International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

# A Novel Routing Protocol to Enhance Trust in P2P Networks

**Uppula Nagaiah[1], G. Kiran Kumar[2]**

[1]M.Tech student, Department of CSE, Anurag Group of Institutions, Hyderabad, India

[2]Assistant Professor, Department of CSE, Anurag Group of Institutions, Hyderabad, India

**Abstract**: ***Accessible and hidden nature of peer to peer system makes it an ideal forum for traducer to spread malignant content. Managing trust is a problem in peer to peer environment, so a novel trust model is built supported on trust metrics. The trust metrics such as service trust, reputation and recommendation trust are defined to precisely measure trustworthiness of peers. A peer's trustworthiness is evaluated by considering provided services and given recommendations with service and recommendation contexts. An interaction is evaluated based on importance, recentness and three parameters: satisfaction, weight, fading effect, when evaluating recommendation, recommender's trustworthiness and confidence level about the information provided are also considered. Experiments on file sharing application demonstrate that peers with the highest trust value are considered and build the trust model in their contiguity and insulate malignant peers.***

**Keywords:** Peer-to-peer systems, trust management, reputation

## 1. Introduction

Peer systems accomplish tasks by relying on collaboration. P2P systems are exposed to security threats, due to lack of central authority and dynamic in nature. In case of secure environment, building up of trust relationship can reduce the risk and reliable in future interactions. The fundamental challenges for peer-to-peer (P2P) systems is to manage the risks involved in interaction and collaboration with priory unknown and potentially malignant agents. In case of malignant environment, establishing trust is a most difficult task. Moreover, trust is a social phenomenon i.e. firm confidence in the reliability and difficult to measure with numeric values. Benchmarks are needed to symbolize trust. Ranking of peers is necessary so that trustworthiness can be displayed based on metrics defined.

The measurement of trust depends on interactions and feedbacks of peers. Interactions with a peer afford specific information but feedbacks might contain illusive information. Peer to peer is a decentralized network architecture in which each peer can act as a server for sharing of resources. P2P systems can be classified into two groups: unstructured and structured. In unstructured P2P, a limited number of connections are maintained by each peer to other neighboring peers in the network. Searching in an unstructured P2P environment leads to flooding queries in the network. In structured P2P systems, a hash function is used in order to couple keys with objects. To hold the relevant objects, distributed hash table (DHT) is used to route key-based queries efficiently to peers.

In this paper structured p2p is implemented, because all the peers are organized into a clear logical overlay. A novel trust model is proposed that intent to decrease malignant activity in a P2P system by establishing trust relations among peers in their contiguity. Local view of trust is developed by its own based on the past interaction. Thus, good peers form energetic trust groups in their contiguity and can isolate malignant peers. In novel trust, at the beginning of the process the peers are assumed to be strangers. Only after providing a service, a peer becomes an acquaintance of another peer e.g., file uploading. The peer chooses to trust strangers if it has no acquaintance. Each peer has a set of acquaintances, a subset of which is identified as its neighbors. Using a service of a peer is an interaction, which is evaluated based on priority, and recentness of the interaction and contentment of the requester. An acquaintance's observation about a peer, recommendation, is estimated based on recommender's honesties. It contains the recommender's own experience about the peer, data collected from the recommender's acquaintances, and the recommender's confidence level in the suggestion. If the confidence level is low, the recommendation has a low value in evaluation.

Novel defines three trust metrics. Reputation metric represents the belief in the system and allows parties to build trust, or the degree to which one party has confidence in another within the context of a given purpose or decision and is calculated based on recommendations. The service trust metric is used for selection of service providers. The recommendation trust metric is needed when requesting recommendations. When calculating reputation metric, recommendations are evaluated based on recommendation trust metric. Outline of the paper is as follows: Section 2 discusses the related research. Section 3 explains the proposed model. Section 4 presents the result analysis. Section 5 summarizes the proposed work.

## 2. Related Work

Trust model creation based on following trust principles such as,

a) Trust is content-dependent.
b) Negative and positive belief is supported.
c) Trust is based on past experience.
d) Information exchange through recommendation.
e) Different opinions of all the agents are considered.

f) Recommendations may increase or decrease the trust level [2].

