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.

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.

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

reputation of a provider as either bad or good is discussed in (Jøsang, A.& Quattrociocchi ,W. ,2009). This approach was later extended such that a feedback is considered to be fair if it falls in the range of lower and upper boundaries among all the ratings Jøsang, A. & Golbeck, J.; 2009). The limitation of this strategy is that raters could collude as a group to manipulate the majority ratings. However, majority ratings scheme alone is not sufficient to accurately measure the trustworthiness of a user. The authors (Yu, B. & Singh, M., 2003) proposed models based on assumption that that all customers in the system have provided feedbacks for a given period of time. For example, new users could be treated as bad users and their feedback will carry less weight in trust assessment. Similarity-based filtering technique such as (Jøsang, A. & Golbeck, J., 2009; Whitby, A.; Josang, A., & Indulska, J., 2004) are frequently used to filter out low similarity ratings that are seen as more trustworthy. One of the problems with this approach is that customers can submit ratings with the same value as many as possible to a provider. On the other hand, we think this similarity-based filtering technique method is unfair to customers. Providers who supply a good quality product may not necessarily provide a further different product of similar quality.

3. 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 (shown in Figure 1). 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.

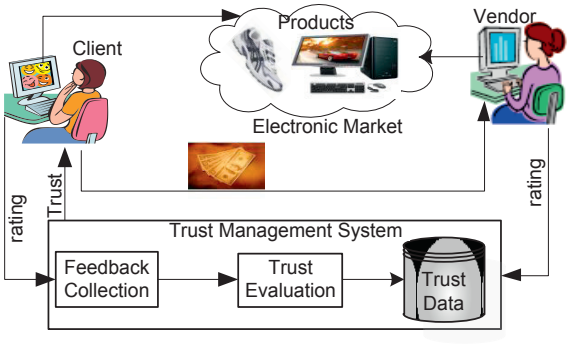

Figure 1: A generic trust management system

3.1 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.

4. Trust Management Requirement

The threats discussed above are relevant to the general requirement upon the reliability of the trust management system. In this section, we address the requirement of an effective trust management system.

4.1. Accuracy of Information

The accuracy of trust value means the correctness or truthfulness of trust information. This also means the estimation of trust value of users is accurate at the time of evaluating. Users have no control over the accuracy of the trust value given by the trust management system. Much of the information needed to compute trust value can be gathered from various sources as mentioned earlier. This information could be accurate or could be designed to mislead the user into falsely trusting the provider. Accurate estimation is crucial for trust management system as accurate trust information improves trust relationships between businesses and end users, as trust between businesses and consumers are crucial to the expansion of e-commerce. On the other hand, inaccurate trust information leads to misinformed business decisions, resulting in poor judgment and bad business outcomes. Trust information can be improved if each user shares her experiences about aspects of the level of services provided by the users she interacts with are truthful. Therefore, the user would like to ensure the accuracy of the supplied information so that trust the party that can be trusted. The main problem when attempting to give users accurate trust values are that the trust information is too general. It provides one single trust value to represent overall services of a provider, but does not specify the trust information of the product which the customer acquires. Transactions in the same amount category can be considered relevant when evaluating a transaction trust bound to a new transaction. For example, a provider may not good in service “A” but excellent in service “B”. Thus, the previous transactions in the same product category should be considered as one of the factors in trust evaluation.

Trust assessment requires gathering more information such as to compute trust information that is represented different services of a provider. Another issue is in online e-commerce environments, the reliability of the trust management system depends on numerous problems such as falsified and biased ratings (Ifinedo, P., 2006). The intention of falsifying rating is to inflate or deflate a vendor/customer’s reputation. Falsified feedbacks can compromises the reliability of the trust management systems and seriously affect the trust level of good providers. While trust management systems are increasingly being used in e-commerce environments, they are susceptible to tampering with ratings. For example, a small percentage of falsified ratings 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 ratings in an open environment such as e-Commerce, it is necessary to have an approach that is able to detect falsified ratings to protect the integrity of the trust management system. Although there have been techniques to encourage trustworthy behavior (Jøsang, A & Golbeck, J., 2009; Yang, Y.; Sun, Y., Ren, J.& Yang, Q., 2007) the general trend in trust management system is to consider all ratings 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. Hence, mechanisms to identify and action falsified ratings and an efficient trust metric that includes all necessary factors is required to improve the current trust assessment techniques. As the quality of trust management system depends on the integrity of the ratings received as input, thus effective protection against unfair ratings is a basic requirement and is an integral part of a robust trust management system.

