ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Trust Model Based on Hybrid System for Peer-to-Peer Networks

Pradnya Bhirud, Prof. Avinash Shrivas

ME Student, Dept. of Computer, Vidyalankar Institute of Technology, Mumbai University, Maharashtra, India

Assistant Professor, Dept. of Computer, Vidyalankar Institute of Technology, Mumbai University, Maharashtra, India

ABSTRACT: Security is one of the most critical constraints for the expansion of peer-to-peer networks. In a peer-to-peer (P2P) network, every machine plays the role of client and server at the same time. In peer-to-peer networks, one of the most important issues is trust management. In peer to peer network, P2P users unfamiliar with each other. A feasible solution is to set up a Service trust metric, Reputation-based trust metric, and Recommendation trust metric. Our trust model based on the hybrid system can create trust relationship among peers. In service Trust Metric, measure how the service is given by service provider. The model utilizes fuzzy logic to integrate trust factors into the reputation evaluation process for improving the efficiency and security of peer to peer system. The reputation and recommendation trust metric is combined for computing a global trust metric which helps in selecting the best service provider. Add one more module like user feedback. User feedback is used to calculate satisfaction of peers regarding specific services. So, this paper focuses on developing trust model based on the hybrid system for peer to peer networks.

KEYWORDS: Peer-to-peer networks; trust; reputation; security; recommendation; hybrid system.

I. INTRODUCTION

With the increasing availability of high bandwidth Internet connections and low price of computers, peer-to-peer (P2P) networks have become very popular in resource sharing and exchange. There are no fixed clients and servers. Any node could be a client or a server.

A peer-to-peer network is a type of decentralized and distributed network architecture in which individual nodes in the network act as both suppliers and consumers of resources, in contrast to the centralized client–server model where client nodes request access to resources provided by central servers. In this network, tasks are shared amongst multiple interconnected peers who make a portion of their resources directly available to other network participants, without the need for centralized coordination by servers. Below figure provides a conceptual representation of the P2P overlay topology. In this, every machine plays the role of client and server at the same time. Although a P2P network has a number of advantages over the traditional client-server model in terms of efficiency and fault-tolerance, additional security threats can be introduced. Users and IT administrators need to be aware of the risks from propagation of malicious code, the legality of downloaded content, and vulnerabilities within peer-to-peer software [1].

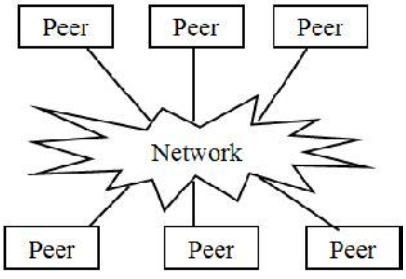

Fig. 1 P2P overlay topology

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Peer-to-Peer file sharing systems provide a large collection of files available for download. In traditional systems, little information is given to the user to help in the peer-selection and file-selection processes. For example, if a user wants to download a file, the user is given a list of peers that have the requested file. The process of selecting the right peer with no a priori information is frustrating and risky. To positive interactions and reduce the risk involved in P2P file sharing systems, peers need to reason about trust and reputation systems are used to this end. Reputation systems are based on collecting information about peers past transactions and computing a reputation value for these peers. The reputation values will be the basis for identifying trustworthy peers. In a P2P system, peers communicate directly with each other to exchange information and share files.

II. LITERATURE SURVEY

Many types of research have been done to establish the trust model. Marsh [9] defines a formal trust model based on sociological foundations. An agent uses own experiences to build trust relations and does not consider information of other agents.

EigenTrust [10] gives a method to aggregate global trust value. The work in [5] improves EigenTrust [10] by eliminating the pre-trusted entities and introduces the recommendation trust mechanism. PeerTrust [5] indicates that the super-node can be selected as a recommended trust node for community-based P2P architecture. By taking the advantage of simulation the way of human thinking, fuzzy logic inference rules are introduced in Fuzzy Trust [6] to calculate local trust scores and aggregate global reputation. Based on [6], Fuzzy Comprehensive Evaluation [7] puts forward evaluation factor sets (such as reliability of recommendatory as well as QoS and capability of peers) for fuzzy trust decision-making. Due to its good performance on handling uncertainty and imprecision, MHFTrust [8] further designs the capability factors of trust evaluation with hierarchical fuzzy systems.

