Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 129 (2014) 314 – 321

Procedia
Social and Behavioral Sciences

**ICIMTR 2013**

International Conference on Innovation, Management and Technology Research,
Malaysia, 22 – 23 September, 2013

# Enhancing Trust Management in Cloud Environment

Soon-Keow Chong[a]* Jemal Abawajy[b], Masitah Ahmad[c], Isredza Rahmi A. Hamid[d]

[a,b,c,d]*Parallel and Distributed Computing Lab,*
*School of Information Technology, Deakin University, Victoria 3217, Australia*

**Abstract**

Trust management has been identified as vital component for establishing and maintaining successful relational exchanges between e-commerce trading partners in cloud environment. In this highly competitive and distributed service environment, the assurances are insufficient for the consumers to identify the dependable and trustworthy Cloud providers. Due to these limitations, potential consumers are not sure whether they can trust the Cloud providers in offering dependable services. In this paper, we propose a multi-faceted trust management system architecture for cloud computing marketplaces, to support customers in identifying trustworthy cloud providers. This paper presents the important threats to a trust system and proposed a method for tackling these threats. It described the desired feature of a trust management system. It security components to determine the trustworthiness of e-commerce participants to helps online customers to decide whether or not to proceed with a transaction. Based on this framework, we proposed an approach for filtering out malicious feedbacks and a trust metric to evaluate the trustworthiness of service provider. Results of various simulation experiments show that the proposed multi-attribute trust management system can be highly effective in identifying risky transaction in electronic market places.

© 2014 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of Universiti Malaysia Kelantan

Keywords: E-Commerce, cloud, Reputation, Unfair Rating, Trust Management.

## 1. Introduction

Cloud computing is a new way of delivering computing resources to run websites and web applications. E-commerce taking the advantage of cloud computing platform provides for sharing resources, services and information among people across the world. But the cloud is not without potential problems, such as considerable security and usability (in terms of choice) hurdles (Fujitsu Research Institute, 2010). A major challenge of serving trust for the

* Corresponding author. *E-mail address*: s.chong@deakin.edu.au.

1877-0428 © 2014 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of Universiti Malaysia Kelantan
doi:10.1016/j.sbspro.2014.03.682

overall system is needed to consider that in real world applications the information about the trustworthiness of the subsystems and components itself is subject to uncertainty. To achieve its potential in cloud computing, there is a need to have a clear understanding of the various issues involved, both from the perspectives of the providers and the consumers of the technology.

Trust management has been identified as vital component for establishing and maintaining successful relational exchanges between e-commerce trading partners in cloud environment (Habib, S. M. Ries, S. & Muhlhauser, M. (2010). It supports customers in reliably identifying trustworthy cloud providers, and to manage the trust relationships between business partners in cloud environment. This is achieved by maintaining the trust-level of the e-commerce participants and makes them available to potential e-commerce customers when needed. The trust level is derived from feedback ratings submitted by the trading partners after the successful completion of the transactions. The trust values accumulated from the past transactions information provide important reference for future users. Both customer and provider judge each other's credibility by their trust values. Establishing trust is the way to build good relationship with both customer and provider which positive activates will increase trust level, otherwise destroy trust immediately. Since trust value must be determined based on past experience from both customer and provider, establishing an initial trust level can be a major challenge to both potential customers and providers. The other question concerning e-commerce management systems is equations do not accurately reflect trustworthy of transaction partners (customers and providers). It is hard to evaluate and exchange reputation between e-commerce participants due to the differences in perception, calculation and interpretation. But most of all because the given reputation is calculated based on overall transaction information with different quality criteria or attributes, it does not reflect the related contexts. There are some common attacks (Cho, J.H. & Swami, A; 2009) deliberately designed to sabotage trust management schemes.

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. In recent years many researchers have focused on trust related issues, the general trend in trust management system is to consider all feedbacks as accurate. Unfortunately, trust management systems rely on the feedback provided by the trading partners, they are frail to strategic manipulation of the feedback attacks. Therefore, identifying and actioning falsified feedbacks remain an important and challenging issue in trust management field (Chong, S.K & Abawajy, J; 2010).

The fundamental criteria and requirements for e-commerce trust models to follow are still not well understood. Two problems need to be solved herein. Firstly, the model must be accurately predicting the trust value of interactions success. Trust model must be able to maintain accuracy even under dynamic condition, adapting to changes introduce by others. Second, the trust management system itself may become the target of attacks and can be compromised. An ideal trust management is needed to improve the support for existing trust management in e-commerce. It should also provide essential security services, such as to validate the identity, provides services, secure storage, privacy support and provide an efficient and effectively trust decision tool. Thus, the major challenge of the trust management system is ensuring the accuracy of trust information.

This paper address the most important procedure which to recognize and understand the type of security threats to the trust information when developing and designing a trust management system. It also proposed a filtering scheme to improve the accuracy of trust evaluation of a trust management system. The rest of the paper is organized as follows. The related work is discussed in Section 2 and Section 3 presents the trust system threats. Trust management system requirement is discussed in Section 4. In Section 5 the proposed feedback verification mechanism is discussed and the performance analysis is presented in Section 5. The conclusions and future directions are discussed in Section 6.

## 2. Related Work

Various types of rating attack against the trust management systems such as ballot stuffing, bad-mouthing, negative discrimination and positive discrimination have been discussed in (Dellarocas, C., 2000; Jøsang, A. Ismail, R. & Boyd C.(2007). It has been identified that customers who falsify feedbacks have similar characteristics to online auction shilling bidders such as a higher bidding frequency to outbid legitimate customers (Trevathan, J. & Read, W. 2007). Similarly, raters who inflate or deflate feedback will attempt to submit feedbacks frequently. Another common characteristic is that raters who falsify ratings usually have low trust value (O'Donovan, J., Smyth, B. V. & Evrim, D., 2007). They also tend to usually engage in minimum value transactions to meet the requirements of submitting a rating (Kerr, R. & Cohen, R., 2009). Also, falsified ratings tend to be either significantly lower or higher than the majority of the set threshold. A rater with a higher trust value is more willing to provide a good rating in order to maintain their reputation (Kerr, R. & Cohen, R., 2009). Thus, a trust management system should have the ability to weigh the ratings of highly credible raters more than those with a low credibility rating (Chong, S.K & Abawajy, J; 2010).

There are several approaches that evaluate trustworthiness of users based on majority opinion, such as beta filtering feedback (Josang, A., & Indulska, J., 2004). This approach works as long as the majority of ratings are not from a group of raters that tend to falsify their ratings. Another approach that uses beta probability density function to estimate the

Download English Version:

https://daneshyari.com/en/article/1116638

Download Persian Version:

https://daneshyari.com/article/1116638

Daneshyari.com