4.2. Information Security

Security refers to data protection in e-transactions, and is recognized to be a fundamental component in e-commerce as e-commerce has led to a new generation of associated security threats. The trust management system architecture requires the adoption of security measure (Pittayachawan, S., Singh, M. and Corbitt, B., 2008). In the studies dealing with trust framework, protection against malicious attacks and recovery from attacks were highlighted (Mäntymäki, M. 2008).

Once a security breach occurs, your trust system must quickly respond so that the scale of the threat is mitigated, the effects on operations and daily business are minimized. A trust management system must be able to support combination of feedback ratings from multiple users. In order to support high availability the trust management service, all history records managed must also become available for trust level evaluations. It also should support the use of different trust evaluation functions by different users over the same feedback ratings from a completely distributed e-commerce users. In addition, when the interaction about different services increase, the trust information request may increase and increase its complexity of the system to obtain information. Moreover, to keep level of trust value updated, any changes of value from information source which is direct and indirect interaction must be used to update the trust value immediately. The trust management system should have the capability to change dynamically in many different ways that could affect the trust values of different users without changing any other interaction details.

As e-commerce customer accessing information relies on online trust management system, supporting the availability, integrity and confidentiality of this information is crucial. It is difficult, if not impossible, to complete a transaction without revealing some personal data, such as shipping address, billing information, or product preference. Users may be unwilling to provide this necessary information or even to browse online if they believe their confidential information is invaded or threatened. E-commerce trust management systems need to ensure users can securely store critical information, ensuring that it persists, continuously accessible, unchangeable and confidential. Effective countermeasures should be studied and seamlessly integrated with the design of trust management systems. Such as using control to to manage traffic and maintain connectivity during a network intrusion and limiting the consequence and scale of a threat or attack.

5. Trust Management Framework

Trust management systems should have the capabilities for cloud provider to present their service capabilities and allow participants to make assessments and decisions regarding the potential transactions. It is important for a trust management system to have a specific mechanism that accurately evaluates the trustworthiness of cloud providers. This framework incorporates the basic security measures and trust evaluation components that filtering all ratings.

5.1. Access Control

In our trust management framework, implementation of a security defense system (Chonka, A., Chong, S.K. Zhou, W. & Xiang, Y.,2008) shows it can protect be 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 allow bodyguards to send updated security information to each other (new attacks that each has encountered, for example). it also send 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) to protect the system, while allowing other applications to run at their full performance potential. 3) Minimise the affect to the performance of applications when there is an attack. Although, system security is not in our focus, the implementation of security mechanism helps to improve the effectiveness of trust management in e-commerce. Further investigating into performance over a practical implementation of this framework is required.

5.2. Trust evaluation

In addition, malicious rater is addressed by services provider. The feedback verification mechanism takes the raw feedback and combines it with the information of rater's transaction history which is records in the transaction record component. A verifying scheme is used to determine if a feedback is genuine or suspicious. Suspicious ratings are

maintained for further evaluation to determine the weight of the ratings. Also, both genuine and suspicious ratings have a trust score. The feedback verifier does this by using its verifying scheme. It first combining the all transaction information including the customer ID, product ID, and provider ID, timestamp of the rating submit and the rating value. To determine the suspicious rating from the genuine rating, the feedback verifier computes the rating using a verifying scheme. It first examines the majority of ratings from raters whose have high trust value within a timeframe, for example, a day or a week depending on the need of the system. All ratings within this timeframe fall within the set threshold and are considered good ratings because they satisfy the rules for rating credibility. If the credibility of the rating is high, it is considered as good rating otherwise it is group as suspicious ratings. The suspicious ratings are then calculated by the proposed weighing scheme. The feedback manager makes a decision as to how much weight should be given to the rating based on the information from the "transaction record" about past transactions of the rater. All weighted rating scores are then used by the trust evaluator to determine how trustworthy a rater is.