Reputation is the opinion of the public towards a person or organization or resources. In p2p, reputation represents the opinions nodes and expectation about an agent‟s behavior based on data or observations of its past behavior. In this, the users rate the reliability of parties they deal with, and share this data with their peers. Reputation trust identifies the malicious responses from benign ones by using reputation of peers provided by them. Peer‟s past transactions are stored in trust vectors, which are of constant-length, binary vector of l bit i.e. (8, 16, 32). A 1 bit represents an honest transaction; 0 represents a dishonest one.

Reputation-based trust management properties:
a) No central coordination. No central database.
b) No peer has a global view of the system.
c) Global behavior emerges from local interactions.
d) Peers are autonomous.
e) Peers and connections are unreliable.

Two types of ratings are performed;
1. Trust rating = (trust vector) 2 /$2_m$. ($2_m$→ used for conversion)
2. Distrust rating = (complement of trust vector) 2/ $2_m$ [3].

A lightweight mechanism that allows the data originator to build up trust in the replica holder by means of protocols that do not require past trust or key establishment. The protocol does not prevent cheating and is based on a checksum or hash that is calculated over key-defined ranges of shared data. This check is performed in an iterative fashion with alternating roles, or compensated by the calculation of responses to challenges to prevent DoS attacks [4].

A peer provides trustworthy service and trustworthy feedback. Service is evaluated based on the parameters (file bandwidth, transaction time). Feedback may provide either good or bad values. Reputation system help peers decide whom to trust before undertaking a transaction. Each peer is designed with two sets of reputation ratings; an aggregated service rating ranging from -1.0 to 1.0 with 0 as neutral rating; an aggregated feedback rating ranging from 0 to -1.0 with 1.0 as good rater. Initially, s-rating is set to zero and feedback to 1.0 for all the peers. A reputation system maintains for each peer a list of peers that has rated it. Defined as;

$$s\text{-}rating(u) = \alpha * s\text{-}rating(u) + \beta * (ru * f\text{-}rating(i))$$
$$f\text{-}rating(u) = 1 / nu * \_nu\ i{=}1\ fu * f\text{-}rating(i)$$

where *ru* indicates a service rating of -1 or 1; *fu* is the feedback rating which can be 0 or 1 depending on malicious feedback or helpful feedback; *n u* represents the total number of transactions that have made use of u‟s feedback; and $\alpha$ and $\beta$ are normalized weight factors, between 0 and 1, used to exponentially decompose reputation ratings. A peer may exhibit honest and dishonest ratings. Once a peer has established a good reputation in the network, it can neglect it, and an honest peer may start behaving in a dishonest way too. Thus peer reputation must be of more recent rating interaction rather than old ratings [5]. A peer-to-peer system is ad-hoc and dynamic: the challenge of these systems is to design a mechanism and architecture for organizing the peers in such a way so that they can cooperate to provide a useful service to the community of users. In a file sharing application, all the peers are organized into a cooperative, global index so that all content can be quickly and efficiently located by any peer in the system. In order to evaluate this peer-to-peer system, the characteristics of the peers that choose to participate in the system must be understood and taken into account [6].

Peer to peer information sharing environments are increasingly gaining acceptance on the internet as they provide an infrastructure in which the desired information can be located and downloaded while preserving the anonymity of both requestors and providers. Reputation sharing is done based on a distributed polling algorithm by which resource requestors can assess the reliability of perspective providers before initiating the download; also it keeps the current level of anonymity of requestors and providers, as well as that of the parties sharing their view on other's reputation [7]. In absence of central database, manage trust in a peer-to-peer network is tedious, which is based on binary trust values, i.e., a peer is either trustworthy or not. In case a dishonest transaction occurs, the peers can forward their complaints to other peers. To store the complaints in a peer-to-peer network, special data structures namely the P-Grid are needed to be designed [8]. An agent uses own experiences when building trust and does not consider information of other agents [9]. Each peer stores its own reputation using signed certificates. This approach eliminates the need for reputation queries, but it requires a public-key infrastructure [10].

