Reputation-Oriented Trustworthy Computing in E-Commerce Environments

Yan Wang
Macquarie University

Kwei-Jay Lin
University of California, Irvine

The reputation-oriented trust issue is critical to e-commerce applications and has drawn much attention from both industry and the research community. Some e-commerce systems have introduced trust management mechanisms that leave some valuable information to customers. However, more comprehensive mechanisms should be provided to more precisely depict the trust level of sellers and forthcoming transactions, and the relationship between interacting entities. Here, the authors review the reputation-based trust evaluation mechanisms in literature and outline some trust issues that are particularly important in e-commerce environments.

Keywords: trust computing, e-commerce, trust evaluation, reputation

E-commerce has been a popular and growing industry in which buyers and sellers conduct transactions on the Web. Numerous e-commerce companies have created very profitable businesses since pioneering e-commerce traders (such as Amazon.com) or e-commerce Web sites (such as eBay.com) emerged more than 10 years ago.

Recently, *service-oriented computing* (SOC) has emerged as an important technology that has received attention from both the research community and service industry. Using SOC, a spectrum of e-services across server domains might be available to customers in a loosely coupled manner. Customers can look for qualified and preferred services via a registry's discovery capability, invoke one or more of the services in an integrated way, and receive their desired outcome from selected services. Services in SOC might result in a business transaction, such as selling a product online, or a functional execution of a specific Web service, such as responding to a query on a stock quote. Thus, in an SOC context, the notion of service encompasses most e-commerce applications.

In both e-commerce and e-service applications, a seller's reputation is a big concern for buyers prior to placing an order or making a payment. In the abstract sense, *trust* is the extent that one party measures the other party is willing and able to act in the measuring party's interest.[1] It's also the probability by which party A expects that another party B will perform a given action. When a customer looks for a service from a large set of candidates or service providers, the promised quality and the trust placed on that promise are key factors to the customer making the service selections. These factors are also critical for service registries, which are responsible for maintaining recommended lists of reputable and trustworthy services and service suppliers.

An e-commerce support environment can produce the trust value by measuring the delivered service quality as well as service evaluations from customers and trust management authorities. Without any trust-management mechanism, many customers might invoke fraudulent services with deceptive advertisements. On the other hand, a simple but incompetent trust management system could let service providers selectively victimize customers (for example, by providing good services with low-cost transactions but then deceiving customers by offering expensive products) and trust management authorities (for example, by launching collusion attacks in trust evaluations). All such attacks will lead to service quality degradation and monetary loss among customers. Thus, the e-commerce industry must have effective trust management.

Here, we review the reputation-based trust evaluation mechanisms reported in literature and outline critical issues for future research.

Trust Computing Categories

The ICT (Information and Communication Technology) community has actively studied trust evaluation since Stephen P. Marsh's pioneering work in the 1990s.[2] The notion of trust varies in different contexts. Broadly speaking, there are two classes of trust computing: security-oriented trust computing and non-security-oriented trust computing. We can further divide the latter into two subclasses: socially-oriented trust computing and service-oriented trust computing.[3]

In security-oriented trust computing, trust provides a mechanism for enhancing security, covering issues of authentication, authorization, access control, and privacy.[3] Trust is the degree by which a target object (such as software, a device, a server, or any data they deliver) is considered secure, and it has a binary status — that is, secure or insecure.

In both socially oriented and service-oriented trust computing, we can define trust in terms of *trust belief* and *trust behavior.*[1] Trust belief between two parties is the extent to which one party believes that the other is trustworthy in a given situation. Trustworthy means one party is willing and able to act in the other's interest. Trust between two parties is the extent to which a party depends on the other in a given situation with a feeling of relative assurance, even though negative consequences are possible. If a trust belief means "A believes that B is trustworthy," it will lead to a trust behavior, such as "A trusts B."[4]

In both e-commerce and e-service contexts, trust evaluation usually occurs via reputation evaluation based on service, transaction, or interaction history. In the context of socially oriented environments, **some studies have** focused more on depicting and deriving the relationship between interacting parties, and conducting the final trust evaluation. In comparison, service-oriented trust is a mechanism for achieving, maintaining, and reasoning about the quality of services (QoS) and interactions.[3] In this context, in addition to service quality evaluation, **studies** must look at how to evaluate recommendations and recommendation trust.

Reputation-based trust evaluation correlates to both socially-oriented and service-oriented trust computing. In general, a service gains a good reputation after it has accumulated good quality services over a long time period. The evaluation is usually based on customer ratings. However, to compute the final reputation value correctly, studies on relationships among raters and ratees are necessary, and might help reduce the rating noise (which we discuss further later on) and obtain more objective trust results.

