Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.626 – 632

RESEARCH ARTICLE

EFFICIENT AND DISTRIBUTED NETWORK MODEL FOR P2P SYSTEMS

K.KAYALVIZHI[1]
M.Tech Student
Department of Computer Science and Engineering
PRIST University Pondicherry, India
kkayal1988@gmail.com

BHARATHI.R[2]
Assistant professor
Department of Computer Science and Engineering
PRIST University Pondicherry, India
prist2009cse@gmail.com

ABSTRACT

Peer-to-peer networks are networks composed of heterogeneous and autonomous peers that cooperate with each other in a decentralized manner. All peers are both users and providers of resources and can access each other directly without intermediary agents. In the proposed system, we introduce 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. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. . Finally, an experimental study is conducted on a real P2P prototype, and a large-scale network is further simulated. The results show the effectiveness, efficiency and scalability of the proposed system.

KEYWORDS: Peer-to-peer systems, trust management, reputation, security

I. INTRODUCTION

We 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. No a priori information or a trusted peer is used to leverage trust establishment. Peers do not try to collect trust informa- tion from all peers. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. Since peers generally tend to interact with a small set of peers, forming trust relations in proximity of peers helps to mitigate attacks in a P2P system.

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. An acquaintance is always preferred over a stranger if they are equally trustworthy. Using a service of a peer is an interaction, which is evaluated based on weight (importance) and recentness of the interaction, and satisfaction of the requester.

II. PROBLEM DEFINITION

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. Interactions and feedbacks of peers provide information to measure trust among peers. Interactions with a peer provide certain information about the peer but feedbacks might contain deceptive information. This makes assessment of trustworthiness a challenge

III. PROBLEM DESCRIPTION

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. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on 16 different malicious behavior models. In the experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers.

IV. FEASIBILITY STUDY

The next step in analysis is to verify the feasibility of the proposed system. "All projects are feasible given unlimited resources and infinite time". But in reality both resources and time are scarce. Project should confirm to time bounce and should be optimal in there consumption of resources. This place a constant is approval of any project.

Feasibility has applied to Digital Tune pertains to the following areas:

- Technical feasibility
- Operational feasibility
- Economical feasibility

Technical Feasibility:

To determine whether the proposed system is technically feasible, we should take into consideration the technical issues involved behind the system.

Operational Feasibility:

To determine the operational feasibility of the system we should take into consideration the awareness level of the users. This system is operational feasible since the users are familiar with the technologies and hence there is no need to gear up the personnel to use system. Also the system is very friendly and to use.

Economic Feasibility:

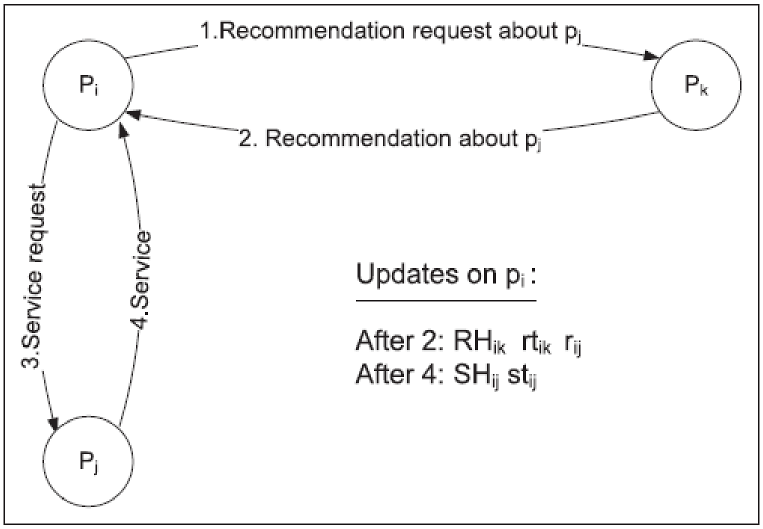
To decide whether a project is economically feasible, we have to consider various factors as:

- Cost benefit analysis
- Long-term returns
- Maintenance costs

V. PROPOSED SYSTEM

In the proposed system, we introduce 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. No a priori information or a trusted peer is used to leverage trust establishment. Peers do not try to collect trust information from all peers. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. Since peers generally tend to interact with a small set of peers forming trust relations in proximity of peers helps to mitigate attacks in a P2P system.

