A Self-Organizing Trust Model for Peer-to-Peer Systems

M Mounika[1], S Ramesh[2]
[1] *Student, Dept. of MCA,EAIMS*
[2] *Professor, Dept. of MCA,EAIMS, Tirupati,A.P.*

***Abstract*- Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. This paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust, service, and recommendation contexts are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations.**

***Index Terms*- purpose of the system, existing system, proposed system, architecture, modules.**

I. INTRODUCTION

PEER-TO-PEER (P2P) systems rely on collaboration of peers to accomplish tasks. Ease of performing malicious activity is a threat for security of P2P systems. Creating long-term trust relationships among peers can provide a more secure environment by reducing risk and uncertainty in future P2P interactions. However, establishing trust in an unknown entity is difficult in such a malicious environment. Furthermore, trust is a social concept and hard to measure with numerical values. Metrics are needed to represent trust in computational models. Classifying peers as either trustworthy or untrustworthy is not sufficient in most cases. Metrics should have precision so peers can be ranked according to trustworthiness.

1.1 Purpose of the system

This thesis propose a Self-ORganizing Trust model (SORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. In SORT, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers.

1.2 Existing System

Abdul-rahman and Hailes evaluate trust in a discrete domain as an aggregation of direct experience and recommendations of other parties. They define a semantic distance measure to test accuracy of recommendations. Yu and Singh's model propagates trust information through referral chains. Referrals are primary method of developing trust in others.

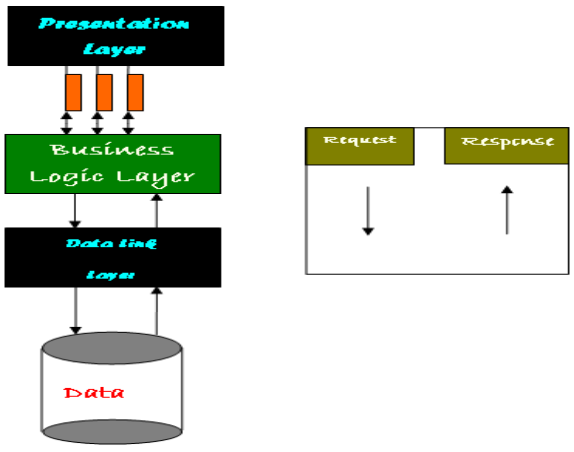
1.3 Proposed System

This thesis propose a Self-ORganizing Trust model (SORT) that aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. In SORT, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers.

Advantages:

1. It efficiently finds the malicious node.
2. It can be adapted various application like, CPU sharing, storage networks, and P2P gaming Easy to manage historical data in a secure manner

II.ARCHITECTURE DIAGRAM



III.MODULES

The project has been divided into 4 different modules:

1. Network formation module
2. Service Metric module
3. Reputation Metric module
4. Recommendation module
5.Select Service Providers

3.1 Network Formation

In this module the peer to peer network is formed for communication and file sharing. Each peer have unique id. Each peer in the network will give the own details such as Peer ID and IP address, through which the transmission is done and similarly give the known peers details ie., neighbor peer information such as Peer ID, IP address and port number which are neighbors to given node.

3.2 Service Metric

In this module a peer can compute the service metric. For evaluating an acquaintance's trustworthiness in the service context, a peer first calculates competence and integrity belief values using the information in its service history.

3.3 Reputation Metric

In this module the peer find the reputation metric. It measures a stranger's trustworthiness based on recommendations. Assume that p_j is a stranger to p_i and p_k is an acquaintance of p_i. If pi wants to calculate r_{ij} value, it starts a reputation query to collect recommendations from its acquaintances.

