Trust Management Framework for Distributed E-Business Environment

A.Kannammal
Coimbatore Institute of Technology, Coimbatore 641014, TN, INDIA
kannaphd@yahoo.co.in

and

N.Ch.S. N. Iyengar
School of Computing Sciences, VIT University, Vellore 636 014, TN, India,
nchsniyr@gmail.com

Abstract **- Today's electronic systems face important problems of security and trust. In a paperless e-business environment, the lack of legal documents with signatures and other identification proof of authorized business entities introduce the problem of non-repudiation and security which arises as a result of lack of trust. Proper mechanism to ensure trusted e-business transactions is a much-felt need of the moment. This paper introduces the design of a new trust management framework for distributed e-business environment. The approach followed is a hybrid of policy based and reputation based models that ensure trustworthy business transactions to be carried out between the business entities. Detailed design of the framework and procedures are described with an indication to the future direction of research.**

Keywords- **Trust Management, Distributed E-Business, Trusted Transactions**

I. INTRODUCTION

Evolution of information technologies and the Internet has transformed the e-business into dynamic e-business with security and trust as primary requirements. In a conventional business system, involved parties directly know each other face-to-face, or atleast have proper legal documents with signatures and other proof to securely conduct business transactions. But in an e-business environment, there is a strong need for establishing the trust among the business parties to conduct business transactions electronically, so that the power of latest technologies can be utilized for business growth. The e-business environment must be able to ensure the trust value by any means that puts forth a strong trust management mechanism in place. Without proper trust management mechanism, the involved parties, either a seller or a buyer basically, may invoke fraudulent activities, thereby causing loss to the other.

The lack of proper trust management mechanism may lead to collusion attacks, deceptive behavior, opportunistic behavior, etc. Many companies like e-bay, Amazon now offer e-transaction evaluation platforms to facilitate trusted e-business transactions. A system based on reputation must be present to help users locate trustworthy partners and do business transactions securely with confidence. The effectiveness of a reputation system depends on the trust model behind the system. E-bay is a typical example for reputation based system that is built on centralized model of trust, in which every entity in the centralized model would have the same opinion. The other trust model is called as Transitive Trust Model, in which the recommendation from the recommender is highly emphasized for the trustworthiness. These models have some drawbacks like: most of the models in existence today are developed for the purpose of file-sharing, and hence are not suitable for e-commerce

applications, the trust and reputation are based on long-term behavior and hence are not dynamic to reflect the current behavior, many latest attacks like puffery and slandering attack are not addressed by the previous models. In this paper, a trust model suitable for today's e-business environment that spans across the globe is presented with detailed architecture and algorithms.

II. RELATED WORK

In general, trust management is based on the reputation models built on previous history of experience from others and from one's own experience. A model based on reputation is described by Shmatikov and Talcott [2], which analyzes user's behaviors and categorises them. A reputation based trust management for P2P networks is designed by Selcuk et. Al [3]. A reputation based trust management framework is designed for sensor networks also, by Ganeriwal and Srivastava [4]. This framework formulates a community of trustworthy sensor nodes based on their behaviors and also evaluates the trustworthiness. Though many systems and frameworks have been designed based on reputation models, these mechanisms do not prevent users from giving false information while making a reputation. Also, sufficient information is not available regarding the new users who have not in business for a long period of time or just started doing business online.

Other kind of systems come under the category of policy-based trust management systems, that rely on trusted third parties like Certification Authorities and the digital certificates to determine the trust of a business entity. Based on access control rights and policy rules on hand, the users are allowed to access resources or to conduct business [5]. eBay is a well-known consumer-to-consumer ecommerce 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. eBay's mechanism for trust management and trust calculation is fairly simple, and it also supplies raw data to buyers for their own judgment [7]. Cheng Su et. al [8] combined P2P trust model and e-transaction characteristics, presented a new P2P-based trust model for e-commerce. By computing interactive experiences, recommendations of other peers, risk factors and the transaction context, the model evaluates every peer's global trustworthiness in order to guide transaction participants. However, all the work in this area considers dynamic updating of the trust level based on current experiences in real-time [6]. These mechanisms are built on static behavior and algorithms to evaluate trust.

