Available online at www.sciencedirect.com
ScienceDirect
Procedia - Social and Behavioral Sciences 129 (2014) 396 – 405
Procedia
Social and Behavioral Sciences

ICIMTR 2013

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

A Multilevel Trust Management Framework for Service Oriented Environment

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

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

Abstract

In service-oriented computing applications, trust management systems are emerging as a promising technology to improve the e-commerce consumers and provider's relationship. Both consumers and providers need to evaluate the trust levels of potential partners before engaging in interactions. The accuracy of trust evaluation greatly affects the success rate of the interaction. This paper addresses the threats and challenges that can compromise the reliability of the current trust management system. This paper studies and examines the importance of the trust factors of the trust management framework, specifically in dealing with malicious feedback ratings from e-commerce users. To improve the reliability of the trust management systems, an approach that addresses feedback-related vulnerabilities is paramount. A multilevel trust management system computes trust by combining different types of information. Using this combination, we introduce a multilevel framework for a new interactive trust management to improve the correctness in estimate of trust information.

Keywords: E-Commerce; Filtering, Malicious; Trust; Rating; Trust Management

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

doi:10.1016/j.sbspro.2014.03.693

1. Introduction

E-commerce consists primarily of distributing, buying, selling, marketing, and servicing of products or services over the Internet. It brings new ways for vendors to conduct business and for consumers to purchase online from anywhere at any time. However, e-Commerce, as any other form of commerce, depends on a level of trust to exist between a buyer and a seller (Chen & Singh, 2001). It has been shown that the level of trust has an approximate inverse relationship to the degree of risk (Pittayachawan, Singh & Corbitt, 2008) and (Trevathan & Read, 2007). Trust is a well-known concept in everyday life and often serves as a basis for making decisions in complex situations. Trust is a major factor for the success of any business in general and e-commerce in particular. Trust is a complex subject encompassing concepts such as honesty, truthfulness, competence and reliability. Thus, trust can mean different things to different people. In this paper, we consider trust as a measureable belief of one entity about another entity performance for a specified context (Jøsang, Ismail, & Boyd, 2007). While consumers have embraced e-commerce to a certain degree, their enthusiasm has not exceeded expectations. Lack of trust has been identified as a major barrier for sustainable growth in e-commerce (Mäntymäki, 2008; Pittayachawan, Singh, & Corbitt, 2008). According to the recent IC3's report, there is an increase of 22.3% in an online fraud which is an indicative of why the consumers feel uncomfortable engaging in online business transactions. To address this problem, several trust management systems have been proposed (Jøsang & Golbeck, 2009; Whitby, Josang & Indulska, 2004). A trust management system is to manage the trust relationships between the trading partners.

While trust management systems are increasingly being used in e-Commerce environments, they are susceptible to tampering with feedbacks. For example, a small percentage of falsified feedbacks could degrade the accuracy of the trust level, compromise the overall trustworthiness of the participating parties and render the trust management system unreliable. While it is impossible to expect all rating providers to provide actual feedbacks in an open environment such as e-Commerce, it is necessary to have an approach that is able to detect falsified feedbacks to protect the integrity of the trust management system. Although there have been techniques to encourage trustworthy behaviour (Trevathan & Read, 2006; 2007; Raza & Hussai, 2008; Chong, & Abawajy, 2010), the general trend in trust management system is to consider all feedbacks as accurate. Unfortunately, since the trust management systems rely on the rating provided by the trading partners, they are frail to strategic manipulation of the rating attacks.

This goal is achieved by maintaining the trust-level of the e-commerce participants and makes them vailable to potential e-commerce customers when needed. The trust level is derived from feedbacks submitted by the trading partners after a successful completion of the transactions. The submitted feedbacks are analysed, aggregated, and made publicly available to the interested parties to select trading partners and make commitment decisions. Trust management has been receiving attention in various domains such as grid and (Kerr & Cohen, 2009) and cloud computing and e-commerce (Gregg, & Scott, 2008). Therefore, identifying and actioning falsified feedbacks remain an important and challenging issue in trust management field.