3.4 Recommendation Metric

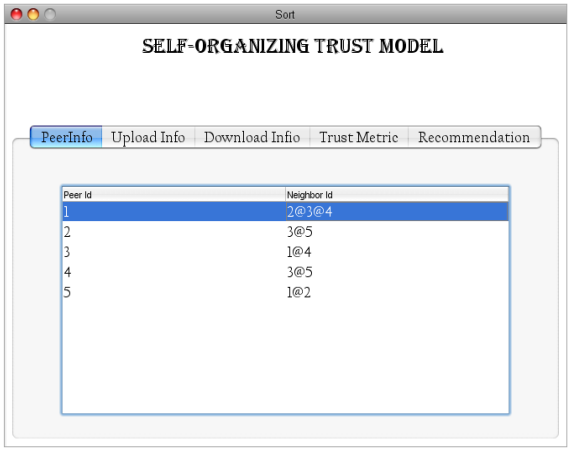
A recommendation is evaluated according to recommendation trust value of the recommender. In particular, pi evaluates pk's recommendation based on rtik value. After calculating rij value, pi updates recommendation trust values of recommenders based on accuracy of their recommendations.

3.4 Select Service Providers

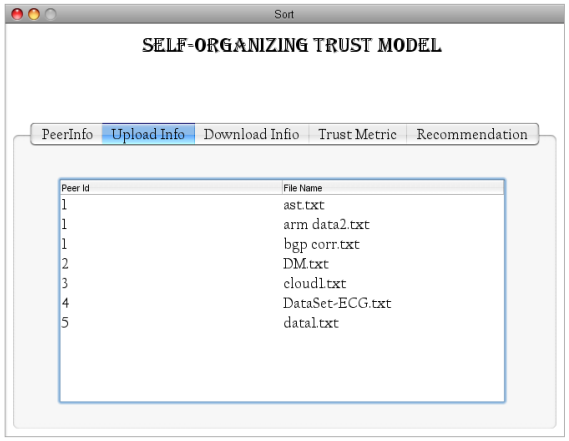
Service provider selection is done based on service trust metric, service history size, competence belief, and integrity belief values. When pi wants to download a file, it selects an uploader with the highest service trust value. If service trust values are equal, the peer with a larger service history size (sh) is selected to prioritize the one with more direct experience. If these values are equal, the one with a larger cb – ib/2 value is chosen. If cb – ib/2 values are equal, the one with larger competence belief value is selected.

IV.SCREENSHOTS

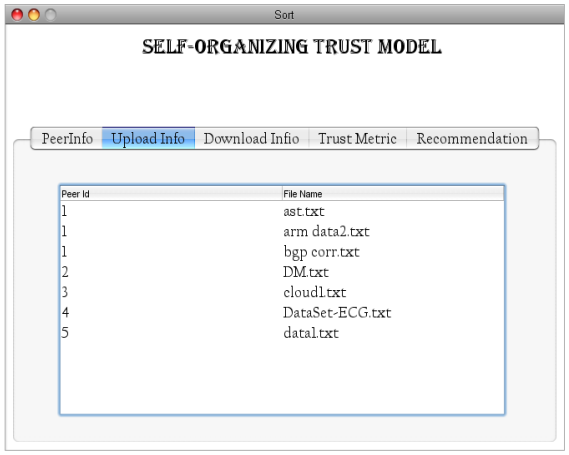
PeerInfo:



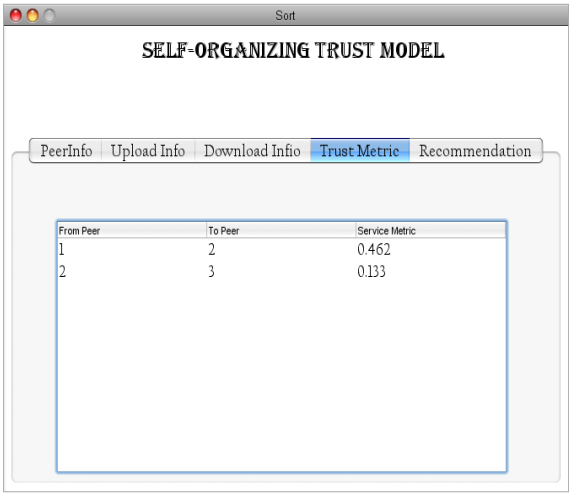
Upload Info:



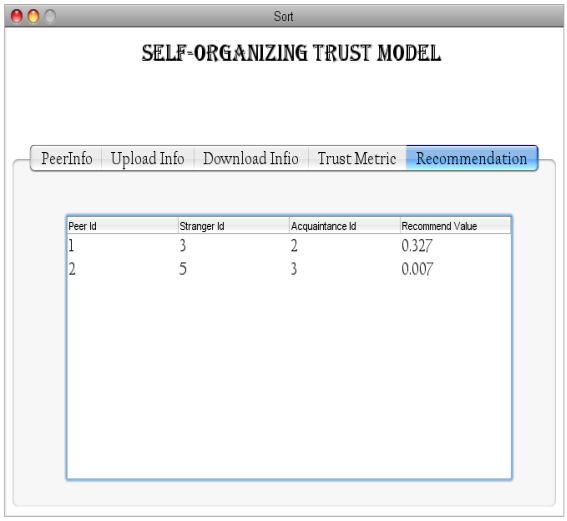
Download Info:



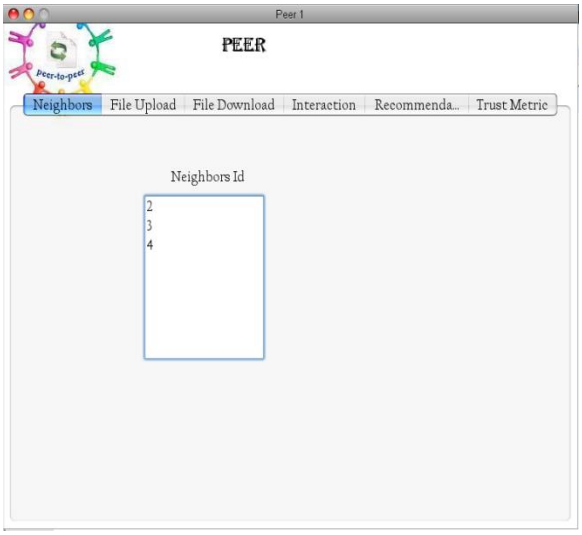
Trust Metric:



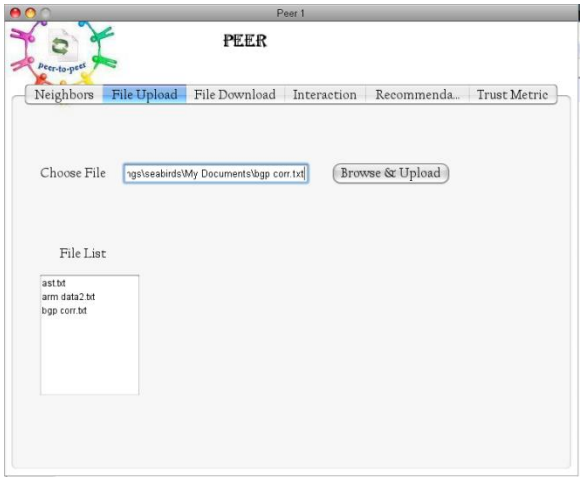
Reccomendation :



Peer1:



Upload Page:



V.CONCLUSION

A trust model for P2P networks is presented, in which 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. Two context of trust, service and recommendation contexts are defined to measure capabilities of peers in providing services and giving recommendations. Interactions and recommendations are considered with satisfaction, weight, and fading effect parameters. A recommendation contains the recommender's own experience, information from its acquaintances, and level of confidence in the recommendation. These parameters provided us a better assessment of trustworthiness.

REFERENCES

[1] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. 33rd Hawaii Int'l Conf. System Sciences (HICSS), 2000.

[2] A. Jøsang, E. Gray, and M. Kinateder, "Analysing Topologies of Transitive Trust," Proc. First Int'l Workshop Formal Aspects in Security and Trust (FAST), 2003.

[3] B. Yu and M.P. Singh, "Detecting Deception in Reputation Management," Proc. Second Int'l Joint Conf. Autonomous Agents and Multiagent Systems, 2003.

[4] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of Trust and Distrust,"

Proc. 13th Int'l Conf. World Wide Web (WWW), 2004.

[5] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1:1-1:31, 2009.

[6] R. Zhou and K. Hwang, "Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr. 2007.

[7] 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.