Reputation Evaluation on eBay

eBay is a well-known consumer-to-consumer (C2C) e-commerce Web site. Its trust-management mechanism is one of the earliest such systems. At eBay, after each transaction, a buyer can give feedback to the system about the seller's service quality that can be positive, neutral, or negative. eBay stores this rating at a centralized management location. It calculates the feedback score via $S = P - N$, where P is the number of positive ratings left by members (customers) and N is the number of negative ratings. eBay displays the S value on the seller's Web page. Another value $R = (P - N)/(P + N)$ $(1 \geq R \geq 0)$ is the *positive feedback rate*, based on which eBay will reward the seller as a *power seller* if $R \geq 98$ percent (the current threshold).

eBay also provides a table with a seller's rating data for the past 12 months, divided into the most recent one-month, six-month, and 12-month columns. Thus, we can see that eBay's mechanism for trust management and trust calculation is fairly simple, and it also supplies raw data to buyers for their own judgment..

Peer-to-Peer Trust Evaluation

Many researchers have actively studied trust issue**s** in peer-to-peer (P2P) information-sharing networks, in which a client peer must know, prior to downloading data, which serving peer can provide the complete files the client needs. P2P trust evaluation can use a polling algorithm,[5] a binary rating system for calculating a given peer's global trust value,[4,6] or a voting reputation system[7] that calculates the final trust value by combining those values returned by responding peers and the requesting peer's experience with the given peer. As pointed out elsewhere,[8] binary-value ratings work pretty well for file-sharing systems, in which a file is either the complete version or not. In most other studies,[8,9] researchers adopt a numeric rating system with, in which, for example, a rating is in the range of [0,1]. This is more suitable for complex applications, such as service-oriented ones.

Trust Evaluation in Multiagent Environments

Researchers have also actively studied trust issues in multiagent environments. A software agent is autonomous and self-interested, expected to complete the tasks its owner or other agents specified. In addition to evaluating trust in agent interactions (such as transactions in an e-commerce context or services in an SOC one), studies looking at multiagent environments must consider other issues, such as agents' motivations and the influence and dependency relationships among them.[10]

Nathan Griffiths[11] proposes a multidimensional trust model that lets agents model other agents' trustworthiness according to various criteria. This is important in a multiagent collaboration situation. Indrajit Ray and Sudip Chakraborty study a generic vector trust model for developing trustworthy systems that aims to take various aspects into account.[12] The trust vector consists of three elements: the accumulated evaluations in a certain period, the truster's knowledge in a context in which the truster evaluates the trustee, and the evaluating party's trust on trusters. Le-Hung Vu and his colleagues[13] propose a model to evaluate and rank the trust and reputation of QoS-based services, which is quite useful for service search and selection. In particular, their model measures the difference between advertised quality and delivered quality, and users can select good services based on this evaluation..

Management Architecture Types

Choosing a trust management architecture can depend on various factors, such as workload, cost, scalability, reliability, and the nature of trust management tasks. An implementation should weigh each architectures' pros and cons and choose the right one for its applications.

One way to build up a trust management system is via a centralized management server (such as eBay), in which service clients or buyers report ratings to a trust authority after transactions. The server manages providers' and clients' portfolio data as well as service providers' trust data. Another option is a decentralized (such as P2P) architecture for trust management, which also has its benefits.[13]

A centralized management architecture has fewer communication costs because trust computation is based on stored trust ratings. The centralized management architecture does incur costs when setting up the server, and when customers send their feedback. In contrast, a P2P-based architecture doesn't require extra costs to set up separate servers, but once a requesting peer needs to know a service provider's trust status, in general, it must broadcast a request to other peers. Hereafter, the requesting peer will collect trust data and compute the result locally. This process might then repeat whenever a peer wants to know a target peer's trust status. Thus, this architecture is costly in terms of network communication.

The decentralized architecture has another problem — every time a requesting peer broadcasts the request, it isn't likely that all peers with a transaction history with the target service provider will be online and respond. In contrast, in a centralized management architecture, the requesting client can simply communicate with the central trust management server, which stores trust history data, computes the trust value accordingly, and responds to the clients. However, the centralized architecture is subject to the single point of failure, whereas the decentralized architecture is more scalable.

Different from either of these architectures is a distributed architecture, which comprises a set of trust management brokers[14] that partition the data among themselves. This method also helps partition the trust computation workload and provides a more reliable environment because it can ensure a relatively complete data set. However, the collaboration among brokers and the cost to set them up might be the concerns.