III. PROPOSED FRAMEWORK FOR TRUST MANAGEMENT

In this paper, a framework is designed that facilitates e-business transactions to be conducted in a trust-worthy manner, globally.

A. General Architecture

The proposed architecture offers the merits of previous trust management systems by combining the approach of Trusted Third Parties, Policy-Based and Reputation-Based models. It also facilitates real-time trust management in a globalized manner. Figure 1 depicts the environment for which the proposed solutions are designed. This model has a component called Central Trust Authority (CTA) which maintains the trust information of all the entities involved in electronic business. The different kinds of entities present in the system are: the customers with different roles as buyer and seller, the organizations which do business electronically that also act as Intermediate Trust Authority (ITA), and the Certification Authority (CA). Electronic marketplaces can also play the role of ITA. A trusted third party that is free from any commercial

transactions can also play the role of ITA. The main functionality of ITA is to retrieve trust information from the CTA on behalf of individual customers. The CTA is assumed to have members from different countries to formulate the rules and policies. The CA is an international independent body that issues digital certificates and keys as an authority. Also, other assumptions made are, CA, CTA, ITA are trustworthy and provide proper available information whenever required for the purpose of verification, decision making or to handle legal issues.

The entities that want to do electronic business should get a digital certificate from CA. The details of digital certificates issued are maintained by CTA along with the rating value for trust information. The customers do transactions with ITA. The ITAs update the trust rating information in their own database and also update the same information in the CTA for the corresponding entity. The ITA can also request information from CTA to analyze the trust rating of an entity. The ITA can get the information from other ITAs in case if the CTA is busy for some reasons. If the ITA is an individual organization, it can analyze the information received from the CTA along with information that is available in its own database. This is a kind of Peer-to-Peer based model of trust management that combines with the centralized model. An individual customer can contact an ITA which is not a business organization, for getting the information regarding the entity with which it wants to have business relationship.

The approach followed here is a decentralized one where the information regarding a particular entity is available with a number of ITAs with whom it has conducted business transactions earlier. After getting the trust information, the customer can analyze and take a decision on whether he can do business transactions with the selected e-business organization. Assumptions behind the realization of this model are: CA, CTA, ITA are trustworthy to provide proper available information. The functionalities of each of the major components are depicted in Figure 2.

B. General Architecture for Trust Management in ITA

The trust management system in each of the ITAs is described in this section. This architecture is based on the distributed objects model. Various objects are used in a distributed manner to update and maintain trust information of customers. Figure 3 depicts the architecture with components and their interface. Trust Management System is responsible to capture and update