An algorithm is introduced to classify users and assign them roles based on trust relationships [11]. Reputation systems are vulnerable to incorrect and false feedback attacks. Thus feedback ratings must be based on goal criteria [12].Trust and distrust metrics are defined. A nonzero distrust value lets an agent to distinguish an untreated user from a new user [13]. Reputation is been used as a currency. A central agent issues money to peers in return for their services to others. This money can be used to get better quality of service [14]. A history of interactions is stored and considers ratings and recentness of interactions when evaluating trust. Number of interactions with a peer is a measure of confidence about the peer [15].

## 3. Proposed Frame Work

### 3.1 Introduction of trust model

Trust is a degree of belief. Based on principles of trust, trust model is created. In this design, multiple peers are connected and interact with one another for file sharing and downloading. Once all the peers are connected to the database, one of the peer is chosen for interaction. Trustworthiness of a peer is calculated based on service, recommendation and reputation metrics. After every interaction the acquaintance list is updated. The service trust metric is calculated based on bandwidth and transaction time. Also the trust value of each peer is calculated by fading effect, competency and integrity belief. With these calculated trust values, the reputation metric and recommendation

metrics are evaluated by file importance, recentness and satisfaction parameters. All peers are assumed to be strangers at the start. Peers must contribute others in order to build trust relationships. A trusted peer cannot observe all interactions in a P2P system and might be a source of misleading information. A peer becomes an acquaintance of another peer after providing a service to it. Using a service from a peer is called a service interaction. A recommendation represents an acquaintance‟s trust data about a stranger. A peer requests recommendations only from its acquaintances. There are no trusted peers to manage trust relationships. Some peers behave malignant but some might behave trusted. Peers periodically leave and join the network.

### 3.2 Interaction Process

The interaction process takes place by connecting all the peers that wish to upload and download the files in which peers are denoted by p, for example $i_{th}$ peer can be represented as $p_i$. The Interaction process consists of two phases.

a) Upload process

b) Download process

When $p_i$ uses a service of $p_j$ , a service interaction for $p_i$ occurs. Unidirectional of interaction occurs. $p_j$ is stranger to $p_i$, if $p_i$ has no service interaction with $p_j$ . $p_i$' „s set of acquaintances is denoted by $A_i$ .Each peer stores a transaction history of service interactions for each acquaintance. $p_i$'s service history with $p_j$ is denoted as $SH_{ij}$.. $SH_{ij}$ is a time ordered list, since new interactions are appended to the history. After finishing a service interaction, $p_i$ evaluates quality of the service. $0 \leq e_{kij} \leq 1$ denotes $pi$‟s satisfaction about $k_{th}$ service interaction with $p_j$. If the interaction is cancelled, $e_{kij}$ gets 0 value. $k$ is the sequence number of the interaction in $SH_{ij}$ . A service interaction is associated with a weight to quantify importance of the interaction. $0 \leq w_{kij} \leq 1$ denotes the weight of $k_{th}$ service interaction of $p_i$ with $p_j$.

In upload process, all the peers can upload their files to share with other peers, and it is designed by peer‟s origin and terminal. The file is shared by allocating it to other concerned peer. Once the file is shared, acquaintance list is updated in order to know its neighborhood process that has interacted. In upload process, the quality of service is calculated. The quality of service is calculated based on bandwidth, transaction time. In download process, the recommendation and reputation of peers are evaluated.

### 3.3 Service Trust metric (stij)

A peer becomes an acquaintance of another peer after providing a service. Using a service from a peer is called a service interaction. Trustworthiness of a service provider is based on the trustworthiness of its services and rates of its properties. In addition to providers‟ properties, a provider can provide important clues for requestors to assess its trustworthiness. The importance of an interaction fades as new interactions happen. $0 \leq f_{kij} \leq 1$ denotes the fading effect of $k_{th}$ service interaction of $p_i$ with $p_j$. It is calculated as follows: $f_{ijk}=\mathrm{k}sh;\ 1 \leq k \leq sh_{ij}$

A peer first calculates competence and integrity belief values using the information about service interactions. Competence belief is based on how well an acquaintance satisfies the needs of interactions. $cb_{ij}$ denotes the competence belief of $p_i$ about $p_j$ in the service context. Competence belief is measured based on average behavior in the past interactions. The $cb_{ij}$ is calculated as follows:

$cb_{ij}= 1\beta cb\ (s_{ijkshijk=1}..f_{ijk})$

$\beta cb= w_{ij.k}\, f_{ijk\ shijk=1}$ is the normalization coefficient.

