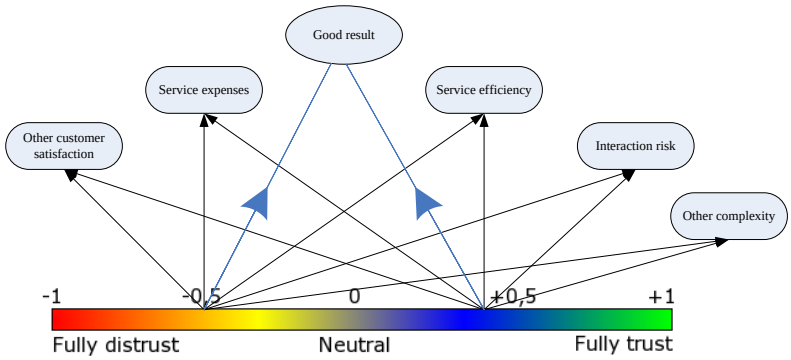

Figure 3. The Cloud Customer's Targets in Trust Making Process

Figure 2 provides a better understanding of trust's definition and trust making process. However, it doesn't show the interaction target of customer from the trust decision-making process. Studying of this target can help to define and formalize the trust decision making process and the criteria that are used in this process by the provider. Goal Requirement Language of URN's component is used to illuminate the mentioned targets. Figure 3 shows the targets of a trust making process which has been showed as Figure 2. Using GRL, this figure shows the effects of trust and distrust – the two available selections for customer in Figure 2. Service expenses, service efficiency, interaction risk, other customer satisfaction and other complexity are some of the criteria that the cloud customer may use for decision making in this stage. In addition, Figure 3 also shows a comparison between trust and distrust and their contributions to customer's targets. This model helps to select the right partner in each interaction, based on customer's targets evaluation. With the same approach, this model can also be used for comparing and evaluating two or more third participants to see which one has better impact on the targets of the trust process.

3) Trust evaluating

The trust value is computed using the following conditions:

Trust(i) =1 if Reputation(i)>= TRUST_THRESOLD_VALUE

Trust(i) =0 if Reputation(i) < TRUST_THRESOLD_VALUE

The threshold values are the points where cloud customers, based on the associated values to the cloud service provider, decide between trust and distrust – Figure 4. The thresholds could be different form one customer to another and even for the same customer in different situations. As the result, based on each

individual's targets, one party can be trusted by an individual while it is not trusted by another.

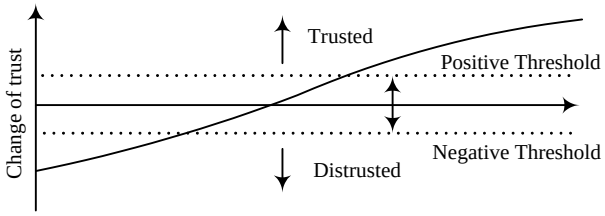

Figure 4. Trust Threshold Value

The reputation of cloud service provider i is computed based on the following formula:

$$V_i = \sum_{k \in S} \left(\frac{w_k}{\sum_{k \in s} w_k} f_{ki} \right) = \frac{\sum_{k \in s} w_k f_{ki}}{\sum_{k \in s} w_k}$$

where *Vi* is the reputation of provider *i* , S is the set of customers with whom provider i has conducted transactions, f_{ki} is the feedback score of provider *i* rated by customer *j*, and w_k is the aggregation weight of f_{ki}. The aggregation process runs multiple iterations until each *Vi* converges to a stable reputation rating for provider *i*. To tackle the message overhead issue, the trust evaluating scheme partially queries qualified customers that meet an aggregation threshold.

This computed trust value can be used by parent customer nodes in order to forward or aggregate a provider's reputation value received from children customer nodes that are trustworthy, and ignore reputation values from children customer nodes in which they do not trust. After a trust tree change, two nodes that were not neighbors in the previous cycle can become parent and child after a preprocessing phase. The parent is now able to use the information it has previously obtained about the new child node.

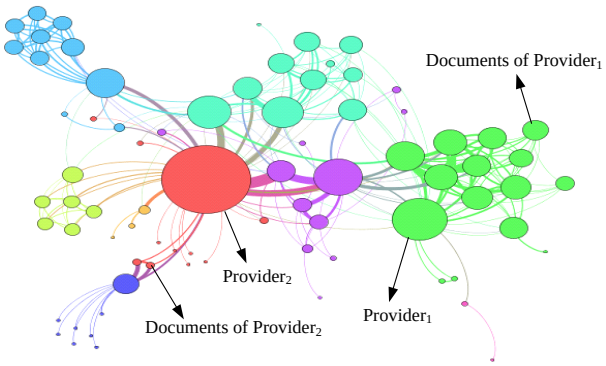

Figure 5. Visual Trust Evaluation Result of TrustSocieties with 2000 Nodes

We have developed a prototype implementation of the TrustSocieties using a simulated distributed file sharing service in cloud computing environment. The technique can be used to visualize the trust relationships of the file service providers as well as their documents in the system. With TrustSocieties, the file service providers are organized into societies according to their trust level (see Figure 5).

