Credibility Based Corrective Mechanism for Reputation Computation in Peer to Peer Communities

V. Valli Kumari, B. Dinesh Reddy, T. Sri Devi, Ramaprasad R. Kalidindi and KVSVN Raju

Department of Computer Science and Systems Engineering, AU College of Engineering,
Andhra University, Visakhapatnam-530003, India.

Abstract
Trust plays a key role in each transaction in online peer–to–peer (P2P) communities. Transaction based trust computation is an insufficient mechanism when the number of transactions is less. Reputation plays a major role when a peer transacts with other peers for the first time. Reputation computation which is very close to the reality is very important to all the online transactions. Several methods were proposed in the literature for reputation computation. The mechanism discussed in this paper offers a weighted feedback based reputation computation. In case, a malicious peer deceives by exaggerating or underrating the feedback, the method includes a dynamic corrective procedure, which forces a peer to give correct feedback. Thus, this mechanism attempts to solve the reputation computation problem with minimum overheads of storage and retrieval.

Key words: *Peer to peer systems, reputation based trust, credibility based corrective mechanism.*

1. Introduction

A tremendous growth in P2P decentralized electronic communities has motivated users in sharing files, buying and selling products online. As P2P communities have no centralized control, it is possible that some peers misbehave with other peers thus resulting in loss of trust in electronic transactions as well as denial of service attacks and distribution of various viruses. Sometimes when a transaction occurs, the buyer is more vulnerable to risk about quality of the product or its delayed delivery. Though some peers in the electronic communities may be malicious, many of the remaining may be honest. The main purpose of our work is to minimise ratings given by bad peers against good peers.

To do this a good reputation computation mechanism close to reality is required[8]. When a peer has had very few or no interactions with a particular peer, reputation computation of that particular peer needs to be done. When a peer Q wants to decide if transaction can be done with peer T, it has to depend on past transactions with T. This may be termed as the trust Q has got on T. If there is no sufficient past experience, it has to depend on reputation of T which is a weighted aggregate of other peers' feedback. The more the reputation, the more reliable the peer is. It is mostly that a peer that is honest in a few transactions or with a few peers, may not be so always. For instance, misbehavior may vary depending on how big the amount is. Some peers may misbehave at transactions involving big amounts and might behave genuinely with small amount transactions. Some peers may give wrong feedback about a peer thus lowering its reputation. Similarly, exaggerated feedback is possible. This would result in wrong reputation computation, ultimately downgrading or exaggerating a peer's reputation. This becomes a problem for online consumers and it is a form of online fraud [12]. Thus a corrective mechanism is required which would force the misbehaving peers' contribution towards reputation computation to be minimized.

The mechanism discussed in this paper attempts to solve the reputation computation problem, with dynamic correction. The simulation results with highly dynamic peer behaviors, changing malicious feedbacks and the dynamic corrections are presented. The feasibility of this mechanism with respect to minimum overheads of storage and retrieval are also discussed.

This paper is organised as follows: Section 2 discusses the related work, Section 3 presents the reputation computation mechanism, Section 4 gives the storage and retrieval overheads, and Section 5 covers the dynamic correction and simulation results.

2. Related work

An extensive review on trust in peer to peer systems is given in [6][9]. The review categorizes the whole literature on trust in P2P systems into two broad categories: reputation based and trade based. It also puts forth a discussion on possible attacks in P2P systems. In reputation based trust schemes, a peer's reputation is determined by other peers' opinions. In trade based trust schemes peers contributing to other peers are remunerated directly or indirectly.

As the current work is based on reputation based trust scheme, the rest of the section focuses on literature related to this category only. Work in reputation based trust is essential to identify the correct recommender. One solution to obtain this is to consult a central, trusted third party that has had previous experience with the agent and can provide a reputation value. Citing the problems with centralized systems, most research focuses explicitly on decentralization for reputation management.

Let us consider an example of a file sharing system in P2P network. Each peer plays two roles, the role of file provider offering files to other peers and the role of user using files provided by other peers. In order to distinguish this when a peer acts as a file provider we call it service provider otherwise simply as an agent or a consumer. In the trust computation scenario, each provider has reputation which is an aggregate of feedbacks (ratings) given by other consumer peers. Every consumer peer has a rating capability to rate the providers. Thus every peer has two roles: file provider, and consumer and these two roles are associated with reputation and rating respectively.