The confidence level about the prediction of future interactions is called integrity belief. $ib_{ij}$ denotes the integrity belief of $p_i$ about $p_j$ in the service context. The measure of integrity belief is the deviation from the average behavior. Therefore, $ib_{ij}$ is calculated as:

$ib_{ij}= 1sh_{ij}\, s_{ijk}.w_{ij\mu}.f_{ij\mu} - cb_{ij\ 2\ shijk=1}$

If $pi$ sets $st_{ij} = cb_{ij}$ , half of the future interactions will likely to have a satisfaction value less than $cb_{ij}$ . Thus, $st_{ij} = cb_{ij}$ is an over-estimate for $p_j$‟s trustworthiness. A lower estimate makes $pi$ more confident about future decisions with $p_j$ . $p_i$ may calculate $st_{ij}$ as follows:

$st_{ij} = cb_{ij} - ib_{ij} / 2$

**Table I Notation of trust metrics**

| Notation | Description |
|---|---|
| $p_i$ | a peer with identifier $i$ |
| $f^k_{ij}$ | fading effect of $pi$'s $kth$ interaction with $pj$ |
| $e^k_{ij}$ | satisfaction of $pi$'s $kth$ interaction with $pj$ |
| $w^k_{ij}$ | weight of $pi$'s $kth$ interaction with $pj$ |
| $cb_{ij}$ | $p_i$ 's competence belief about $pj$ |
| $ib_{ij}$ | $p_i$'s integrity belief about $pj$ |
| $st_{ij}$ | $p_i$ s service trust value about $pj$ |
| $sh_{ij}$ | size of $p_i$ s service history with $pj$ |

### 3.4 Reputation Trust Metric (r ij)

Reputation metric is a trusted agent who keeps track of the behavior of other agents. Assume that $pj$ is an intruder to $pi$ ; if $pi$ needs a service from $pj$ ,it sends a recommendation request to nearby peer $pk$ . $pi$ selects trustworthy acquaintances and a threshold is set. After collecting all recommendations, $pi$ calculates $erij$, an estimation for the reputation of $pj$ , by aggregating $rkj$ values in the recommendations. $rkj$ should be considered with respect to $\eta kj$.

$er_{ij}= 1\beta er\, rt_{i.}\eta_{kj}\, .r_{kj\ pk \in Ti}$

Then, $p_i$ calculates estimations for the competence and integrity beliefs about $p_j$ which are denoted by $ecb_{ij}$ and $eib_{ij}$ respectively. These values are calculated by aggregating $cb_{kj}$ and $ib_{kj}$ values in the recommendations. $cb_{kj}$ and $ib_{kj}$ should be evaluated based on $sh_{kj}$ .

$r_{ij}=\lfloor \mu_{sh} \rfloor sh_{max}\, ecb_{ij} - eib_{ij} / 2 + 1 - \lfloor \mu_{sh} \rfloor sh_{max}\, er_{ij}$

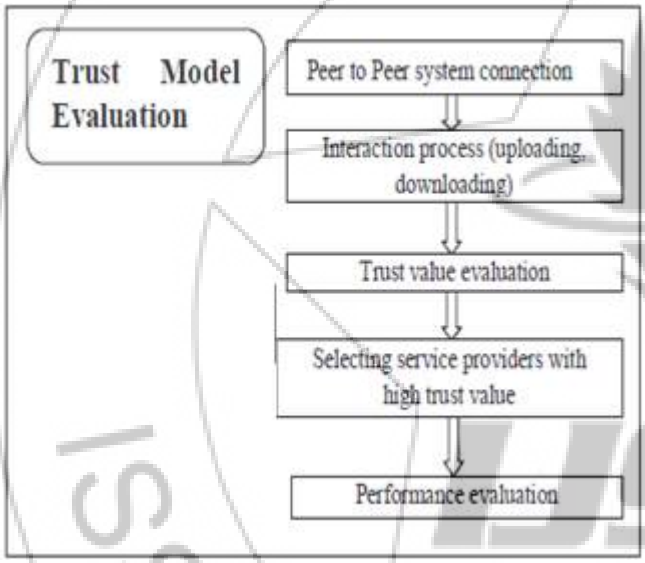
### 3.5 Recommendation Trust Metric (rtik)