Each society is colored in such a way to give some indication of the trust level of each society. Different colors represent the various trust levels.

4. Experimental Study

In this section, in order to evaluate the effectiveness of TrustSocieties, a series of test scenarios are developed. We will study the impact, effectiveness and cost of the visual framework in computing trustworthiness of a service. All simulations were conducted over 1000 sessions. To simulate various real-world reliability scenarios, we generate individual Cloud customer, we used a bimodal distribution to represent a system that has a mix of highly-reliable workers and compromised or poorly-connected nodes.

We use the reputation of cloud provider as a metric to evaluate the accuracy of the proposed approach to measure the correctness of visual mapping. Accuracy of the trust evaluation is one of the important metrics to analyze the strength of a given trust management system. An accurate trust evaluation system should help the users to defend themselves against malicious information, including trust values propagated by other users into the system. The system is accurate if this property is accomplished.

4.1. Visual Mapping

One of the goals of TrustSocieties is to help select the right way in each individual case, based on trustworthiness evaluation of a service provider.

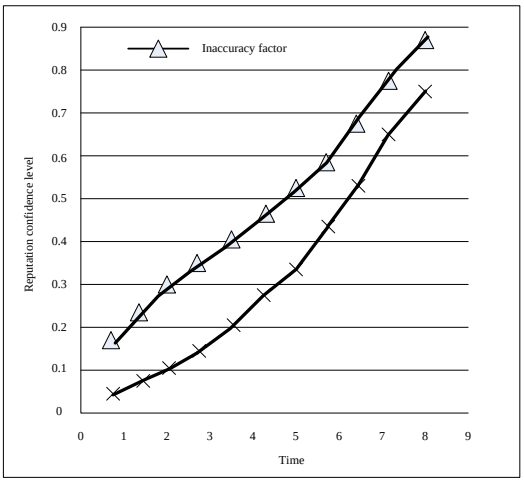

Figure 6. Inaccuracy Weight Impact

Having someone trusted to do a specific piece of work may also increase the confidence for success. However, it may increase the risk, especially when a customer doesn't have enough knowledge or prior interaction with the provider. The main goal of a reasonable provider is to increase the associated trust to her. When no experience with a service provider is made in a long time, the trust relationship might drop back to a low state. However, a good visual representation of the provider and her services can help to increase the reputation confidence level of provider's behavior for the customer. We represent the effect of this visual mapping with a inaccuracy factor as a real number $\lambda \geq 0$. The higher the inaccuracy factor, the faster the trust confidence level drops back to a state specified by the trust evaluating algorithm. This state might be a state of no trust and no confidence.

Figure 6 shows the significance of a good visual representation in trust making process.

4.2. Accuracy of Trust Evaluation

The proposed mechanism can help to improve the accuracy of trust evaluation. As mentioned earlier, in a cloud computing environment, some service providers may provide services with low quality; so a provider that may not be functioning may provide incorrect information that can deceive the whole network. It is therefore important in cloud computing to detect malicious providers.