If particular agent does not have any experience with the file provider, it would ask other agents' who had interaction with the file provider with the same criteria. In this way it can take a decision on its own rather than depending on centralized system.

Trust decision can be a transitive process, where trusting one agent requires trusting another associated agent. For example one might trust a thing because of brand, and the brand may be trusted only because of the recommendation of a friend. Computation of transitive trust depends on reputation values. If there is no link between pair of entities, it means no trust decision has yet been made. This is the case in which trust transitivity can be applied. For example if A trusts B and B trusts C, then A trusts C.

Abdul-Rahman and Hailes [1] proposed a distributed trust model containing trust generalisation and recommendation, which was the basis for many later papers. Several models discussed in [6] are based on boolean relations or fuzzy logic, techniques to analyse unfair behaviour, model based on eigen trust algorithms and trust propagation schemes.

The P2Prep system [11] gives protocols and algorithms for sharing reputation information with peers in a P2P network. This work also uses the idea of referral trust in its approach. XRep protocol was proposed in [12] allows for an automatic vote using user's feedback for the best host for a given resource.

Xiong and Liu [4], [5] give a reputation based trust supporting framework-*peertrust*. They define a trust metric based on three parameters: feedback a peer receives from other peers, the total number of transactions a peer performs, the credibility of the feedback sources and two adaptive factors (context factor and community context factor). They also identify that previous literature is based on two assumptions as below and that the second one need not be true:

i) Untrustworthy peers have a higher probability of submitting false or misleading feedback in order to hide their own malicious behavior.
ii) Trustworthy peers are believed to be honest with a high probability on the feedback they provide.

So, they came out with another trust metric based on querying peer's personalized experience. Srivatsa *et. al.*, [3] proposed Trustguard, a highly dependable reputation-based trust building framework, which focused on vulnerabilities of a reputation system, like fake transactions, dishonest feedback etc.

Trust plays a major role in several application areas. It is not a new research topic in computer science, spanning areas such as security and access control in computer networks, reliability in distributed systems, and recommendations in recommender systems. The concept of trust in these different areas differs in how it is evaluated, represented and used.

This paper is based on peertrust of Xiong and Liu [4][5], in that it computes reputation in the same manner as they do. But is different, in that we use a new approach to compute credibility. This credibility based computation also includes corrective procedure. While they have computed credibility based on assessment of other peers[7][10]. This paper computes credibility based on assessment of other peers as well as their relative assessment. As number of malicious peers increase, getting correct reputation value is difficult. This paper contains a mechanism to give less weight to the malicious peers as the number of malicious peers increase.

3. Reputation System

3.1 Feedback

Trust is believed to be subjective and that it cannot be calculated directly [2]. In electronic communities it is computed based on successful transactions. The model discussed in this paper suits any electronic commerce scenario. But the explanation is based on a file provider-consumer application. The application as introduced in section 2, has the peers assuming two roles, of that of a file service provider/vendor and a file consumer. And any peer can act as either the file provider or as a consumer, but not both at the same

point of time. The consumer gives ratings to the providers from whom the services were consumed. The ratings may be based on download speed, quality etc. or are based on number of transactions done. An aggregate of these ratings gives the reputation of a particular file provider. The terminology used in the remaining sections is given below.

Target (T) is a peer with which transaction is to be performed.
Requester (Q) is a peer which wants to do transaction with target.
Recommender (R) is a peer which had transactions with the target and is providing feedback to the requester.
Vendor (V) is a peer with which both requester and recommender have transactions.
Feedback (f) is defined as the ratio of satisfaction and the number of transactions performed. Satisfaction normally depends on the content quality, quality of service etc. Requester requests the recommender for information about the target. The recommender provides feedback based on the transactions it has performed with the target.
Reputation (Rep) is defined as the combined feedback that other peers give to a particular peer. Reputation and feedback can be measured.