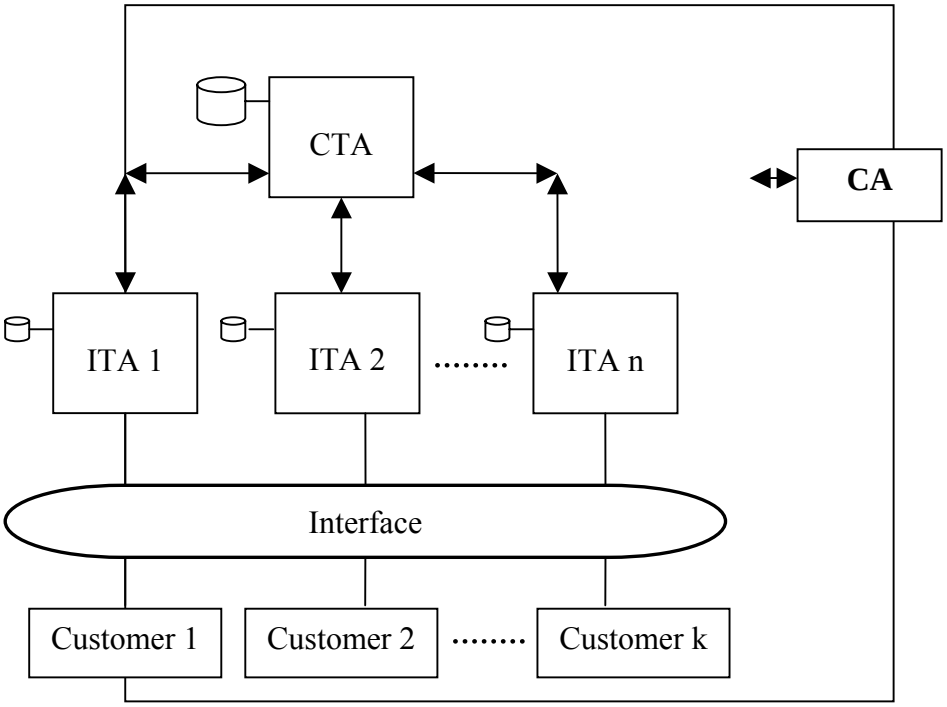

Fig. 1 General Architecture for Trust Management

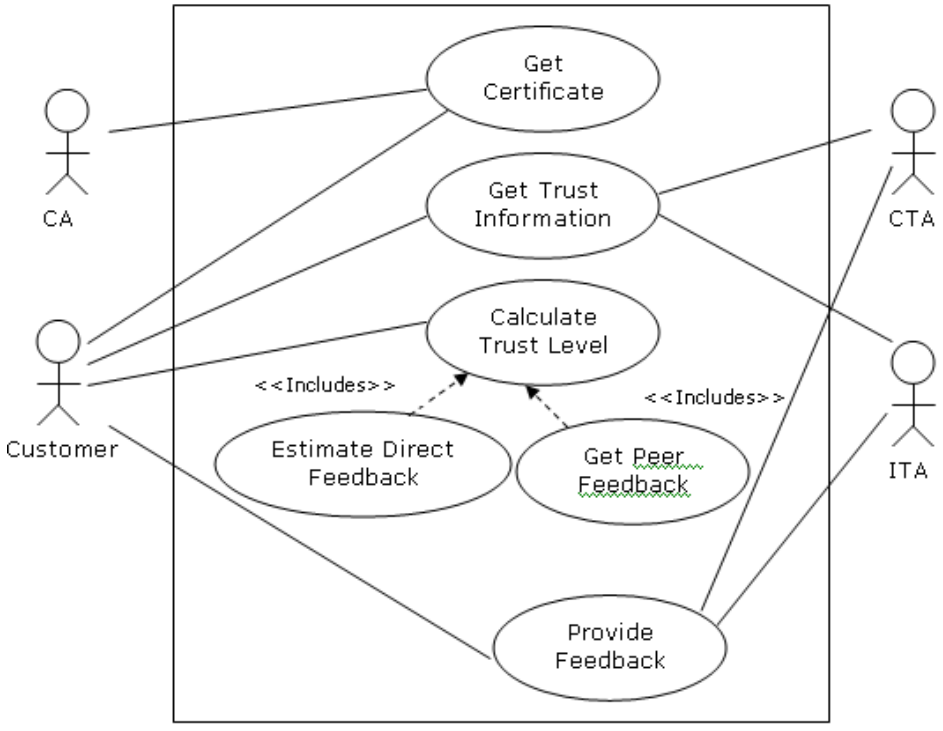

Fig. 2 Use Cases for the Business Entities

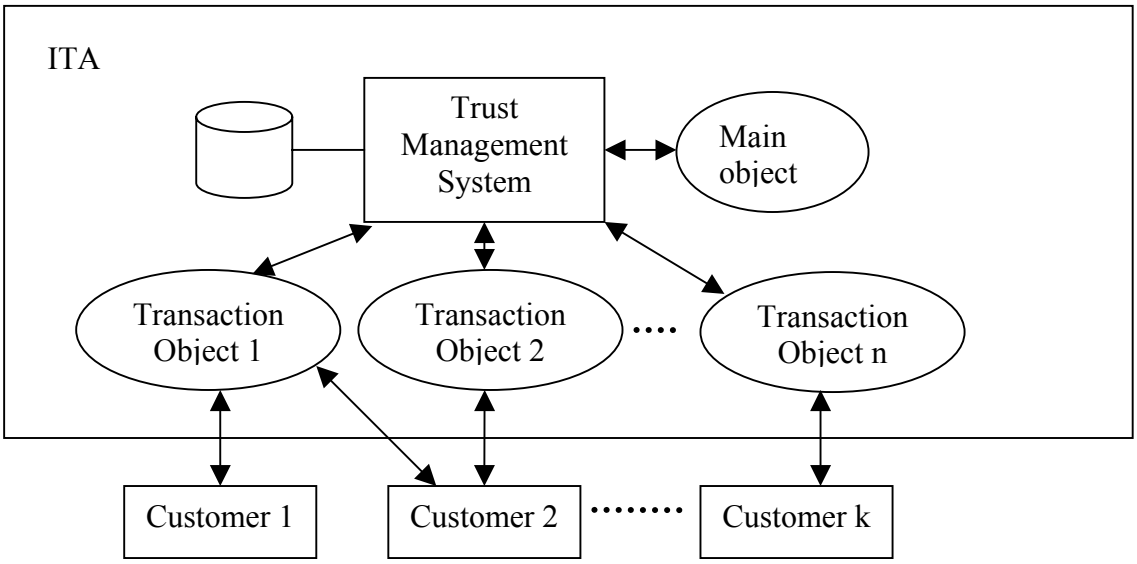

Fig. 3 Architecture for Trust Management in ITA

trust information from the transactions. The Main object provides an interface to the administrator of the system to manage the transactions, to create and initialize transaction objects whenever a client initiates a transaction. For each transaction, one transaction object is created; these objects are distributed in nature, collaborating with each other and also with the trust management system. Users can involve in more than one transaction at a time.

The trust management system allows only authenticated users to do the transaction. The users are authenticated through the regular password mechanism. Also, the user should have a minimum credential to enter into the system. After the user is authenticated, they are allowed to access the system based on the access control rights they have. Users are assigned with specific roles with permissions for access to particular object or service in the system. Users can assume two different roles namely seller or buyer. Initially, they can only purchase or they can only assume the role of a buyer. Only after certain number of transactions successfully completed with the minimum value specified, they are allowed to take the role of a seller. During the initial phase, which can be called as a learning phase of the system, the sellers provide feedback of the buyers based on the transactions completed as explained in section IV-A.

The feedback details are maintained in the database, as transaction history which includes: the transaction date, transaction value, payment mode and other details. The buyers when they evolve as sellers after a specified number of transactions with the specified transaction value can give feedback for the seller also. By regularly updating the feedback information, the trust level information is maintained up to date. If any entity misbehaves, then its trust level is reduced by negative feedback and it can improve its trust level afterwards by its improved behavior. Also, information is outdated after some