The trust-based recommendation approach, which provides recommendations to a requester in a trust network, is built on a vertex similarity measurement between graphs. After calculating $r_{ij}$ value, $p_i$ updates recommendation trust values of recommenders also $p_i$ updates $rt_{ik}$, according to peer recommendation. $p_i$ compares competency , integrity, reputation values of $p_i$ and $p_j$ with $p_k$ and $p_j$ . If these values are close, then $p_k$"s recommendation is good and a high trust value is assigned.

$$rt_{ik}=rh_{ik}rh(rcb_{ik}-rib_{ik}/2)+rh_{max}-rh_{ik}rh_{max}\,r_{ik}$$

### 3.6 Trust value evaluation

The trust evaluation is done based on the three metrics that measures quality of service, opinion values and suggestions. The trust value of all the peers are evaluated and validated. Thus the graph is plotted based on trust values of the three peers and the peer with highest trust value is displayed and chosen as the best service provider.




## 4. Results

### 4.1 Implementation Details

In the design phase, three peers are connected to the database for interaction process. From the fig 2; one of the peer is chosen for file sharing with origin and its terminal and the file is chosen and allocation is done. Once the file is shared, acquaintance list is updated. On the terminal side, the file is received and the performance is evaluated based on bandwidth and transaction time. By this the service trust metric is calculated for all the three peers. The process is done for file uploading process.

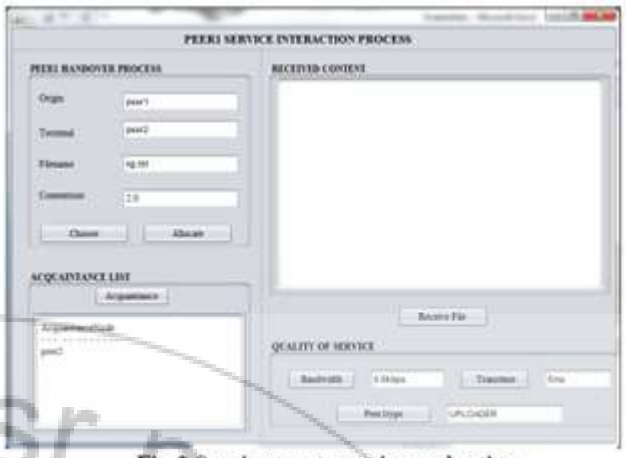



Fig 2 Service trust metrics evaluation

From the fig 3; during file downloading process, service provider is selected from its nearby acquaintance list. If a peer is already interacted during uploading process then the transaction history is displayed with its origin, terminal, filename, and content size. Thus the peer is chosen for selecting a file and the request has been sent to the service provider. Incase if a peer had no interaction during uploading process then a recommendation request is sent for trustworthiness.