According to Bharat Bhargava and Ahmet Burak Can [2] 'SORT' for peer to peer systems can decrease malicious activity by creating trust relations among peers in their closeness. Qiyi Han, Hong Wen, Ting Ma and Bin Wu [3] proposed a Self-Nominating Trust Model Based on Hierarchical Fuzzy Systems for Peer-to-Peer Networks. The hierarchical fuzzy system integrates 8 factors into the reputation evaluation process.

The work in [4], studied trust models based on various approaches like reputation, service, and recommendation out of which SORT model[2] is quite better as compared to other models with respect to performance and accuracy but only one drawback is that Using trust information does not solve all security problems. In Self-nominating trust model[3] based on Hierarchical Fuzzy Systems to improve the security of P2P systems but in this trust model consider the only reputation and recommendation module and not focused on the service module. So, in proposed system combine these two trust model [2], [3] and Add one more module like user feedback. User feedback is used to calculate satisfaction of peers regarding specific services for better Performance.

III. PROPOSED METHODOLOGY

The proposed system has been partitioned into following modules: Interaction process (promise model), Feedback module, Service Trust Metric, Reputation trust metric, Recommendation Trust Metric and Global Trust Metric.

In our proposed system, some assumptions are taken to make the system,

- Peers are given with equal privileges.
- Peers can leave and join the network anytime.
- Each peer can provide services and uses services of others.
- Peers are free to give feedback to the other peers from which service is to be taken.
- Peers are strangers to each other at the starting of process because of no interaction takes place.
- A peer becomes an acquaintance of another peer after providing a proper service like uploading, downloading a file as we taken in our current system.
- There are no privileged, centralized, or trusted peers to manage trust relationships but for remove bandwidth allocation problem we make a peer manager who keeps the record of all peer like how much data is being utilized by the peers.
- If a peer has no acquaintance, assume that it has to choose a trust strangers.
- Again an acquaintance is to be chosen over a stranger if they have same trust values.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Figure 2 depicts the Architecture of trust model based on hybrid system. Once the peer logs in, it can interact with otherpeers via upload and download process. After interaction, trust metrics are calculated so upload and download file on the basis of trust metrics.

