This is the published version (version of record) of:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30008039

Copyright : ©2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.
A Multilevel Trust Management Framework

Soon-Keow Chong, Jemal H. Abawajy and Robert A. Dew
School of Engineering and Information Technology
Deakin University, Geelong, 3217 Vic, Australia
{ skchon, jemal, rad } @ deakin.edu.au

Abstract

Lack of trust in e-commerce transactions has been identified by researchers as one of the main factors that hamper e-commerce from reaching its full potential. Various trust-related supporting features for online transactions are available to improve trust management. However, most of these existing approaches have insufficient conditions to establish online trust among businesses and customers. There are many relevant factors that influence potential buyers to make decisions. In this paper, we identify several desirable properties of an ideal trust management system that existing trust management systems do not support. A multilevel trust management framework is proposed to improve the support for existing trust management in e-commerce.

Keywords
E-commerce, trust management, feedback verification, reputation, trust.

1. Introduction

E-commerce is the process of buying and selling goods and services over the Internet. One of the major advantages of e-commerce is that it provides opportunities to extend businesses to anywhere in the world. While e-commerce provides enormous opportunities, it also presents potential threats and risks due to a lack of trust. Different from traditional businesses, participants in an e-commerce environment are unable to have face to face meetings as they have no prior knowledge of each other and with no legal protection enforcement to reduce the likelihood of business risks. As a result, it is generally believed that lack of trust is one of the main reasons that business transactions in an e-commerce environment are still not living up to their full potential [8].

To mitigate such problems, many trust management systems have been developed in establishing trust between trading partners in e-commerce [5, 6, 7, 11, 13]. Trust management systems compute the trust value of an entity, relying on feedback data received from participating parties [7]. It is supposed to provide ways to increase trust and assist potential buyers in making decisions on e-commerce transactions. However, due to potential manipulations by malicious players and the enormous amount of information updated everyday trust management systems still encounter considerable challenges and are incapable of supporting all different trust relationships to improve users’ confidence.

In this paper, we identify several desirable properties of an ideal trust management system and propose a new multilevel trust management system that fulfills all these desirable properties. The proposed new trust management framework includes a feedback data verification component to ensure the credibility of the feedback provided by the participants, and a dispute resolution mechanism to solve any dispute on feedback received. The rest of this paper is organized as follows: in Section 2, desirable properties of trust management systems are presented. Section 3 introduces the proposed multilevel trust management architecture and shows how it meets these expected requirements. The conclusion of the paper is given in Section 4.

2. Background

2.1 Desirable Properties

Trust is an essential element in all forms of commerce [2, 4, 10]. Although the concept of trust has been addressed within many disciplines (e.g. philosophy, psychology, sociology, transaction economics, and organization theory), no single acceptable definition of trust has emerged. For the purpose of this paper, we define trust to mean the interaction between parties who have little knowledge of each other and must deal with any uncertainty and
risks that are out of their control [12]. The reason for choosing this definition is because it is more appropriate to e-commerce environment.

One of the major problems of existing trust management systems emanate from the feedback data used to compute the reputation or trust-level of an entity. Given that e-commerce have serious vulnerabilities due to potential manipulations by dishonest or malicious players, it is very important to ensure that trust values of entities are accurate and not manipulated by malicious and dishonest participants. The quality of a trust management system depends not only on the accuracy of the trust value it computes, it should able to scale as business transaction load grows, and also maintain system availability that satisfies business needs. Thus, without the following four basic properties of accuracy, security, fault-tolerance and scalability, a trust management system is unable to support all different trust relationships within domains and will not gain participants’ confidence.

- **Accuracy**: Accuracy means the correctness or truthfulness of trust information. Inaccurate data leads to misinformed business decisions, resulting in poor judgment and bad business outcomes. However, accuracy and security are always incorporated in a system. A trust model should have an adequate method to conduct the evaluation process of the trust value of a participant, and these trust records are protected. It should be able to verify and mitigate various feedback-related threats to the feedback data collected. It should also be efficient and effective in detecting and removing the trust vectors belonging to peers that are no longer active, in updating the trust value and its credibility; this is to avoid malicious peers and ensures users receive the most recent trust data.