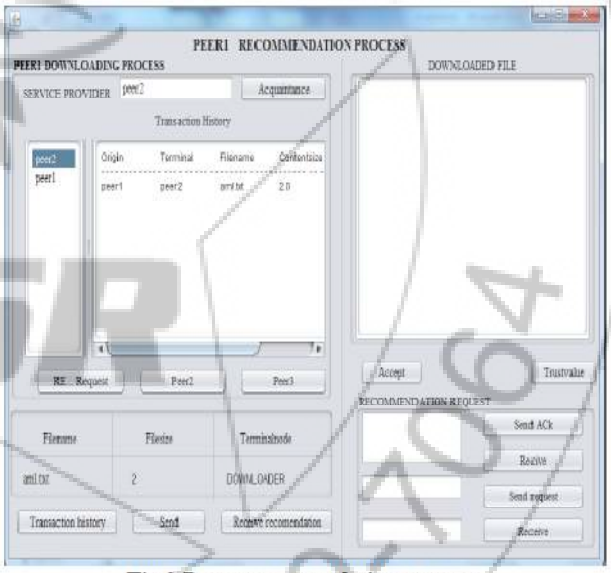



Fig 3 Peer recommendation process

If no interaction is done with its service provider a recommendation request is sent to its acquaintance. This acquaintance peer checks for its transaction history. If an interaction is done then it "**sends ack**" to the requested peer. If not it displays as "**No Interaction**". ***4.2 Graph Analysis*** A file sharing program is implemented in java using Net Beans to observe results of using novel trust in a P2Penvironment.

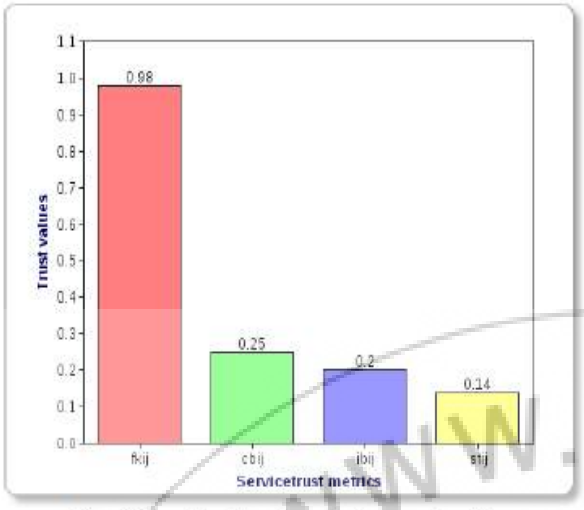



Fig 4 Service trust metrics evaluation

Based on service trust metric, reputation metric and recommendation metric calculation and graph is plotted by which a peer‟s trust value is evaluated and the one with highest service trust peer is chosen as the service provider. X-axis represents the number of peers and Y-axis represents trust value for each peer. From the fig 4 it is known that, service trust metric is evaluated based on fading effect (0.98), competency belief (0.25) and integrity belief (0.20). These trust values are evaluated and stored for computing the trust value. Bandwidth and transaction time are taken for this analysis with uploading concept.

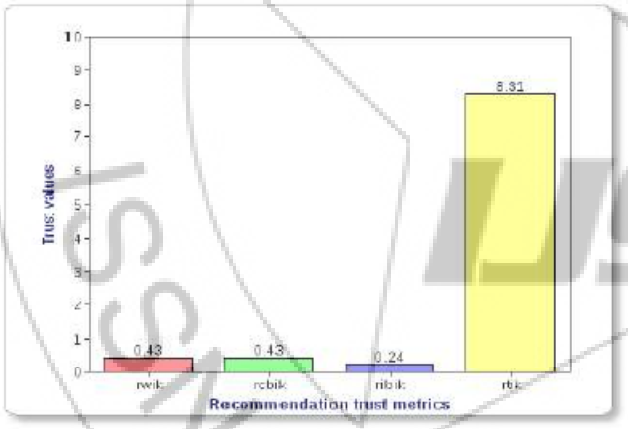



Fig 5 Recommendation trust metrics evaluation

From the fig 5 it is observed that recommendation trust metric is evaluated on the basis of recommendation: weight (0.43), competency belief (0.43), integrity belief (0.24) and recommendation trust value (8.31). These values represent trusted peer recommendation.

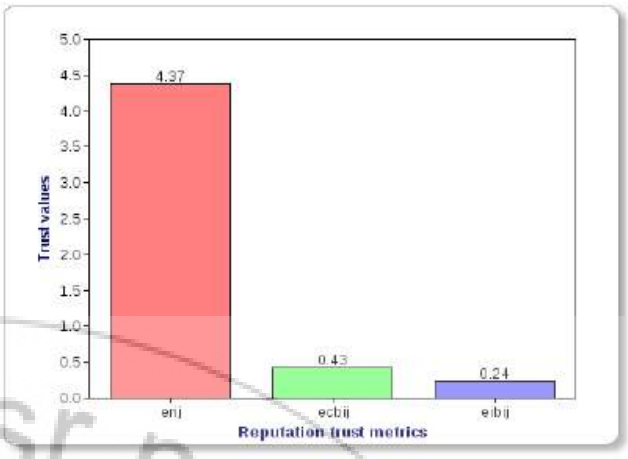



Fig 6 Reputation trust metrics evaluation

From the fig 6 it is known that, reputation metric that measures intruders and is evaluated based on interaction history with a peer, number of acquaintances and peer estimation about reputation of other peer.