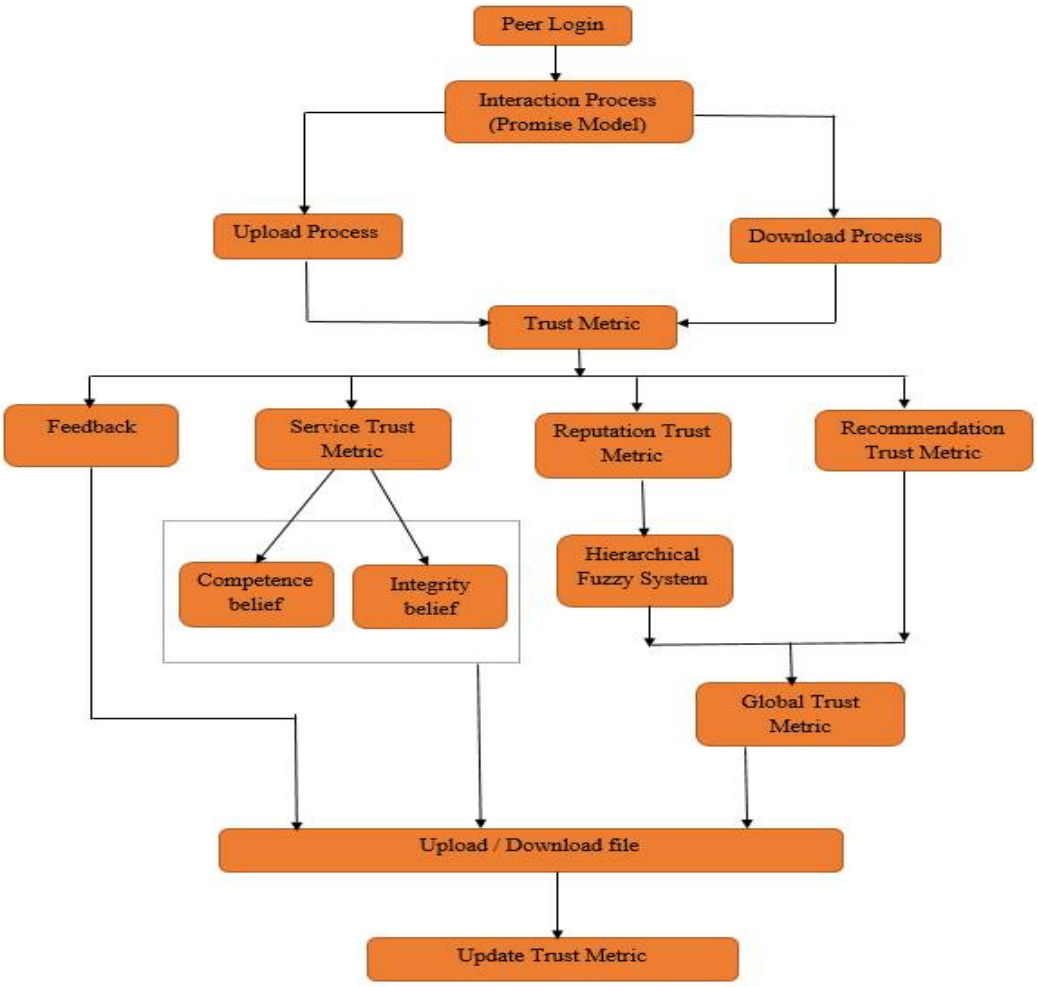

Fig. 2 Architecture of trust model based on hybrid system

2.1 Modules in Proposed System

A. **Interaction Process (Promise model):**

The interaction process takes place by connecting all the peers that wish to upload and download the files. The interaction process consists of two phases: Upload process and Download process.

In upload process, a peer shares resources with different peers. When the file is shared, acquaintance list is reorganized in order to know its neighbourhood process that has interacted. In download process, peer request other peers to download the resources. After the interaction process, trust values are evaluated.

B. **Feedback Module:**

In this calculate user satisfaction regarding to specific services. Extract the emotions of peers who got services using polarity measurement to evaluate the feedback is positive or not. For giving feedback to particular service provider, the NLP (Natural Language Processing) concepts used like feature extraction by finding polarity of the opinion given by the user for particular service.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

C. **Service Trust Metric Module**

A peer first calculates competence and integrity belief values for evaluating service provider's trustworthiness in the service context, using the information in its service history. How well an acquaintance satisfied the needs of past interactions represented by Competence belief. The overall behavior in the past is a measure of the competence belief while interacting with others.

As cb_{ij} is a $peer_i$'s competence belief about $peer_j$, $Peer_i$ calculates cb_{ij} as follows: Competence belief,

$$cb_{ij}=\frac{1}{\beta_{cb}}\sum_{k=1}^{s^{h_{ij}}}\left(s^{k_{ij}}.w^{k_{ij}}.f^{k_{ij}}\right) \quad \ldots\ldots\ldots \quad (1)$$

$$\beta_{cb}=\sum_{k=1}^{s^{h_{ij}}}\left(w^{k_{ij}}.f^{k_{ij}}\right)$$

Where β_{cb} (normalizing coefficient) ensures that the value of cb_{ij} will remains between 0 to 1 as the value of$s^{k_{ij}}$= 1 for perfect interaction. Importance of competence is as equal as the consistency of interactions between peers. To make sure this, we implement one more belief factor i.e. integrity belief. As ib_{ij} is a $peer_i$'s integrity belief about $peer_j$, which shows confidence regarding future interactions. ib_{ij} is derived from overall average behavior so that we have to calculate approximation to the standarddeviation of interaction parameters.

$$ib_{ij}=\sqrt{\frac{1}{sh_{ij}}\sum_{k=1}^{s^{h_{ij}}}\left(s^{k_{ij}}.w^{\mu_{ij}}.f^{\mu_{ij}}-cb_{ij}\right)^2} \quad \ldots\ldots\ldots \quad (2)$$

The weight of an interaction is calculated based on two variables: File size and Popularity.Smaller the value of integrity belief gives assurance to the predictable behavior of $Peer_j$ in future.