The reliability of a trust management system depends on their capability of subsystems and its component. How information is collect by the subsystem and how the trust values are assessed. To support customers in reliably identifying trustworthy providers, extending our earlier work (Chong, et. al., 2007), we propose a multilevel trust management framework for service oriented marketplaces.

The rest of the paper is organized as follows. Trust management system threats and challenges are discussed in Section 2, the multilevel trust management system framework and its components are in Section 3. The conclusions and future directions are presented in Section 4.

2. Trust Management System Threats and Challenge

Trust management systems manage the trust relationships between business partners by maintaining the trust-level of the e-commerce participants and make 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 submitted feedbacks are analyzed, aggregated, and made publicly available to the interested parties. However, the open natures of e-commerce trust management systems are susceptible to the following critical threats and attacks due to the presence of malicious participants.

2.1 System and Social Threats

A security threat is the type of threat that is likely to cause damage of trust information accuracy, whereas vulnerability is the level of exposure to threats in a particular context. Security threats are one of the main concerns of designing and developing an efficient trust management system. In an open architecture, malicious participants may launch an attack on individuals or groups of participants to disable the service such as denial of service (DoS). The primary goal of denial of service attacks is to disable the system or make it impossible for normal operation to occur. Some of the common attacks identified in (Kerr, R. & Cohen, R., 2009) deliberately designed to sabotage trust management schemes. Those attacks include simple false information injection attacks, Sybil attacks and collusion attacks. A simple false information injection attack happens when a malicious entity generates false information on purpose.

In addition to the technical threats that exploit system vulnerabilities such as denial-of-service, social computing takes social interactions into account to compute trustworthiness and reputation of business partners. There are some providers who commit trust fraud to make their businesses look prosperous so as to attract more customers. For example, intentionally provides fake ratings about service providers and consumers, possibly acting under false identity.

An imprecise management of these threats could result of security deficiencies and weakness of a trust management system. However, not all trust models address knows all possible threats that undermine the accuracy of trust management system. Identifying these security threats helps the trust management system in improve vulnerability measures thus reducing or removing known weaknesses in the e-commerce environment.

To sum up, a small percentage of falsified ratings could compromise the overall trustworthiness of the participating parties as well as degrade the accuracy of the trust management system. Unreliable feedback ratings are often introduced by the malicious participants. The general behaviour of malicious participants has been described and the characteristics and strategies of a malicious participant are also discussed in much work (Jøsang, A & Golbeck, J., 2009) and (Kerr, R. &Cohen, R., 2007). Hence, an effective technique to verify the reliability feedback ratings from participants of e-commerce urgently needed. There is typically an assumption that feedback ratings are truthful and unbiased, which may not always be the case. Applying an appropriate filtering technique to the collected data would help trust management system made their transactions smoothly and safely. If a trust management system is compromised under a malicious attack, it can start giving out false trust information to a request, such as returning false data to a search query.

2.2 Challenges

Developing an effective trust management solution for e-commerce in an open environment is a challenging task. This paper focuses on enhancing the effectiveness of a trust management system thus building up trust relationship among its users. Managing trust in such an environment is crucial in improving current e-commerce deficiency. Increasing trust among buyers and sellers is thus a crucial factor that must be tackled. While designing a trust management model the following four challenges will be investigate:

- How to unify framework and cover a broad variety of trust mechanisms? Without providing a unified and broad framework for trust, it is very challenging to define a suitable trust management model for e-commerce. The framework should provide essential security services, such as validating the identity, providing services, securing storage, to support privacy and providing an efficient and effectively trust decision tool. Here the focus is on improving the overall architecture used in developing an ideal trust management to improve the support for existing trust management in e-commerce. Finding the requirement of a reliable trust modelling methodology is essential, and thus by applying the model to build up a trusted system. The current trust management systems lack a consistent model to help managing trust.
- How to reduce and manage ratings deception? There is typically an assumption that feedback ratings are truthful and unbiased. However, this may not always be the case. Feedback data can be manipulated by malicious participants by submitting fraudulent transactions. Fraudulent sellers or buyers could also build up their positive reputations by malicious way which is an obvious problem. Such feedback-related vulnerabilities have been identified in (Kerr, R. and Cohen, R. 2007 & 2009). Applying an appropriate filtering technique to the collected feedback data could help the trust management system make their transactions more smoothly and safely.
- How does the using of different context and factors help improve the accuracy of trust values? - Trust evaluation techniques must accurately reflect the contributing evidence to improve the customers' confidence. Trust model must be able to maintain accuracy even under dynamic condition, adapting to changes introduced by others. Existing work on e-commerce trust systems often compute trust based on overall performance instead of individual service performance. That is the contextual relevance of evidence is not taken into account for trust evaluation. For example, a participant may have many transactions of small value items and provide either positive or negative feedback ratings to influence the trust value of either party. The trust evaluation schemes must encompass the ability to reduce this type of feedback ratings. Trust evidence requires a formal evaluation scheme to represent the relationships between different entities. This is to ensure the trust relationship established for an intended purpose and sustained until the purpose is fulfilled.

How can a trust model predict risk before transaction? According to (Amland, S. (1999), information about history and knowledge of previously identified risk helps to predict risks correctly and increases customers' confidence. Thus, one way to address uncertainties is to develop strategies to determine the risk of an e-commerce transaction. Finding prediction technique that can inform potential buyers the risk level associated with a given product and develop a system that can assists buyers in assessing the level of trust they should place on an e-commerce transaction enhance the effectiveness of trust management system.

3. Trust Management System Framework

This framework encompasses components such as data collection, verification, evaluation and update management as shown in Figure 1. This trust system integrates a rating data verifying component to identify the trust worthiness of rating. Verification and evaluation is one of the most important

components, it perform the rating ratings collection and verification when evaluating the trust level or reputation of a vendor.

A set of questionnaire was constructed in collecting data. The questionnaires were divided into three sections namely; demographic details, business information, and women entrepreneurship programme. Those questionnaires were mailed to the selected entrepreneur or owners and they are given ten days to complete and return it to us. From 50 questionnaires that had been distributed, 40 entrepreneurs or owners return it. The data collection will be analyzed through descriptive analysis and frequencies analysis.

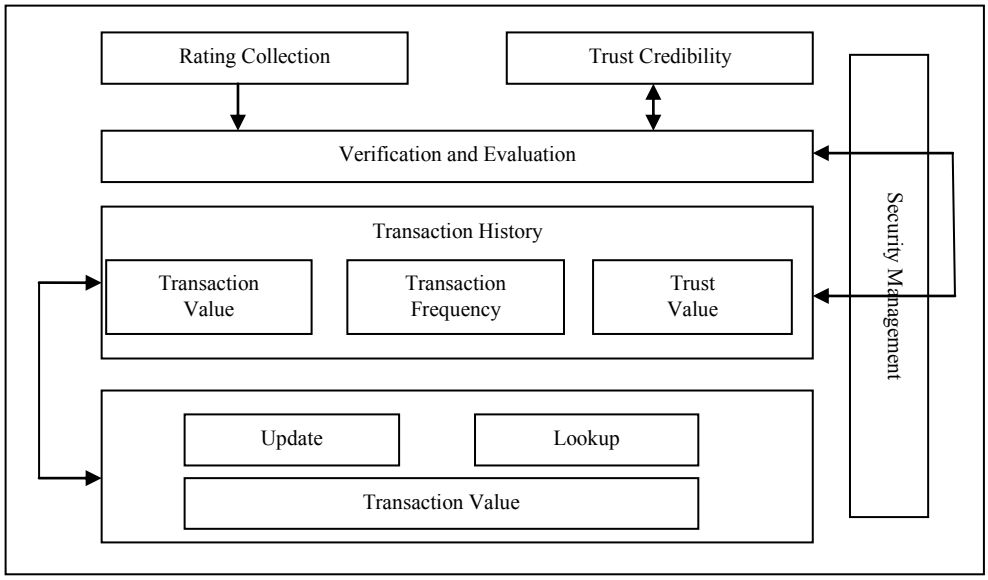

Figure 1. Trust Management System Framework

The system consists of the following components:

1. Rating collection. This component collects ratings service users after completed e-transactions. These ratings are vulnerable to attacks as identified by (Kerr & Cohen, 2009).
2. Rating verification. This component applied a verifying metric to verify the credibility of all ratings received before there are make available for trust evaluation.
3. Trust evaluation. The aim of trust evaluation is to compute a trust value from the verified ratings. Trust metric applied parameters associated to the derived trustworthiness
4. Trust data storage. Storage is needed for maintaining past behaviours and all trust information. Mechanism may be implemented to ensure data integrity confidentiality and availability.
5. Security Mechanism.