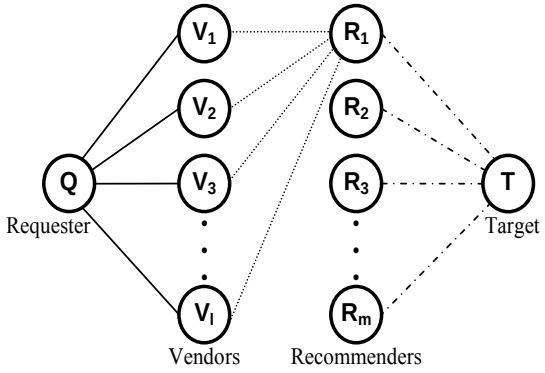

Fig. 1. Reputation in Peer to Peer Network

In the figure 1, Q is the requester, T is the target, R_1, R_2, R_3,.., R_m are recommenders and V_1, V_2, V_3,.., V_l are the vendors with whom R_1 and Q have interactions.

Let *j* and *k* be any two peers, then feedback (*f*) about *j* given by *k* is represented by f_{jk} and is computed as below.

$$f_{jk} = \frac{\sum_{i=1}^{n} S_{jk_i}}{n} \quad \text{.....(1)}$$

where *n* is the total number of transactions performed by *k* with *j*. S_{jk_i} represents the satisfaction of *k* on *j* in i^{th} transaction. This measure is assigned by the peer based on the quality of the transaction. And its value is always assumed to be between 0 (*not satisfied*) and 1 (*completely satisfied*).

Assume a peer Q wants to do transaction with a peer T as in figure 1. Trust of Q on T is usually based on the number of successful transactions done. As in the first few interactions there is no sufficient information to determine trust, Q computes reputation of T and determines if further transactions can be done or not.

Let R_1 and Q be two peers who have transactions with set of peers V_1, V_2, V_3, .., V_l. The feedbacks given by R_1 and Q are shown in Table 1.

Table 1: The feedbacks given by R_1 and Q on a set of peers

Peers	$\mathbf{V_1}$	$\mathbf{V_2}$	…	$\mathbf{V_l}$	T
$\mathbf{R_1}$	$f_{V_1R_1}$	$f_{V_2R_1}$	…	$f_{V_lR_1}$	f_{TR_1}
Q	f_{V_1Q}	f_{V_2Q}	…	f_{V_lQ}	---

--- Represents no transactions had been preformed by Q with T.

A good feedback on T by R_1 means that R_1 has good trust on T. There are two cases in which the recommender R_1 may give wrong feedback about target T to the requester Q. First if R_1 wants to boost the product related to T then it may exaggerate its feedback (to a value often more than its actual trust value) or may downgrade by giving wrong feedback (to a value often less than his actual trust value). In both the cases R_1 is said to be behaving maliciously. So a peer is rated as a good peer if it gives correct feedback. If a peer gives feedback which does not reflect its trust then it is called as a malicious peer. Feedback given by good peer is to be given high weightage and feedback given by a malicious peer should be given low weightage. Trust of a peer about another given peer is known to itself and if not communicated is unknown to other peers. Hence, it is difficult to say whether a peer is good or malicious. To overcome this problem distance vector and correlation are used in this paper to calculate credibility of a peer giving feedback. The method also incorporates a corrective mechanism, if the feedbacks are from more number of malicious peers.

3.2 Similarity Assessment

Distance vector can be used to find relationship between two peers and assessment about the same service. If the distance vector yields a small value then their assessment is assumed to be similar. If the distance vector yields a large value then their assessment is thought to be dissimilar.

Distance vector (Dv_{R_1Q}) has value between 0 and 1 for 'N' common vendors and is computed as:

$$Dv_{R_1Q} = \sqrt{\frac{\sum_{i=1}^{N}\left(f_{V_iR_1} - f_{V_iQ}\right)^2}{N}} \quad \ldots\ldots\ldots(2)$$

If Dv is small then assessment of R_1 and Q are similar. If Dv is large then assessment of R_1 and Q is dissimilar. Based on the application the threshold values α and β are defined such that $0<\alpha<\beta<1$. The values of these thresholds are defined based on the three ranges. If $0<Dv<\alpha$, then Dv is small hence the objects on which it is computed are assumed to be similar. If $\alpha<Dv<\beta$, then the similarity cannot be defined, hence we go for correlation measure. If $\beta<Dv<1$, then the objects are assumed to be dissimilar.