Therefore, $Peer_i$ calculates stij (service trust)as follows:

$$st_{ij}=\frac{sh_{ij}}{sh_{max}}\left(\frac{cb_{ij}-ib_{ij}}{2}\right)+\left(1-\frac{sh_{ij}}{sh_{max}}\right)r_{ij} \quad \ldots\ldots\ldots \quad (3)$$

D. **Reputation Trust Metric:**

Reputation is a peers belief in another peers capabilities, honesty and reliability. In this fuzzy based trust model eight factors are integrated into the reputation evaluation process. At the beginning phases of an interaction, it is hard to build the reputation because, it is dangerous to contact another peer and download its resources. These trust factors permit a peer to recommend themselves whenever and accordingly advance their resources.

The trust factors are defined as follows:

1) **Malicious behavior (MB)** In peer to peer environment, malicious behavior is a vital security factor. One way of preventing malicious peers is to decline their reputation level in the event that they are undesirably elected as service providers. In the mean time, malicious peers ought to be recognized and stamped too.

2) Bandwidth (BW) Bandwidth decides a peers capacity for giving data transactions. A bigger bandwidth gives more data transactions.

3) Online time rate (OR) Due to the dynamic and self-governing nature of peer to peer networks, a peer can join and leave the system whenever. Online time rate is recorded to demonstrate the rate of peer's login time.

4) Download success rate (DR) Only successful downloads are the precondition for sharing. Peer can record the quantity of success download and the quantity of failed download to get the download success rate.

5) File Size (FS) It shows the size of the requested resource and the quantity of files included in the resource.

6) Time to live (TL) This component demonstrates the remaining (online) time before a peer clears out. The requester can estimate the task progress in light of this component.

7) Upload Speed (US) Similar to the bandwidth, upload speed decides the capacity of sending information.

8) Content relevance (CR) Spam and irrelevant files are not common. Indeed a true and accessible file can be appended with irritating data for example unfamiliar popup link or spam advertisement.

The above trust factors are integrated by a Hierarchical fuzzy trust system to compute the reputation value of peers. The outline of Hierarchical Fuzzy System is given underneath.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

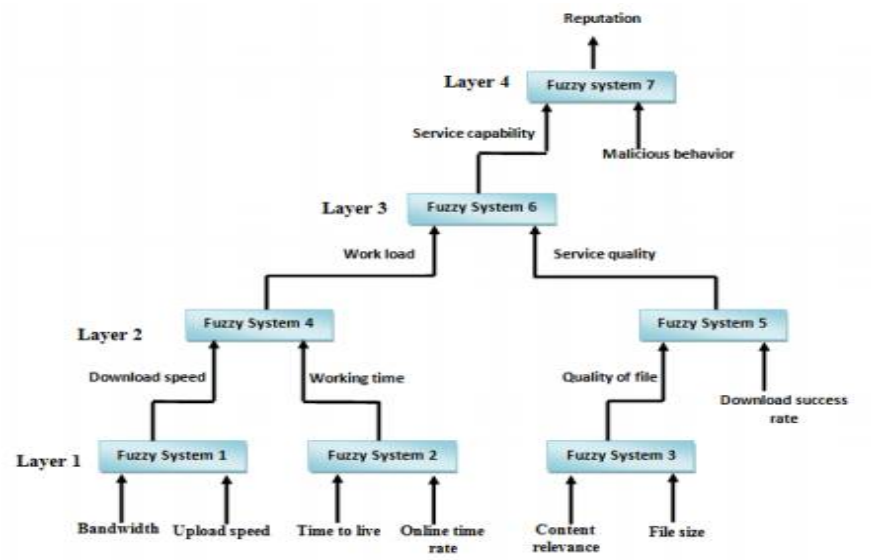

Fig 3 Hierarchical Fuzzy Trust System

There are six intermediate variables in the system. Bandwidth and upload speed is utilized to infer the download speed. Time to live and online time rate is utilized to infer the working time of the peer. Content relevance and file size contributes the quality of file. Download speed, working time, quality of file and download success rate will be fed as inputs to the 2nd layer fuzzy system. Thus the outcome of 2nd layer fuzzy system that is work load and service quality is utilized by 3rd layer fuzzy system to infer service capability. Fuzzy logic utilizes the service capability and malicious behavior to infer the reputation value of the peer.