Research on New Trust Models

Obtaining objective trust result**s** is a trust management system's ultimate goal. To reach it, **researchers** should explore and develop some new trust models.

General Trust or Transaction-Specific Trust

When a person A trusts person B to drive him to the airport, it doesn't mean that A will trust B to perform other jobs, such as driving the airplane that A will take[2]. In e-commerce, for each new transaction, the *transaction-specific trust* is important to the buyer. Based on a set of previous transactions and trust ratings, new transactions might produce different trust levels given that each new transaction has a different nature.

In most existing trust models, it is to compute a given seller's trust as the *general trust* based on ratings from all previous transactions with the seller in a recent period. This trust value might not indicate exactly the trust level that a new transaction might have which is, however, a consumer's real concern particularly when the seller is unknown.

Assuming the general trust is the same as the transaction-specific trust is misleading and risky. A typical attack in a trust management-enabled e-commerce system occurs when a malicious seller obtains a good reputation by selling low-cost products, then later begins to deceive buyers by selling expensive products and may disappear. Thus, the trust calculation should be bound to the new transaction’s attributes (that is, the goods purchased in the transaction and the transaction’s price) and lead to a transaction-specific trust result. Researchers have studied one method that differentiates transaction price in trust evaluation and can prevent attacks such as the one just described.[15] Researchers should conduct more studies that bind the trust evaluation to other properties of a new transaction.

Recommendation Trust and Its Evaluation

Trust ratings are customers’ local trust data. Once a trust management authority or other customers (such as a requesting peer in P2P environments) receive the data, the rating becomes a recommendation from the receiver’s viewpoint. Thus the rating provider’s *recommendation trust* is a big concern.

Some e-commerce systems (like eBay) use a mutual rating system — after a buyer rates a seller, the seller can rate the buyer as well. However, this could cause buyers to worry about receiving bad ratings if they themselves give a seller a bad rating. The relationship between the rater and the rating receiver is analyzed elsewhere.[16] For example, if the rating receiver and the rater are friends, the former might trust the recommended rating. This relationship can form a chain or a graph if multiple parties are involved.

Other studies assume that transaction trust is somewhat equivalent to recommendation trust[6] or aim to analyze raters’ credibility.[8,9] This can somewhat reduce the bias in trust computation, but these studies calculate credibility from the requesting party’s viewpoint, using its own experience, which yields local and subjective result. Thus, it’s not global and might not be valuable to other service customers. We must develop new approaches to analyzing a rating’s trustworthiness.

One study proposes a role-based recommendation and trust evaluation model,[17] which uses a recommender’s role to evaluate the recommendations he or she gives. This role includes recommenders’ social position, title, or rank reflecting the expertise level, as well as the recommendations’ impact level in the target domain. Typical scenarios from real applications include job hunting, in which a referee for the job seeker plays an important role in terms of how his or her recommendation influences the potential employer. However, when using this realistic role-based framework, knowing how to build up or describe the role hierarchy remains challenging.

Relationship Analysis behind Trust Ratings

One major impediment to obtaining objective trust results is rating noise, which can occur when a friendship or competitor relationship exists between a rater and ratee, leading to low accuracy ratings. For example, if a rater is a friend of the ratee, his or her rating might be overly high. On the other hand, if the rater is a competitor (or a friend of a competitor) of the ratee, the rating might be overly low.

Traditional studies focus more on analyzing the trust rating data itself, which might identify the noise statistically. We think the analysis should consider some additional relationships as well. We can adopt data mining and social network analysis (SNA) techniques for this purpose, based on graph theory and algebra for analyzing social relationships between individuals.[18] Massive quantities of data are available via blogs, e-commerce sites, social networking sites, newsgroups, chat rooms, and so on. These networks typically have tens of thousands to millions of nodes and contain sufficient information for assembling into analysis models.[19] By applying SNA, we can analyze various parties’ relationships and enhance our abilities to trace colluding attacks in trust evaluations.

Of the three models discussed above, the first utilizes transaction parameters to inspect only relevant ratings, whereas the second and third improve rating data’s accuracy. The latter two models go beyond the basic trust network model to explore socially oriented relationships. Further study on these topics might require developing new and extended theoretical models to manage the complex issues behind trust.

Trust management in e-commerce will remain challenging for some time because the issues and solutions surrounding it are so complex. Not only do technical solutions require effectiveness and efficiency, but we must take into account cultural, psychological, and social factors and their impact on trust evaluations. Researchers in the ICT field should cooperate with social scientists to find sensible technical solutions.