Correlation is used to find the similarity between assessments of two peers. Correlation is a numeric value which lies between -1 and 1.

Correlation (Cor_{R_1Q}) is computed as:

$$Cor_{R_1Q} = \frac{\left(N\sum_{i=1}^{N}\left(f_{V_iR_1}\times f_{V_iQ}\right)\right)-\left(\sum_{i=1}^{N}f_{V_iR_1}\times\sum_{i=1}^{N}f_{V_iQ}\right)}{\sqrt{\left(N\sum_{i=1}^{N}\left(f_{V_iR_1}\right)^2-\left(\sum_{i=1}^{N}f_{V_iR_1}\right)^2\right)\times\left(N\sum_{i=1}^{N}\left(f_{V_iQ}\right)^2-\left(\sum_{i=1}^{N}f_{V_iQ}\right)^2\right)}} \quad (3)$$

Cor_{R_1Q} will be more if increasing values of Q map with increasing values of R_1. In other words if Cor_{R_1Q} is large when relative assessment of R_1 and Q is same on the set of peers. That is, if $f_{V_1R_1} > f_{V_2R_1} > f_{V_3R_1}$ and $f_{V_1Q} > f_{V_2Q} > f_{V_3Q}$, then we can say the relative assessment of R_1 and Q are same. Both R_1 and Q agree that peer V_1 is more reliable than any other peer, and less reliable peer is V_3. If Cor_{R_1Q} is more, then both Q and R_1 agree on relative feedback on set of peers. If Cor_{R_1Q} is less, then it is assumed that both Q and R_1 do not agree on relative feedback on set of peers. Thus, to find the credibility of a peer's feedback we use both distance vector and correlation. Table 2 gives the relationship between assessment of two peers.

Table 2: Correlation

Range	Relationship
$Cor_{R_1Q} \geq 0.5$	Strong
$0< Cor_{R_1Q} <0.5$	Medium
$Cor_{R_1Q} <0$	Weak
$Cor_{R_1Q}=0$	No

3.3 Credibility

Credibility factor gives information about to what extent the feedback f_{TR_1} is dependable. Cr_{R_1Q} represents the credibility factor of R_1 with respect to Q, when $\{V_1,V_2,V_{3,..,}V_l\}$ are the common vendors. It is assumed that credibility factor lies between 0 and 1. Using Dv_{R_1Q} and Cor_{R_1Q} we calculate the credibility factor (Cr_{R_1Q}) as shown in Table 3. Nf_{TR_1} represents normalized feedback.

Table 3: Relationship according to Correlation value

Cor_{R_1Q}	Dv_{R_1Q}	Cr_{R_1Q}	Nf_{TR_1}
≥ 0.5	$Dv_{R_1Q} < \alpha$	1	f_{TR_1}
<0.5	$Dv_{R_1Q} < \alpha$	$1 - Dv_{R_1Q}$	f_{TR_1}
≥ 0.5	$\alpha \leq Dv_{R_1Q} \leq \beta$	1	$\min(f_{TR_1} + \frac{\sum_{i=1}^{n} f_{V_iQ} - \sum_{i=1}^{n} f_{V_iR_1}}{N}, 1)$
any	$Dv_{R_1Q} > \beta$	$1 - Dv_{R_1Q}$	f_{TR_1}

If both requester and recommender do not have common vendors we cannot calculate distance vector and correlation. So we take credibility factor as default value and it is dependant on application.

3.4 Reputation

Let $Rep_{R_1R_2}$ represent reputation of R_1 with respect to R_2. $Rep_{R_1R_2}$ may not be equal to $Rep_{R_1R_3}$. Let 'N' be the number of peers which have been already interacted with R_1 and peers be $\{V_1, V_2, V_3, .., V_N\}$

$$Rep_{R_1R_2} = \frac{\sum_{i=1}^{N}\left(f_{R_1V_i}\times Cr_{R_2Vi}^{\rho}\right)}{\sum_{i=1}^{N} Cr_{R_2Vi}^{\rho}} \quad \ldots\ldots..(4)$$

Cr_{R_1Q} represents the credibility factor of R_1 with respect to Q and its value is between 0 and 1. ρ is a value greater than 0 and depends on the application. The inclusion of ρ results in minimizing the participation of low credibility peers in the reputation computation. If ρ is 1, then the feedback is weighted according to the credibility of the specified peer. In

this case, even though a peer with high credibility gives a positive feed back, if several low credibility peers give negative feedback, the reputation will deviate more from the high credibility peer's recommendation.