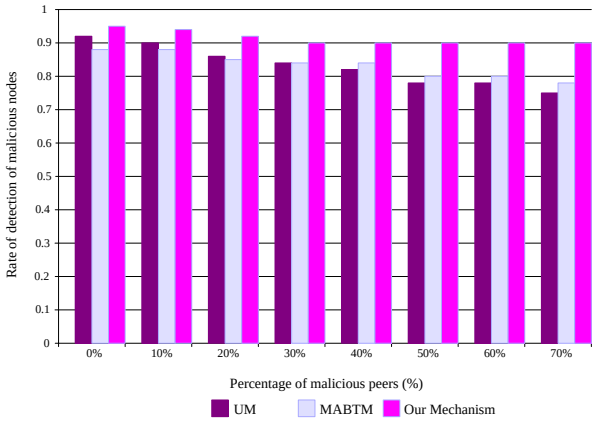

Figure 7. Simulation Results of Nodes under Independent Cheat

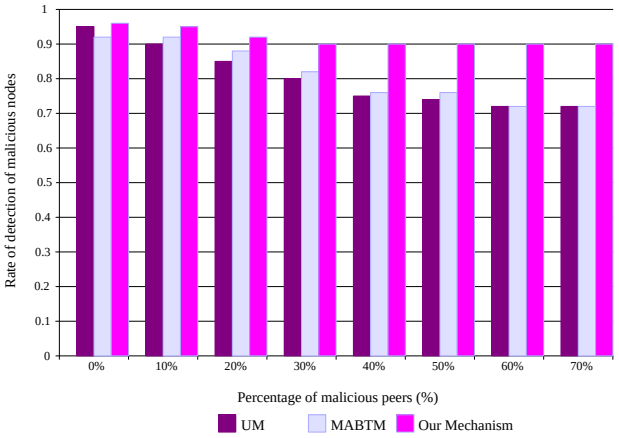

Figure 8. Simulation Results of Nodes under Group Cheat

The rate of detection of malicious providers is evaluated in the group of experiments. We add a number of malicious servers to the network such that malicious providers make up between 0% and 70% of all servers in the network. For each fraction in steps of 10% we run experiments under two attack models separately and depict the results in Figure 7 and Figure 8. We observed a 90% fraction of detection of malicious providers of our mechanism at least in Figure 7 and Figure 8. For independent cheat and group cheat, our scheme performs well even if a majority of malicious providers is present in the network at a prominent place. Even if no malicious providers are present in the system, providers are evaluated as malicious in 3%-5% of all cases – this accounts for mistakes providers make when providing a service, *e.g.*, by providing the wrong meta-data or creating and sharing an unreadable file. As Figure 8 and Figure 9 shows, comparing with

MABTM [10] and UM [13], our proposed scheme gets more efficient. The main reason is that TrustSocieties is used to categorize entities in a distributed cloud computing environment. Entities are automatically laid out in each society with their size, color, and orientation conveying information about the trust properties of each entity.

5. Conclusions and Future

In the paper, we present a novel trust management method (TrustSocieties) for developing an effective trust management in cloud computing environments. 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. The main contribution of TrustSocieties is to provide a visualization representation of trust, its components and the trusting process by using user requirements notation for trust modeling. The benefits of TrustSocieties are threefold: First, it gives a better understanding of the components that can be used in a trust management system. Second, it illustrates that the components contributing to the trust making process can be different from one service environment to another; and third, it shows that the way one person trusts can be different from others. We have studied the performance of TrustSocieties in a simulated environment. Our work appears to be the first attempt to research the visualization of trust management for cloud computing. In future, we will develop a full list of threats against the proposed visualization trust management framework and analyze the vulnerability of the system to these threats.

Acknowledgments

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 Shanxi Provincial Education Department (Program No. 15JK1679).

References

[1] M. A. Imad and L. John, "Challenges for Provenance in Cloud Computing", Proceedings of the third USENIX Workshop on the Theory and Practice of Provenance, **(2011)**, pp.1-6.
[2] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges", Proceedings of the 33rd International Convention, **(2010)**, pp. 344-349.
[3] M. Bret and D. Georeg, "Establishing trust in cloud computing", IAnewsletter, vol. 13, no. 2, **(2010)**, pp.4-8.
[4] http://www.cloudsecurityalliance.org/csaguide.pdf.
[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] 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, **(2010)**, pp. 490-494.
[7] N. Santos, K. Gummadi and R. Rodrigues, "Towards Trusted Cloud Computing", Proceedings of the HotCloud, **(2009)**.
[8] H.-Z. Wang and L.-S. Huang, "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, **(2010)**.
[9] Z. Yang, L. Qiao, C. Liu, C. Yang and G. Wan, "A collaborative trust model of firewallthrough based on Cloud Computing", Proceedings of the 14th International Conference on Computer Supported Cooperative Work in Design. Shanghai, China, **(2010)**, pp. 329-334.
[10] 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, **(2011)**, pp. 12-15.
[11] 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.

[12] 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.
[13] P.S. Pawar, M. Rajarajan, S. K. Nair and A. Zisman, "Trust Model for Optimized Cloud Services", In: Proc. of the 6th IFTP International Conference on Trust Management, **(2012)**, pp. 99-112.
[14] D. Amyot, "Introduction to the User Requirements Notation: Learning by Example. Computer Networks, 42(3), **(2003)**, pp. 285-301.
[15] R. Zhou and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted P2P Computing", IEEE Transactions on Parallel and Distributed Systems, vol.18, no.5, **(2007)**.

Author

Xu Wu, she 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. Her research is supported by National Natural Science Foundation of China (Program No. 71501156) and China Postdoctoral Science Foundation (Program No.2014M560796).