- **Security**: Trust system should have a security mechanism to prevent unauthorized disclosures and eavesdropping. Must comprise an efficient mechanism to prevent unauthorized disclosures and ensure the integrity of feedback data. The trust model should be able to deal with any threats to the system such as data issues that include preventing malicious players accessing trust information and so preventing manipulation of trust data for financial gain; and the trust model must be able to discover problems from potentially correlated attacks.

- **Fault tolerance**: Trust systems should be configured for fault tolerance to maintain system availability, and it should be able to retrieve information when necessary. If these systems failed to ensure the availability of the applications, businesses suffer loss of customers trust, in addition to financial loss. The impact of downtime varies from business to business, and within a business it varies from application to application. Therefore, a fault tolerant trust system must be able to maintain high availability of the system, and recover in seconds; these are absolute requirements for remaining competitive and ensuring customer satisfaction in an e-commerce environment.

- **Scalability**: To remain competitive, a trust management system’s processing power should be able to grow quickly, providing throughput and reliability as the load of business transactions grows to millions of transactions. Businesses need to improve their performance and scalability of its transaction system to accommodate more transactions and more clients. Thus, a trust system must be able to add new server capacity on demand in order to provide true scalability.

### 2.2 Related Work

Existing trust systems such as eBay rely on feedback submissions from participants who have direct experience about that particular transaction. The trust value of a user is the sum of these individual feedback data, and the system stores and manages the reputation centrally. One major problem of this system is that, in a large and centralized system to which anyone may contribute, and users’ id is the only access control for the system, the accuracy of the trust value of an entity is questionable. Moreover, feedback data can be manipulated by malicious users by submitting fraudulent transactions. Other shortcomings of this system are the central management and processing of data represents a single point of failure, and this results in a scalability bottleneck. The volume of everyday incoming data causes slow response times to counteract new threats to the system.

Other trust systems [11, 13, 14] focus on authentication and authorization. KeyNote computes whether a particular request is authorized by using a given set of policies and credentials, but it does not have a mechanism to compute whether the set of policies and credentials are meaningful, and any permission can be freely re-delegated as it has no control over the delegation. SD3 handles all details needed to authenticate user requests and check whether access should be granted according to the policy, including retrieval of digital certificates and verification of signatures. SD3 security infrastructure has the advantage of producing proofs automatically and is capable of retrieving certificates for use in its proofs. It includes a credential verification module, a policy compliance checker and a negotiation strategy module which is this system’s core. Trustbuilder
includes a credential verification module, a policy compliance checker and a negotiation strategy module which is this system’s core. Similar with SD3, it is a prototype-rating tool that calculates the weights of ratings of e-commerce service providers. Unfortunately, these trust systems only focus on security issues.

The existing trust methods, models and approaches in establishing trust between entities, focus on trust model algorithms for aggregating trust information, and the mechanism for interpreting trustworthiness from the collected feedback data. Others focus on only authentication issues. We have not been able to find any other trust systems that fulfill all desired requirements in which a trust management system should comprise.

3. Multilevel Trust Management Framework

The above requirements are motivated in more detail in this section along with the approach for meeting them. A new multilevel trust management infrastructure that meets the requirements of accuracy, security, fault-tolerance and scalability is proposed. The architecture of this proposed multilevel trust management system is discussed in the following sections.

The proposed multilevel trust management architecture encompasses components such as data collection, verification, evaluation and management as shown in Figure 1. This trust system integrates a feedback data verifying component and a dispute resolution mechanism in order to overcome the limitations. This feedback component is one of the most important components to perform the feedback collection and verification when evaluating the trust level or reputation of a vendor. The Feedback verifier is configured to commence when the value of the feedback is above or below some acceptable level (e.g., very high or very low rating). A dispute resolution mechanism is designated to dissolve any dispute regarding an allegation defective feedback. This dispute resolution mechanism verifies the allegation and provides a general accepted resolution of the dispute.

Figure 1. The proposed multilevel Trust Management Architecture

The proposed multilevel trust management infrastructure makes use of the advantages of UDDI (Universal Description Discovery and Integration) to overcome the limitation of the existing trust models.