Hence, in a given scenario, if all are highly credible peers, equation (4) may be used directly for reputation computation. But if there is a considerable number of peers who are malicious or have low credibility, and less number of peers with high credibility, ρ may be assigned with a value greater than or equal to 2. This would minimize the feedback of malicious peers on the reputation computation.

4. Storage and Retrieval overheads

The model was implemented in JADE. The number of peers was initially varied from 10 to 100. Each peer was programmed to behave like a file provider as well as a consumer. The results were encouraging. The requester Q initially broadcasts its request about feedback on T. The peers (Recommenders) that have already had transactions with T respond. The recommenders send the list of vendors they have had transactions with, along with ratings(feedback) about each of those vendors. Q finds a list of common vendors with each recommender and computes similarity between itself and the recommender using the distance vector and correlation. The extent of similarity is called credibility. The feedbacks of the recommenders are now adjusted according to their credibility.

The experiments lead to the following observations:

a) Each peer needs to store i) a list of vendors it has had transactions and ii)the corresponding ratings. This results in storage overhead.

b) Each requester has to broadcast its message to as many peers as possible. This corresponds to the communication cost.

c) Each responding rater needs to send a list of vendors and the corresponding ratings. This accounts for the communication cost.

d) Each requester needs to compute distance vector and correlation for each of the responding peers. This results in storage overhead.

Table 4: Storage and Communication costs

Np-number of peers, Nr-number of recommenders Ap- Average number of peers with which a recommender has done interactions with	
Storage Cost	Communication cost
Peers with which transactions done + Total number of interactions + Sum of satisfaction	Broadcast of message + feedback sent by recommender

5. Dynamic Correction

While most of the studies carried out in literature base their discussion of reputation on malicious peers behaviour, we base our discussion on the numbers of malicious peers contributing in reputation computation. The equation given in (4) allows minimizing malicious peers contribution by adjusting the value of ρ. In the real electronic communities correcting the malicious peers behaviour is practically difficult. Instead of correcting each such malicious peer, if their impact can be minimised, it would be more practical.

In the simulations carried out, feedback ratings for a good peer were collected. It was assumed that malicious peers give bad ratings and good peers always give good ratings. Several simulations have been carried out on peers numbering from 100 to 10000, for varying values of ρ, and varying percentages of malicious peers. The results are shown in the following graphs. Figs. 2 to 4 show the varying reputation, when ρ is varied from 1 to 5. When ρ=1, credibility is taken as it is. When ρ=2 to 5, credibility of a given malicious peer reduces drastically. When ρ=5, least weightage is given to the malicious peers' feedback. Now the question arises as to which peer should be treated as a malicious peer. The simulation experiment has generated feedbacks, such that 90%, 75%, 50%, and 0% peers are malicious. A peer was treated to be malicious if its credibility fell below 0.5.

In Fig. 5. all the peers were assumed to be good peers. The reputation computed for varying values of ρ was the same.