E. **Recommendation Trust Metric:**

- Use promise model, when peer pi collects the recommendation trust information of peer pj.
- Peers who have the direct interaction experiences with peer pj will send a feedback to peer pi.
- Peer pi aggregates these feedbacks to compute a recommendation trust metric of peer pj.
- $$R(A,B) = \sum_{i=1}^{N} sim(A,i) \cdot LT(i,B) \Big/ sim(A,i)$$
  - where N is the number of peers who send the feedbacks.
  - $LT(i,B)$ is the feedback of local trust metric of peer B.
  - $sim(A, i)$ is the similarity measure between Peer A and Peer i.
- Let R(A,B) as rtij For further calculation.

F. **Global TrustMetric:**

The global trust metric is integrated as the weighted sum of the local and the recommendation trust metrics, as formulated in

Global Trust = (α * LT) + ((1-α)R [32]

where the weighting factor α is a value between 0 and 1, denoting the proportion between local trust metric and recommendation trust metric. **α** can be different due to personal preference of peers. A headstrong peer assigns **α** large value, because it would rather believe its own experience. In contrast, a softhead peer assigns a small value to α. α can also be automatically assigned as,

$\alpha = m / (n + m)$

where m is the number of reputation feedbacks, and n is the number of recommendation feedbacks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

IV. EXPERIMENTAL RESULTS

By looking at the results provided by proposed algorithm and the results obtained by study different Trust-based system compared against various factors and following points are worth noted.

Table 1 shows the Comparison between proposed Trust Model, SORT and Self Nominating Trust Model using trust factors. A number of factors increase the accuracy of the system. Multiple factors in the trust evaluation process, where the requester has been provided requested resource by resource provider on the basis of trust factors. For this, here we introduce some trust factors like Bandwidth, Average Download Speed, Average Upload Speed, Online/Offline period, File Size, download Success Rate and Popularity of File. These factors are provided by resource holder to demonstrate their desires. Where the other models hardly include all these factors which will lead to reduced accuracy.

Figure 4 shows the same comparison in the graphical format to show this difference clearly between the different trust system and our proposed system.

Trust Factors	Proposed trust based System	SORT	Self-Nominating Trust model
Authenticity of file	YES	YES	YES
Bandwidth	YES	YES	YES
Average Download Speed	YES	NO	NO
Average Upload Speed	YES	NO	YES
Online Time Rate	YES	YES	YES
Time To Live	YES	NO	YES
File Size	YES	YES	YES
Download Success Rate	YES	NO	YES
Content relevance	YES	NO	YES
Popularity of File	YES	YES	NO

Table 1 Comparison between Proposed Trust Model, SORT and Self Nominating Trust Model using trust factors

Fig 4 Comparison between Proposed Trust Model, SORT and Self Nominating Trust Model using trust factors

Attacks	Proposed trust based System	SORT	Self-Nominating Trust model
Covers Service Based attacks	YES	YES	NO
Covers Recommendation Based attacks	YES	YES	NO

Table 2 Comparison between Proposed Trust Model, SORT, Self-Nominating Trust Model based on attacks covers