3.1. UDDI

UDDI is a service registry architecture that presents a standard way for businesses to build a registry, discover each other, and describe how to interact over the Internet. In this proposed system, UDDI is integrated with Web services to retrieve necessary information needed for trust assessment. At present, IBM and Microsoft are running public registries.

UDDI defines a programmatic interface for publishing (publication API) and discovering (inquiry API) Web services. It presents high level business information. Conceptually, the information provided in a UDDI registry consists of white pages (contact information), yellow pages (industrial categorization) and green pages (technical information about services). IBM UDDI is one of the many implementations of UDDI registries. The infrastructures for Web services are also readily available through well-established application servers like IBM WebSphere, Microsoft .NET Framework or BEA WebLogic. These application servers allow for creating SOAP messages, initiating SOAP invocations, and receiving SOAP invocations. These application servers also provide WSDL generation and interpretation functionality and UDDI connectivity.
3.2. Data collection

Users provide feedback ratings about each service provider’s performance in the transaction it received. These feedback ratings are to be potentially used as a reference. In this proposed system, a feedback data collection component is responsible for collecting all online feedback from raters who use the trust management system. These feedback ratings may include some from malicious users who intentionally enter the system to provide and manipulate feedback ratings as well as those ratings from authorized users who provide untruthful feedback either intentionally or unintentionally. As such malicious ratings are inevitable, thus, the feedback verifier is to verify the feedback ratings provided by raters. The data collection component provides all feedback collected to the verifier for verification.

3.3. Verification

The purpose of feedback verification is to verify the credibility of feedback collected which is needed to improve the support of existing trust management in e-commerce.

All feedback collected are identified with the provider’s unique User ID. When a feedback value is out of an acceptable range, the feedback Verifier checks the ID of the feedback provider. It is assumed that the system keeps track of past feedback profiles of users in the “Feedback” database. The system also maintains the types of businesses that a member is involved in, along with a unique business ID number. The feedback verifier is able to discover Web services by integrating the system with UDDI.

Similar to [15], the verification of feedback is based on the reputation of the transacting individuals, the business type of the participating parties, and feedback history of raters. It is assumed that the system keeps track of past feedback profiles of a user in a Feedback database. The system also maintains the types of businesses a member is involved in, along with a unique business ID number.

This Feedback verifier could be configured to commence when the value of the feedback is above or below some acceptable level (e.g., very high or very low rating). In this case, it checks to see if the rating providers and rated participants are the same individual. This could be achieved by checking the ID of the feedback provider and that of the service provider. Similar to [1], the verifier checks the business type of the service user and the provider to ensure no collusion between them. The profile of the past feedback and the reputation of the feedback provider could be used to ensure the weight level assigned to the feedback. Figure 2 demonstrates the proposed Feedback verifying system.

![Figure 2. The proposed Feedback Verifying system](image)

- a). The first layer of the verification architecture is the authentication layer. Once the verifier receives the feedback, it validates the feedback ID. The ID is only valid when the users are active in the system. It is considered invalid when the participants have not been participating in the system for a specific period of time. This is to avoid any feedback coming from fraudulent parties. As it is unique to every participant, the feedback ID can uniquely identify an individual. Therefore, the verifier could identify whether the feedback ratings come from a true provider or from a feedback provider who impersonates someone else. Then the feedback verifier looks up the feedback provider’s business profile, including the business details through the UDDI directory. This is to ensure no collusion between the rating provider and the service provider. If the business type between the feedback provider and the service provider is the same, this feedback rating is considered suspicious. These two participants might be colluding to provide high ratings to each other. On the other hand, if very low feedback is given, the reason can be the provider tries to force the opponent out from the market. When authentication has been completed, the verifier continues to investigate the feedback at the second layer.

- b). The Feedback Verifier gets the feedback history through the lookup mechanism. The rating provided is compared with the feedback history ratings. The feedback history is insufficient to justify the feedback
credibility. Reputation of the service provider is needed.

c). The Feedback Verifier retrieves the reputation information of the service provider. Depending on the feedback history and the reputation of the service provider, the feedback is assigned with a credibility value, and trust data are sent to the trust data storage.

d). The Access Control Mechanism is implemented to provide access to the trust data storage. It is responsible for maintaining the credibility of feedback data and ensuring that these feedback are properly managed and are available when needed for further usage.