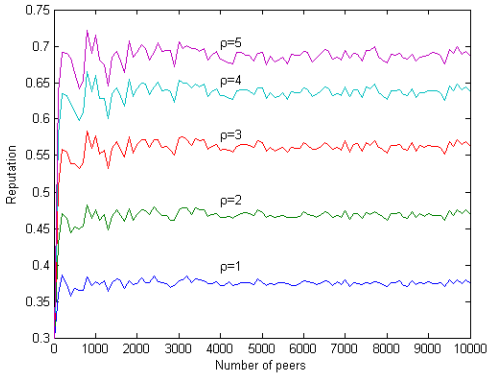

Fig. 2. Reputation with 90% Malicious Peers

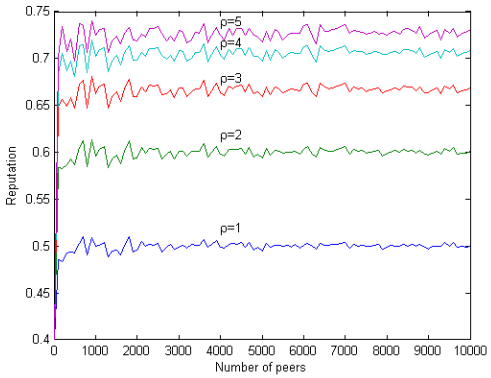

Fig. 3. Reputation with 75% Malicious Peers

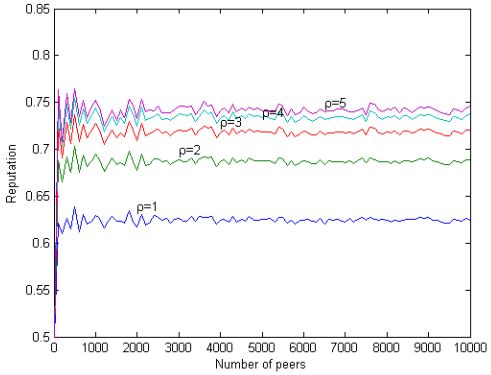

Fig. 4. Reputation with 50% Malicious Peers

In Fig. 6, a comparison of the reputation when computed with varying sizes of malicious peers is plotted.

The following were the observations made from the above plots. When the all the peers are good, irrespective of the value of ρ, the reputation is the same. So, no correction needs to be done. But if it is known for a given application that the most of the peers are malicious, the value for ρ may be high. If it is known that the peers are a mixture of both malicious and good in same proportions, ρ may be fixed to 3. If it is believed that all are good peers, then ρ=1. So, the correction is done based on the electronic communities in general and are not specific to a particular malicious peer.

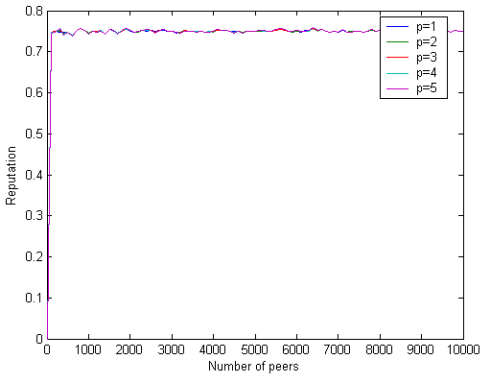

Fig. 5. Reputation with 0% Malicious Peers

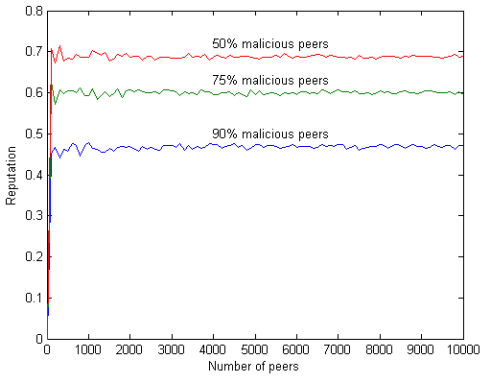

Fig. 6. Comparison of varying Reputation for 90% 75% 50% Malicious Peers when ρ=1

6. Conclusions and Future work

Feedback based reputation computation is mostly used in electronic communities. But much of the published work is based on considering an aggregate of weighted feedback. Most of the papers consider correction of malicious peers by giving incentives for positive feedbacks. This paper addresses the issue in a different perspective. We put forward the corrective mechanisms that are close to reality and that people normally use in daily transactions. When a peer is malicious, correcting him takes a high effort and more storage overheads. Even if, a peer is corrected, there is no guarantee that in the next rating, feedback is given honestly. Moreover, a few peers give malicious feed backs intentionally, and yet a few more may give wrong feedbacks unintentionally. In electronic

communities there may be several peers who should be monitored constantly. So, it is felt that that such a mechanism is not feasible practically. The mechanism suggested in the paper considers the communities in general, and allows reputation correction based on the type of community the particular peer belongs to. The simulation results that support our claims have been presented.
The possible extensions for this work could be in the direction of improving the credibility computation based on context.

References

[1] Abdul-Rahman, A. and Hailes, S., "Using recommendations for managing trust in distributed systems," *Proceedings of the IEEE International Conference on Communication,*1997.