## 5. Conclusion

A novel trust model is designed and observed data of all the peers are available directly for evaluating the trustworthiness and also each peer can provide referrals to other peers, thereby makes the trust level computation easier. Each peer can make assessment of other peer based on trust value on the basis of service, recommendation and reputation metric. Thus each peer‟s resources and contents can be shared by all other peers and these metrics evaluation measure trust level and select best peer trust provider. By this, a trusted peer environment is developed and more interactions are done to enhance trustworthiness.

## References

[1] Ahmet Burak Can, “SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems”- Ieee transactions on dependable and secure computing, vol. 10, no. 1, january/february 2013.
[2] A. Abdul-Rahman and S. Hailes, “Supporting Trust in Virtual Communities,” Proc. 33rd Hawaii Int‟l Conf. System Sciences (HICSS), 2000.
[3] A.A. Selcuk, E. Uzun, and M.R. Pariente, “A Reputation-Based Trust Management System for P2P Networks,” Proc. IEEE/ACM Fourth Int‟l Symp. Cluster Computing and the Grid (CCGRID), 2004.
[4] G. Caronni and M. Waldvogel, “Establishing Trust in Distributed Storage Providers,” Proc. IEEE Third Conf. Peer-to-Peer Computing (P2P), 2003.
[5] G.Swamynathan, B.Y. Zhao, and K.C. Almeroth, “Decoupling Service and Feedback Trust in a Peer-to-Peer Reputation System,” Proc. Int‟l Conf. Parallel and Distributed Processing and Applications (ISPA), 2005.
[6] S. Saroiu, P. Gummadi, and S. Gribble, “A Measurement Study of Peer-to-Peer File Sharing Systems,” Proc. Multimedia Computing and Networking, 2002.
[7] F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, “Choosing Reputable

Servents in a P2P Network," Proc. 11th World Wide Web Conf. (WWW), 2002.
[8] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int"l Conf. Information and Knowledge Management (CIKM), 2001.
[9] S. Marsh, Formalising Trust as a Computational Concept. PhD thesis, Department of Mathematics and Computer Science,University of Stirling, 1994.
[10] B. Ooi, C. Liau, and K. Tan, "Managing trust in peer-to-peer systems using reputation-based techniques," in Proceedings of the 4th International Conference on Web Age Information Management, 2003.
[11] E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, "An Algorithm for Building User-Role Profiles in a Trust Environment," Proc. Fourth Int"l Conf. Data Warehousing and Knowledge Discovery (DaWaK), vol. 2454, 2002.
[12] A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.
[13] P. Victor, C. Cornelis, M. De Cock, and P. Pinheiro da Silva, "Gradual Trust and Distrust in Recommender Systems," Fuzzy Sets Systems, vol. 160, no. 10, pp. 1367-1382, 2009.
[14] M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Peer-to-Peer Networks," Proc. 13th Int"l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2003.
[15] B. Yu, M.P. Singh, and K. Sycara, "Developing Trust in Large- Scale Peer-to-Peer Systems," Proc. IEEE First Symp. Multi-Agent Security and Survivability, 2004.

## Author Profile

**Uppula Nagaiah** received the B. Tech degree in Information Technology from JNTU Hyderabad in 2012 and pursuing M.Tech degree in Computer science and Engineering from Anurag Group of Institutions (Formerly CVSR College of Engineering) JNTU Hyderabad.

**G. Kiran Kumar** working as Assistant Professor in Computer Science Engineering from Anurag Group of Institutions (Formerly CVSR College of Engineering) JNTU Hyderabad.