6. Simulation result and discussions

Unlike previous works that require collaboration of trusted participants by providing trusted rating, we suggest methods to distinguish trustworthy feedback from malicious feedbacks. We combined a majority rating scheme with transaction value (size) and the frequency of ratings submitted (the number of ratings submitted for a particular time period) to form a rating verification metric. The filtering mechanism employs this metric is to determine the quality of a submitted rating. The basic idea is that if the ratings received agree with the majority opinion, the past history of the rater is taken into account. This is to eliminate the re-entry issue as it takes time to generate trust value. Therefore, the credibility of the ratings increases if the trustworthiness of rater is high and decrease otherwise. The information of transaction value and how frequent a rater submitting ratings are taken into account as it would prevent the dishonest provider from building up reputation by cooperating in many small transactions and then cheats in a very large transaction.

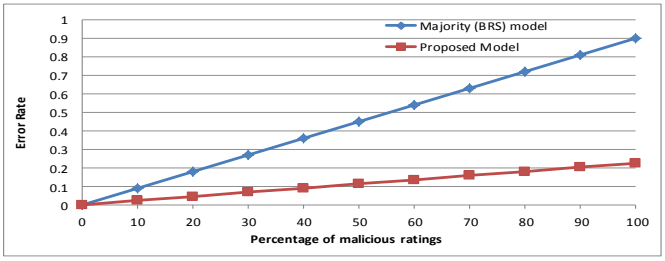

Figure 2

The above Figure 2 shows the result rating credibility is very low compares with the original ratings. Since low majority values are chosen, rating credibility suffers low decrement in the case of dishonest ratings from malicious raters. However, in this scenario, the large number of malicious raters directly affects the majority rating and hence the final assessed reputation. Therefore, the assessed credibility is not close to the performance of using majority ratings. In this case, the majority rating is given a false trust value of a provider.

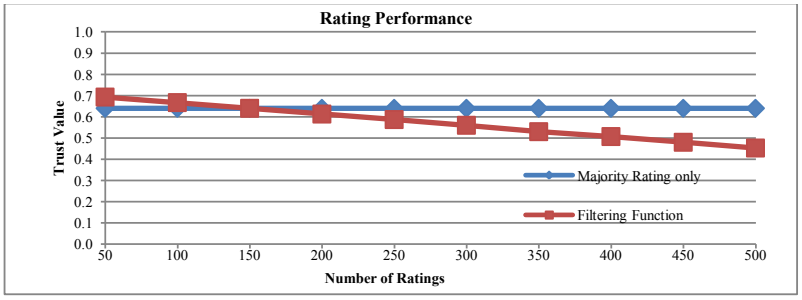

Figure 3

The result in Figure3 shows when trust value of service providers is not relevant to the potential transaction. It also shows when service providers are new in the marker with no trust value. The result shows that the risk indication of the proposed model is higher than the trust reputation-based model at the first half of the result. And all the figures also show that when the percentage of untrustworthy service providers increases the differences of the resulting risk

value of the two models increases as well. This is because of the fact that although trust value is one of the important parameters in transaction risk value assessment, it should not be the only parameter used in transaction risk assessment in online environments.

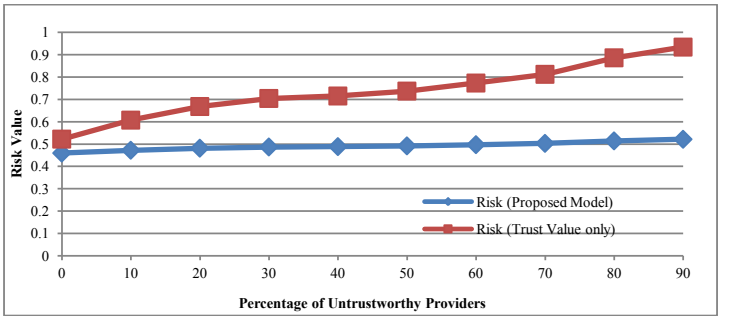

Figure 4

Figure 4 shows the result rating credibility is very low compares with the original ratings. In this scenario, malicious raters are more than the honest raters. The majority ratings are low value. Since low values are chosen, rating credibility suffers low decrement in the case of dishonest ratings from malicious raters. However, in this scenario, the large number of malicious raters directly affects the majority rating and hence the final assessed reputation. Therefore, the assessed credibility is not close to the performance of using majority ratings. In this case, the majority rating is given a false trust value of a provider. The result also shown the aging scale is applied to the testing result but not to the majority ratings performance. The results indicated that applying the credibility filtering function to evaluate the trust value of providers is giving a more accurate performance.