References

1. D.H. Knight and N.L. Chervany, *The Meaning of Trust*, tech. report WP9604, Univ. of Minnesota, 1996.
2. S. Marsh, *Formalising Trust as a Computational Concept*, University of Stirling, 1994.
3. N. Griffiths, “Trust: Challenges and Opportunities,” *AgentLink News*, no. 19, 2005, pp. 9–11; URL: http://www.agentlink.org/newsletter/19/AL-19.pdf

4. L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," *IEEE Trans. Knowledge and Data Eng.*, vol. 16, no. 7, 2004, pp. 843–857.
5. E. Damiani et al., "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks," Proc. of ACM Conference on Computer and Communications Security (CCS 02), ACM Press, 2002, pp. 207–216.
6. S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," *Proc. World Wide Web Conf.* (WWW 03), ACM Press, 2003, pp. 640–651.
7. S. Marti and H. Garcia-Molina, "Limited Reputation Sharing in P2P Systems," ACM Conference on Electronic Commerce (EC 04), ACM Press, 2004, pp. 91–101.
8. B. Yu, M.P. Singh, and K. Sycara, "Developing Trust in Large-Scale Peer-to-Peer Systems," *IEEE 1st Symp. Multi-Agent Security and Survivability*, IEEE CS Press, 2004, pp. 1–10.
9. Y. Wang and V. Varadharajan, "Trust^2: Developing Trust in Peer-to-Peer Environments," 2005 IEEE International Conference on Services Computing (SCC 05), IEEE CS Press, pp. 24–31.
10. T. Huynh, N. Jennings, and N. Shadbolt, "An Integrated Trust and Reputation Model for Open Multi-Agent Systems," *Autonomous Agents and Multiagent Systems*, vol. 13, no. 2, 2006, pp. 119–154.
11. N. Griffths, "Task Delegation using Experience-Based Multidimensional Trust," *Proc. 4th Int'l Joint Conf. Autonomous Agents in Multi-Agent Systems* (AAMAS 05), ACM Press, 2005, pp. 489–496.
12. I. Ray and S. Chakraborty, "A Vector Model of Trust for Developing Trustworthy Systems," *Proc.* of the 9th European Symposium Research Computer Security (ESORICS 04), LNCS 3193, Springer-Verlag, 2004, pp. 260–275.
13. L.-H. Vu, M. Hauswirth, and K. Aberer, "QoS-Based Service Selection and Ranking with Trust and Reputation Management," International Conference on Cooperative Information Systems (CoopIS 05), LNCS 3760/3761, Springer-Verlag, 2005, pp. 466–483.
14. Y. Zhang, K.J. Lin, and R. Klefstad, "DIRECT: A Robust Distributed Broker Framework for Trust and Reputation Management, *Proc. IEEE Joint Conf. E-Commerce Technology* (CEC 06) *and Enterprise Computing, E-Commerce, and E-Services* (EEE 06), IEEE CS Press, 2006, pp. 21–28.
15. Y. Wang et al., "Evaluating Transaction Trust and Risk Levels in Peer-to-Peer E-Commerce Environments," *J. Information Systems and E-Business Management*, vol. 6, no. 1, 2008, pp. 25–48.
16. G. Zacharia and P. Maes, "Trust Management through Reputation Mechanisms," *Applied Artificial Intelligence J.*, vol. 9, issue no. 9, 2000, pp. 881–907.
17. Y. Wang and V. Varadharajan, "Role-Based Recommendation and Trust Evaluation," *Proc. IEEE Joint Conf. E-Commerce Technology* (CEC 07) *and Enterprise Computing, E-Commerce, and E-Services* (EEE 07), IEEE CS Press, 2007, pp. 278-295.
18. F. Martino and A. Spoto, "Social Network Analysis: A Brief Theoretical Review and Further Perspectives in the Study of Information Technology," *PsychNology J.*, vol. 4, no. 1, 2006, pp. 53–86.
19. S. Staab et al., "Social Networks Applied," *IEEE Intelligent Systems*, vol. 20, no. 1, 2005, pp. 80–93.

***Yan Wang** is a senior lecturer in the Department of Computing at Macquarie University, Australia. His research interests include trust computing, e-commerce, software agent and security. Wang has a PhD degree in computer engineering from Harbin Institute of Technology, China. He is a member of IEEE. Contact him at yanwang@ics.mq.edu.au.*

***Kwei-Jay Lin** is a professor in the Department of Electrical Engineering and Computer Science at the University of California, Irvine. His research interests include service-oriented architectures, e-commerce technology, and real-time systems. Lin has a PhD in computer science from the University of Maryland at College Park. He is a senior member of the IEEE. Contact him at klin@uci.edu.*