3.1 System Overview

The following sub section explains the overview of each component of the TMS.

- Data Collection Component

As shown in fig. 1, a service can conceptually be broken up into several components in which the interaction between buyer, seller and trust system via the interface. Initially, buyer searches specific product information. Buyer enquires the trust value about the seller of the specific product. The request is sent to the trust system. The request will be shown to the buyer once the authentication and authorization process are successful through the authentication and access control mechanism. The conditions on which such requests are granted are specified by a local policy. Upon a request, the access control mechanism constructs and sends corresponding policy queries to the evaluation engine. If the answer is positive, the request is granted.

The initial trust value is accepted by both buyer and seller before their interaction. The buyers will rate the quality of a service after the transaction is successfully completed. The trust system uses the ratings received from the buyers to determine the trust level of the seller. A data collection component records a collection of service history. For the purposed of identifying ratings to the corresponding services, each service invocation history record consists of the following fields: user Id that initiated the transaction, service identity (ID), service type and time invoked by user during the transaction. The creating of service history records from the performing by MTMS are created and reported using the following steps.

1. If a buyer B completes a transaction with service S, S creates a service invocation history record H.
   H = (B, S, FV, DT).
   a. FV is the transaction rating value given by buyer B.
   b. DT is the date and time service.
2. The record H will not be created until FV and its associate's attribute can be completely determined. For example, the buyer did not send payment to the service, which would affect rating for the transaction.
3. Once service invocation history record H has been created, service S reports H to the MTMS. In the service infrastructure, each service S has a partial view of buyer B behaviour based on its interactions with each buyer. By reporting rating to the MTMS, each service reports rating on these interactions to the MTMS when needed. These feedbacks are then supplied to the rating verifier. Each aggregate rating is then made available for trust level evaluations by all services.

- Rating Verifier

An effective verifying scheme, which is able to verify and mitigate various rating related threats to the rating ratings collected, enhances the accuracy of the estimation of trust scores. The following demonstrates the verifying process of determining the rating credibility.

a) Once the verifier receives the rating, it validates the rating ID. The ID is only valid when the users are active in the system. It is considered invalid when the users have not been participating in the system for a specific period of time. This is to avoid any rating coming from fraudulent parties. As it is unique to every user, the rating ID can uniquely identify an individual. Therefore, the verifier could identify whether the rating is from a true or valid provider. Then the rating verifier looks up the rating provider's business profile, including the business details through the history database. Combining with associates parameters, a mathematic verification function is used to determine the weight of the rating.
b) The Rating verifier gets the rating history through the lookup mechanism. The rating provided is compared with the ratings history. These histories alone are insufficient to justify the rating credibility. The trust value of the seller is included in the scheme.

c) The Rating verifier retrieves the trust value information of the seller. Depending on the rating history and the level of trust value of the seller, the rating is assigned with a credibility value, and the credibility values of ratings are sent to the rating database which stores the verified ratings.

- Trust Metric

The main functionality of trust metric used by trust evaluation mechanism is to provide a trust value for users. Trust value is the result of trust evaluation. There are several existing mechanisms that can be applied for assessing trust through past history (Resnick, & Zeckhauser, 2006). We develop a trust metric scheme which consists of verified ratings to evaluate trust. The trust metric evaluates user trustworthiness based on the verified current rating received from users after a completion of business transaction and the past behaviour of a user which is represented as a collection of service history records. The following steps illustrate the process of evaluating trust value of users based on our trust model performing by TMS.