threshold period of time to reflect the current behavior of a customer. The feedback details, provider of feedback like who has given what feedback about who are kept as confidential. Apart from maintaining the feedback details, the system maintains details regarding changes in the roles, permissions and trust level of a particular customer so that

sufficient history about the users' behavior can be provided for analysis whenever required.

IV. PROCEDURAL DESIGN OF TRUST MODEL

In the proposed model, the trustworthiness is calculated based on customers' direct experience and feedback from other peers. It includes three major steps namely: estimate trust level based on direct experience, calculate trust level obtained from peers and determine final trust level. Each of the steps is explained in the following sections.

A. Feedback Mechanism Design

The feedback is given over a range of values from 0 to 1, where 1 represents the most trustable and 0 represents the most un-trustable customer. Initially, when the customer wants to do transaction first time, the value of the feedback is set to 0 to indicate that no information is available regarding the trustworthiness of the customer. The trust level can be modified dynamically during the course of transactions, thereby reflecting the current or latest behavior of an entity. The access control mechanism specifies, apart from user id and password, whether the user with specified trust level is allowed to assume the requested level.

B. Estimate Trust Level Based on Direct Experience

The estimation of trust level is done through the direct experiences with the entity in question. The main factors affecting this estimation are: transaction satisfaction, number of transactions, transaction value and transaction date. The transactions carried out during a particular period in the recent past alone are considered for evaluation. Let TL_d denotes the trust level based on direct experience, S_d denotes the satisfaction level based on direct experience, ∂ denotes the relative significance of transaction date and N_{th} denotes the number of days in the past during which the transactions have significance. Older transactions have lesser significance than the newer ones, and hence ∂ ranges from 0.1 to 1.