[2] Wang. Y. and Vassileva J., "Bayesian network trust model in peer-to-peer networks," *Proceedings of the 2nd International Workshop Peers and Peer-to-Peer Computing,* Melbourne, Australia, 2003.

[3] Srivatsa, M., Xiong L. and Liu L., "Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks," *Proceedings of the 14th International Conference of World Wide Web*, pp.422-431, 2005.

[4] Xiong L. and Liu L., "Peertrust: Supporting reputation based trust of peer-to-peer electronic communities," *IEEE Trans. on Knowledge and Data Engineering,* 16(7):843-857, Jul. 2004.

[5] Xiong L. and Liu L., "Building trust in decentralized peer-to-peer electronic communities," *Proceedings of the International Conference on Electronic Commerce Research (ICECR-5),* 2004.

[6] Zhu B., Jajodia S. and Kankanhalli M.S., "Building trust in peer-to-peer systems: A review," *International Journal on Security and Networks*, Vol. 1, Nos.1/2, pp.103-112, 2006.

[7] Yu, B. and Singh, M. P., "A social mechanism of reputation management in electronic communities." *Proceedings of the 4th International Workshop on Cooperative Information Agents* (*CIA'00)*, pp.154-165, Springer-Verlag, 2000.

[8] Nielsen, M. and Krukow, K., "Towards a formal notion of trust," *Proceedings of the 5th ACM SIGPLAN International Conference on Principles and Practice of Declarative Programming (PPDP'03)*, pp.4-7, 2003.

[9] Artz D. and Gil Y., "A survey of trust in computer science and the semantic web," *Journal of Web Semantics: Science, Services and Agents on the World Wide Web,* 5(2):58-71, 2007. DOI: 10.1016/j.websem. 2007.03.002

[10] Yu B. and Singh P.M. "An evidential model of distributed reputation management," *Proceedings of the Autonomous Agents and Multiagent Systems (AAMAS'02),* pp.294-301, 2002.

[11] Cornelli F. and Damiani E., "Implementing a reputation-aware Gnutella Servent," *Proceedings of the International Workshop on Peer-to-Peer Computing,* pp.321-334, Springer-Verlag, 2002.

[12] Gregg D.G. and Scott J.E., "A typology of complaints about e-bay sellers," *Communications of the ACM,* 51(4):69-74, Apr. 2008. DOI: 10.1145/1330311.1330326

V. Valli Kumari received her B.E. degree in Electronics and Communication Engineering and M.Tech. and PhD degrees in Computer Science and Systems Engineering all from Andhra University, India and is currently working as Professor in the same department. Her research interests include Security and privacy issues in Data Engineering, Network Security and E-Commerce. She is a member of IEEE and ACM and is a fellow of IETE.

B. Dinesh Reddy received the B.Tech. degree in Computer Science and Engineering and is currently pursuing his Masters with Department of Computer Science and Systems Engineering at Andhra University, India. He is working in the Department of Computer Science and Engineering at VIIT, Visakhapatnam, India. His areas of interests include Security Engineering and Computer Networks.

T. Sri Devi received the B.Tech. degree in Computer Science Engineering from Jawaharlal Nehru Technological University, India. She is currently pursuing her Masters in Computer Science and Technology with Department of Computer Science and Systems Engineering at Andhra University College of Engineering, Visakhapatnam, India. Her main areas of interests are Security and Privacy.

Ramaprasad Kalidindi received the B.E. degree in Electronics and Communication Engineering from Andhra University, India and M.Tech. degree in Computer Science and Technology from IIT, Roorkee, India. He is currently doctoral candidate in the Department of Computer Science and Systems Engineering at Andhra University, India. He is working in the Department of Computer Science and Engineering at SRKR Engineering College, Bhimavaram, India. He is a member of ACM and IEEE Computer Society. His research interests include security and privacy in sensor networks and trusted computing.

KVSVN Raju received the B.E. degree in Electrical Engineering from Andhra University, India and M.E. degree in Control Systems from Andhra University, India and obtained the PhD degree in Computer Science and Technology from IIT, Kharagpur, India. He is currently working as Professor in the Department of Computer Science and Systems Engineering at A.U. College of Engineering, Visakhapatnam, India. His research interests include Data Engineering, Security Engineering and Software Engineering.