Whenever the system receives a service request from some users, the system send its custom trust level using its trust function defined over a collection of service history records along with the rating identifier to the TMS.

a) Upon receiving feedbacks for some service, the verifier of TMS computes rating credibility over the collection of service history records and returns the resulting to rating storage.
b) TMS computes the trust level of seller S based on these verified feedbacks using its trust evaluation mathematic functions. The trust evaluation offer trust status directly relevant to the product that the buyer is going to purchase.
c) TMS uses trust evaluation factors including rating value, past history, time, product information (such as types of product, cost and warranty) and weighing scale to estimate trust value for each user.

- Trust Data Management

Upon receiving new trust information of users, the trust information is update from the TMS by lookup and update mechanism. In this work, the information regarding trust relationships between buyers and sellers is kept in a trust database. The trust relationship, the users' information, the parameters to evaluate trust, and the access policies are represented as relational entities. All these are translated to tables of the database and the attributes of these entities are expressed as columns in the tables. To prevent overloading, the amount of previously evaluated trust value is deleted based on the recent activity of the services. If inactive service is above a set time by the system, the lookup mechanism checks each service and its membership. Both trust information and the membership of the service will be deleted and then updated.

Trust information has to be kept highly confidential and to maintain its integrity. This means it needs to enforce some form of security mechanism such as access control, credential mechanism, and encryption. When buyer visits seller's web application either login as a user or registered as a new user. Users are authenticated through user id and regular password mechanism. Users are assumed with two different roles namely seller or buyer. User ID and password information is passed to authorisation entity to validate members' ID. If this information and the login table are matched, users are allowed to access the system based on the access control rights they have. If user is new to the system, a registration process is needed in order to register user as a new user to the system. After the authentication process of matching the information is successful, user is authorised to access the trust information of the data storage. The requested trust information of seller is shown. The goal of the access control is to admit only authorized personnel to a particular location. Authentication process relying on one or more authentication factors in an identity-based transaction constitutes an authentication method.

The following algorithm is used to compute the trust relationship with a seller for a given context at any given time:

1. If not already a user, initialize the buyer's information corresponding to the seller and the specific product. If needed, update the same to reflect current circumstances.

2. Initialize access policy with buyer if not already available. Update as needed.

3. Compute credibility of a rating given by buyer
   (a) Read provided rating value
   (b) Read seller trust values from database starting from most recent first of a history table.
   (c) Read buyer trust values from database starting from most recent first of a history table.
   (d) Read information of product interaction.

4. Compute trust value of seller
   (a) Determine last activity in time when trust is evaluated for current seller for the given product.
   (b) Read trust values from database starting from most recent first of the history table.
   (c) Read rating values obtained in steps 3.
   (c) Apply product information to evaluate current trust value.

5. Record current time of trust evaluation.

6. Compute decayed value.

7. Combine trust values obtained in steps 4 - 7 using the weighing factor to get seller's current trust value for the given product.

8. Trust information is updated

- Security management.

A security mechanism (Chonka, et. al., 2008) is implemented to protect the system. The security defense system shows it can protect services from distributed denial of service (DDoS) attack and improve system efficiency. The framework is distributed on each router in the network so that it can provide overall protection. Each Bodyguard is a destination end protector, it provides security as the traffic enters the network. This security framework allows bodyguards to send updated security information to each other (new attacks that each has encountered, for example). it also sends security information down to the next hop for checking application data as it comes into the router (This is to provide better performance, by breaking up the security and application data) and lastly, monitors the performance of each other (So if a successful attack brings down a bodyguard, the next hop router is prepared to handle the security). In general, the main component of the security defense system, which consists of the following objectives: 1) mitigating the problem of distinguishing between normal and DDoS attack traffic, 2) protecting the system, while allowing other applications to run at their full performance potential. 3) Minimising the effect to the performance of applications when there is an attack. Although, system security is not in our focus, the implementation of security mechanism helps improve the effectiveness of trust management in e-commerce. Further investigating into performance over a practical implementation of this framework is required.