The results also shown the aging scale is applied to the testing result but not to the majority ratings performance. The results indicated that applying the credibility filtering function to evaluate the trust value of providers is giving a more accurate performance. We compared the proposed model against the majority vote model. The result shows that our model is more stable than the majority-based model. The results also indicate the proposed weighing metric produces a stable result even though there were increases. Normally, the results using majority metric remain rigid. From the experiments result, we believe that trustworthiness of rater and provider, age of rating and frequency of rating are important parameters that should be considered in the design of a rating verifying scheme.

7. Conclusion and Future Direction

As e-commerce is growing rapidly with new providers, cloud providers will increasingly compete with customers by providing services with similar functionality. Reliable trust management systems are needed to support users in identifying dependable and trustworthy providers. This paper addressed the problem of feedback related security threats to a trust management system and proposed a method for tackling these threats. We propose an approach that predicates suspicious feedbacks such that the impacts of such feedbacks on the computation of trust level could be minimized. The key contribution of this paper is the design of an approach that verifies suspicious feedbacks with the aims of identifying and actioning feedback-related vulnerabilities. This approach filtered out malicious feedbacks for e-commerce trust management system. We have studied the performance of the proposed trust management system in a simulated environment. Due to limitation of space the information of metrics used is not fully presented.

We believe there is more work remains to be done in developing robust underlying models. We are currently developing a full list of threats against the proposed trust management and analyzing the vulnerability of the system to these threats. How to merge all the trust relationships into the overall e-commerce trust management systems provide lots of challenges for further research.

References

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

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

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.

Dellarocas, C. (2000). Immunizing online reputation reporting systems against malicious ratings and discriminatory behavior. *In Proceeding of the 2nd ACM conference on Electronics commerce*. pp. 150-157.

Fujitsu Research Institute, (2010).Personal data in the cloud*: A global survey of consumer attitudes*. http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf. Accessed July 20 2013.

Habib, S. M. Ries, S. & Muhlhauser, M. (2010). Cloud computing landscape and research challenges regarding trust and reputation," *Symposia and Workshops on ATC/UIC* , vol. 0, pp. 410- 415.

Huynh, T.D. Jennings, N.R.& Shadbolt, N.R. (2006). Certified reputation: how an agent can trust a stranger. In: AAMAS '06: *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems*, pp. 1217–1224.

Ifinedo, P. (2006). Enterprise Systems Success Measurement Model: A Preliminary Study. *Journal of Information Technology Management*, Vol. 17, Iss. 1, pp 14 – 33.

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

Jøsang, A. Ismail, R. & Boyd C.(2007). A survey of trust and reputation systems for online service provision, *Decision Support Systems*, vol. 43, no. 2, pp. 618-644.

Jøsang, A. and Quattrociocchi, W. (2009) Advanced features in Bayesian reputation systems, *Trust, Privacy and Security in Digital Business,* vol. 5695, Heidelberg: Springer, pp. 105-114, 2009.

Jurca, R. & Faltings, B.(2003) An Incentive Compatible Reputation Mechanism. *Proceedings of the 6th International Workshop on Deception Fraud and Trust in Agent Societies* (at AAMAS'03)pp. 1026-1027, 2003.

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,

Sajjan, S. Sankardas R. & Dasgupta, D. (2010). Game Theory for Cyber Security. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research.*

Trevathan, J. & Read, W. (2007) A Simple Shill Bidding Agent. *Proceedings of the Fourth International Conference on Information Technology (ITNG'07)*, pp.766-771.

Whitby, A. Josang A. & Indulska, J. (2004). Filtering out malicious ratings in Bayesian reputation system. *In proceeding 7th Int. workshop on Trust in Agent Societies.*

Yang, Y., Sun, Y., Ren, J. & Yang, Q.(2007). Building trust in online rating systems through signal modeling. *In Proceedings of workshop on Trust and Reputation Management.*