3.4. Feedback Evaluation

The Feedback evaluation component is configured to interact with the lookup and update mechanism, it differs from others approaches. In this infrastructure, trust data analysis does not begin until feedback verification has completed. The trust process component evaluates the trust value of participants and continuously updates each participant’s reputation score. The level of credibility to the feedback rating is assigned depending on the profile of reputation and the feedback history of the service provider. The feedback verification mechanism is associated with the reputation store and the feedback history store. The actual ratings and the feedback history are also taken into account in this trust evaluation process.

In conclusion, trust process includes managing and re-evaluating the trust value based on the historical traces of past behavior of the feedback provider and service provider. Four types of feedback credibility are considered here: good, ordinary, bad and intermittent. Each one has a mean level of performance, except for the intermittent. However, in an e-commerce environment, if a dispute arises such as a feedback provider denies the provision of his feedback rating, the system is not able to be sufficiently resolved by any other means, thus, a dispute resolution mechanism is needed to solve these issues.

3.5 Dispute Resolution

The aim of this Dispute Resolution mechanism is to achieve efficient resolution of feedback rating disputes. It interacts with all others components to settle a feedback dispute. Generally, the process of this mechanism begins when a party such as feedback provider files a complaint, this Dispute Resolution mechanism is able to protect non repudiation. It is then proved that collected feedback has not been changed or altered by any means. Therefore, the feedback provider cannot deny having provided the feedback rating to a particular service provider. The search for a responsible party in a dispute about feedback data often depends on the underlying framework. Therefore, it is essential to initially establish the liabilities of the participants, that is, the identities of the feedback provider and the service providers. This can be achieved by using a symmetric encryption infrastructure.

3.6 Data Management

The Lookup component in this proposed system is configured to interact with users in the Feedback History database and business Web services through the UDDI. When there is a need of information of a particular entity, it sends requests to the Lookup component to find the business information and the feedback history of this particular entity. It is responsible for providing the necessary information of a particular participant when requested by the verifier for the verification process. Similarly, the Update component is also configured to interact with users in the Feedback History database and business Web services through the UDDI. It updates all feedback reputation and feedback history of a participant after new information is received. This component is responsible for supplying the most recent and accurate information to the verifier.

3.7 Access Control Management

Access control is necessary to protect information integrity and prevent information disclosure to any unauthorized users. In this system, every user has to provide sufficient evidence of their identity and also evidence that the identity actually belongs to them to establish the person’s identity. Credential verification can be used to establish the authenticity of users at all level of the management system. Credential evaluation can prevent malicious users from impersonating other participants and credential verification to easily add onto most trust models. The most common technique is every participant generates a pair of public and private key. The access policy is then used to determine who has the privileges to access information storage.

3.8 Security and Fault Tolerance

There are two main concerns with respect to maintaining database availability at all times, the server and the storage availability. While the security component is trying to protect the system from malicious outside attacks, fault-tolerance is trying to
protect it from any faulty system components that can fail the whole system. All components of the proposed framework are configured to be fault tolerant, which allows this system to continue functioning after a component failure. In addition to ensuring that the trust data store in the proposed system is only accessible by authorized users, an external firewall and an intrusion detection system can be used to mitigate denial of service attacks. A firewall protects the system from hackers and the intrusion detection system is used to alert the system if a hacker manages to get through the firewall [9].

4. Conclusion

Various trust management approaches have been developed to improve trust relationships between businesses and end users, as trust between businesses and consumers are crucial to the expansion of e-commerce. In this paper, some desirable properties of an ideal trust management system are identified. A multilevel trust management framework is proposed to improve the credibility of feedback data and the improvement of the correctness of trust data. Value-added access management and a security mechanism are implemented at all levels, meeting all requirements that a trust management system should support. We envisage that this proposed framework increases consumers’ trust and encourages consumers to increase their participation in e-commerce.

5. References