4. Conclusions

In this paper, we address the threats and challenges that can compromise the reliability of the current trust management system. It aims to provide the understanding and support for the existing e-commerce trust management system. The proposed multilevel trust management allows unknown parties to access services by showing appropriate credentials that prove their qualifications to get the services. The approach facilitates dynamic updating of trust information to reflect the current or latest behaviour. Also, the decision making is entrusted with the individual user that takes decision based on its own experience and all on the information received from the users. We also show that a trust management system with only one component (e.g., trust value) does not cover all the necessary functions and services. Moving beyond simplistic and vague applications of the notion of trust, researchers are enabled by this framework to recognise when trust is relevant and to address a broader range of elements and process involved in trust assessment. How to merge the trust relationships into the overall e-commerce systems provides lots of challenges for further research. However, we believe that our proposed framework could be used as a helpful tool to model the e-commerce trust relationships.

References

Amland, S. (1999). Risk based Testing and Metrics. International Conference on Testing Computer Software, Washington, D.C., USA.

Chen M. & Singh J.P.(2001). Computing and using reputations for internet rating. In Proceedings of the 3rd ACM conference on electronic commerce. pp. 154-162.

Chong, S-K & Abawajy J.(2010). Risk-Based Trust Management for E-Commerce. In Z. Yan (Ed.), Trust Modeling and Management in Digital Environments: From Social Concept to System Development, pp: 332-351, 2010.

Chong, S-K, Abawajy, J & Dew, R. (2007). A multilevel trust management framework. In 6th IEEE/ACIS *International Conference on Computer and Information Science:* in conjunction with (IWEA 2007), IEEE Computer Society, Los Alamitos, Calif., pp. 776-781

Chonka, A., Chong,S.K., Zhou, W. & Xiang, Y., (2008). Multi-core Security Defense System (MSDS). *IEEE The Australasia Telecommunications Networks and Applications Conference.*

Gregg, D.G. & Scott, J.E. (2008).A Typology of Complaints about Ebay Sellers. CACM. 51 (4).

Jøsang, A. Ismail, R. &Boyd ,C.(2007). A Survey of Trust and Reputation systems for Online Service Provision, Decision support Systems, 43(2), pp. 618-644

Jøsang A. & Golbeck, J.(2009). Challenges for Robust of Trust and Reputation Systems. Proceedings of the 5th International Workshop on Security and Trust Management.

Kerr, R. and Cohen, R. (2007). Towards provably secure trust and reputation systems in e-marketplaces. In Proceedings of the Sixth International Joint Conference on Autonomous Agents and Multi-agent Systems.

Kerr, R. and Cohen, R. (2009). Smart cheaters do prosper: defeating trust and reputation systems. In

Proceeding AAMAS '09 of the 8th International Conference on Autonomous Agents and Multiagent Systems. Vol. 2.

Mäntymäki, M.(2008). Does E-government Trust in e-Commerce when Investigating Trust? A Review of Trust Literature in E-Commerce and e-government Domains. In IFIP International Federation for Information Processing, Towards Sustainable Society on Ubiquitous Networks. pp. 253 -264.

Pittayachawan, S. ,Singh M. & Corbitt, B.(2008). A multitheoretical approach for solving trust problems in B2C e-commerce. International Journal of Networking and Virtual Organisations, 5 (3), pp. 369-395, 2008.

Raza I. & Hussai S.A.(2008). Identification of malicious nodes in an AODV pure ad hoc network through guard nodes. Computer Communications, Volume 31(9), pp. 1796-1802.

Resnick, P. & Zeckhauser, R. (Eds.) (2006). Trust among strangers in internet transactions: empirical analysis of eBay's reputation system. Vol. 11.

Trevathan, J. & Read, W.,(2006). Undesirable and Fraudulent Behavior in Online Auction. SECRYPT'06, pp. 450-458.

Trevathan, J. & Read, W.(2007). A Simple Shill Bidding Agent. Proceedings of the Fourth International Conference on Information Technology, pp.766-771.

Vijayakumar, V. R. S. D. & Abawajy J. (2012). An efficient approach based on trust and reputation for secured selection WahidaBanu of grid resources, Journal of parallel, emergent and distributed systems, 27(1), pp. 1-17.