Then for each transaction,

if (current date - transaction date < N_{th})
then $TL_d = \partial * TL_p$
else $TL_d = (1- \partial) * TL_p$

where TLp is the trust level estimated in the past based on direct experience.

Hence TL_d can be calculated as,

$$TL_d = S_d + \partial * TL_p + (1- \partial) * TL_p$$

C. Calculate Trust Level based on Feedback

In this case, only peers who have a trust level greater than a threshold value are requested for feedback information. Let TL_f denotes the trust level based on feedback from peers. Suppose $I = \{I_1, I_2, \ldots\ldots\ldots, I_n\}$ be the set of ITAs that provide trust information regarding an entity. Let TL_i denotes trust level estimated by peer i, Ag_i denotes the aggregate weight of TL_i. Then the trust level based on feedback from peers can be calculated as

$$TL_f = \frac{\sum_{i \in I} Ag_i \, TL_i}{\sum_{i \in I} Ag_i}$$

Sometimes, the customer if he feels that the feedback information may not be proper, then he can even ignore the lowest and highest ratings and can taken an average of all the information received. To measure the credibility of a peer that provides trust information, a honesty probability may be attributed to each customer and the customer with the highest honesty probability can be given higher significance. This honesty probability can be assigned based on the

number and value of the transactions carried out by the customers.

D. Determine the Final Trust Level

Now the customer has to aggregate the results of above two steps: trust level based on direct experience and the trust level based on feedback from peers. Then TL, the final trust level can be calculated as

$$TL = \rho * TL_i + (1 - \rho) * TL_i$$

where ρ reflects the weights of direct and feedback estimation. ρ ranges from 0.1 to 1. It is upto the customer to give proper significance to his own experience and to the feedback information.

Customer makes the decision based on the above mechanism. Initially, customer needs some learning period to get fundamental information about the entity. If no information is available, buyer can select randomly. After the transaction is over, the selected seller's rating is updated.

V. CONCLUSION

In this paper, a framework is designed that facilitates e-business transactions to be conducted in a trust-worthy manner for today's e-business environment that spans across the globe. The proposed framework presents a hybrid architecture that offers the merits of previous trust management systems based on Trusted Third Parties, Policy-Based and Reputation-Based models. The approach facilitates dynamic updating of trust information to reflect the current or latest behavior. Also, the decision making is entrusted with the individual entity that takes decision based on its own experience and all on the information received from the peers. This work can be further enhanced by implementing it for a real time application and analyzing the performance issues.

REFERENCES

[1] CMU, "Online Auction Fraud: Data Mining Software Fingers Both Perpetrators and Accomplices", ScienceDaily, December 5, 2006.

[2] V. Shmatikov and C.Talcott, "Reputation-Based Trust Management", Journal of Computer Security, Special Issue on Selected Papers of WITS 2003 (ed. Roberto Gorrieri), Vol.13, No.1, 2005, pp.167-190.

[3] A.A.Selcuk, E.Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks", Proc. The 4th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid 2004), Chicago, USA, April 2004.

[4] S.Ganeriwal and M.B.Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks", Proc. The 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004), Washington DC, USA, pp.66-77.

[5] P.A.Bonatti, C.Duma, D.Olmedilla, et. Al., "An Integration of Reputation-Based and Policy-Based Trust Management", Proc. The Semantic Web Policy Workshop, Galway, Ireland, Nov 2005.

[6] S.Ruohomaa and L.Kutvonen, "Trust Management Survey", Proc.The iTrust 3rd International Conference on Trust Management, May 23-26, 2005, Rocquencourt, France, Springer-Verlag, LNCS 3477, May 2005, pp.77-92.

[7] K.J.Lin, Yan Wang, "Reputation-Oriented Trustworthy Computing in E-Commerce Environements", IEEE Internet Computing, July/Aug 2008, pp.55-59.

[8] Cheng Su, Hong Zhang, Fang-ming Bi, "A P2P-based Trust Model for E-Commerce", IEEE International Conference on e-Business Engineering (ICEBE'06), 2006.