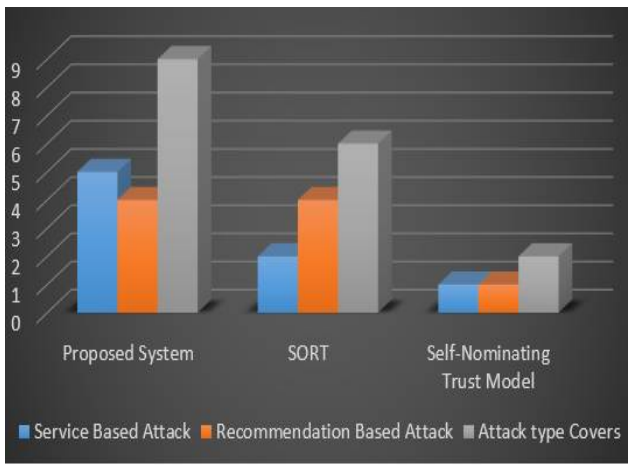

Fig 5 Proposed Trust model vs. other Trust Models

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Trust based systems are faces two different kinds of attacks like service based attacks and recommendation based attacks. Talking about service based attacks, attackers are becoming more isolated from good peers. They lose their ability to attract good peers with time, which decreases attacks. This is done by our system to minimize service based attacks over different trust based systems. In the case of recommendation based attacks, Attackers become more isolated from good peers and get fewer recommendation requests which result in less number of recommendation based attacks.

Table 2 shows the comparison between Proposed Trust Model, SORT, Self-Nominating Trust Model based on attacks covers by them. Figure 5 shows the difference between Proposed Trust Model and Other Trust Models with respect to service based attacks and recommendation based attacks.

V. CONCLUSION

The proposed system overcomes the drawbacks of the existing systems. In trust model based on the hybrid system, a peer can develop a trust network in its proximity. A peer can isolate malicious peers around itself as it develops trust relationships with good peers. Service, Reputation, and recommendation trust metrics are defined to measure capabilities of peers in providing services and giving recommendations.

Trust model will not only resolve the security issues in peer to peer systems but can improve security and the efficiency of systems. Our model can evaluate the trust in a comprehensive manner, where peers are promoted to share by identifying their sharing desires and transmission capabilities. The trust model can speed up reputation accumulation process to promote peer activities while balancing the workload in the network.

REFERENCES

1. Santosh Suresh Padwal, G.P. Bhole, “Study of Trust Management Approaches in Peer to Peer System”, International Journal of Current Engineering and Technology, Vol.4, Issue 4, pp.2439-2443, 2014.
2. Ahmet Burak Can, and Bharat Bhargava, ”SORT: A SelfORganizing Trust Model for Peer-to-Peer Systems”,IEEE Transactions On Dependable And Secure Computing, Vol.10, Issue 1, pp.14-27, 2013.
3. Qiyi Han, Hong Wen, Ting Ma and Bin Wu, ”Self-Nominating Trust Model Based on Hierarchical Fuzzy Systems for Peer-to-Peer Networks”, IEEE/CIC ICCC 2014 Symposium on Privacy and Security in Commutations, pp. 199-203, 2014.
4. Pradnya Bhirud, Prof. Avinash Shrivas, “A Survey on Trust Model in Peer-to-Peer Networks”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 6, June 2016.
5. W. Dou, H. Wan, J. Yan, and Z. Peng, “A Recommendation-based Peer- to-Peer Trust Model,” Journal of software, vol. 15, pp. 571-583, 2004.
6. L. Xiong, and L. Liu, “PeerTrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities,” IEEE Trans Knowl and Data Eng, vol. 16, pp. 843-857, 2004.
7. S. Song, K. Hwang, R. Zhou, and Y. Kwok, “Trusted P2P Transactions with Fuzzy Reputation Aggregation,” IEEE Internet Comput, vol. 9, pp. 24-34, 2005.
8. H. Chen, and Z. Ye, “Research of P2P Trust based on Fuzzy Decision- making,” 12th International Conference on Computer Supported Cooperative Work in Design, Xi'an, pp 793-796, 2008.
9. S. Marsh, “Formalising Trust as a Computational Concept,” PhD thesis, Dept. of Math. and Computer Science, Univ. of Stirling, 1994.
10. S.D. Kamvar, M.T. Schlosser, and Hector Garcia-Molina, “Eigenrep: Reputation management in P2P networks,” In: Proceedings of Twelvth International World Wide Web Conference, vol. 1, pp 123-134, 2003.

BIOGRAPHY

Pradnya Bhirud is pursuing M.E (Comp Engg.) from Vidyalankar Institute of Technology, Mumbai University. She did her graduation B.E (Comp Engg.) from Mumbai University, Maharashtra.