VI. SYSTEM ARCHITECTURE

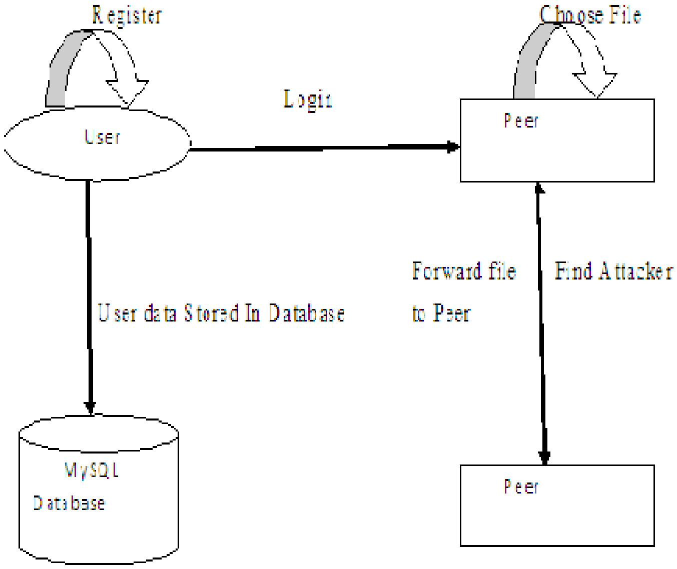

1.Recommendation request about p_j
P_i
P_k
2. Recommendation about p_j
3.Service request
4.Service
Updates on p_i :
After 2: RH_{ik} rt_{ik} r_{ij}
After 4: SH_{ij} st_{ij}
P_j

At the initial phase, TA runs the Setup phase and publishes the system parameters. Then, the company first characterizes the flow chart of an mobile health monitoring program as a branching program which is encrypted under the respective directed branching tree. Then the company will deliver the resulting cipher text and its company index to the cloud, which corresponds to the Store algorithm in the context. When a client wishes to query the cloud for a certain mobile health monitoring program, the i-th client and TA run the Token Gen algorithm. The client sends the company index to TA, and then inputs its private query (which is the attribute vector representing the collected health data) and TA inputs the master secret to the algorithm. The client obtains the token corresponding to its query input while TA gets no useful information on the individual query.

At the last phase, the client delivers the token for its query to the cloud, which runs the Query phase. The cloud completes the major computationally intensive task for the client's decryption and returns the partially decrypted cipher text to the client. The client then completes the remaining decryption task after receiving the partially decrypted cipher text and obtains its decryption result, which corresponds to the decision from the monitoring program on the client's input. The cloud obtains no useful information on either the client's private query input or decryption result after running the Query phase.

VII. DATA FLOW DIAGRAM

A data flow diagram is graphical tool used to describe and analyze movement of data through a system.



VIII. MODULE DESCRIPTION

A. Design Self Organizing Trust Model

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. An acquaintance is always preferred over a stranger if they are equally trustworthy.

B. Implementation of Self Organizing Trust Model

A peer may be a good service provider but a bad recommender or vice versa. Thus, SORT considers providing services and giving recommendations as different tasks and defines two contexts of trust: service and recommendation contexts. Information about past interactions and recommendations are stored in separate histories to assess competence and integrity of acquaintances in these contexts.

C. Find Attacker

In SORT, to evaluate interactions and recommendations better, importance, recentness, and peer satisfaction parameters are considered. Recommender's trustworthiness and confidence about recommendation are considered when evaluating recommendations. Additionally, service and recommendation contexts are separated. This enabled us to measure trustworthiness in a wide variety of attack scenarios.

D. Trust management

Check whether the user is authorized User or unauthorized user. Trusted user only knows the encrypted file Password and decrypted the received file using that Password. Encryption and Decryption using Symmetric encryption Technique. In a key distribution system, a trusted and centralized key server presets and allocates the secret keys to potential users, such that only the privileged users can read the transmitted message. The key server holding the secret key of each receiver can read all the communications and has to be fully trusted by any potential sender and the group members.

E. SCOPE OF THE PROJECT

SORT's performance is the best in all test cases. SORT enables peers to establish stronger trust relationships than NoRQ and FloodRQ methods. In NoRQ, a good peer cannot learn experience of others through recommendations and pseudonym changing lets attackers to launch more attacks. In FloodRQ, collecting recommendations of strangers enables collaborators to disseminate more misleading recommendations. Since SORT collects recommendations only from acquaintances, reputation queries return more reliable information than FloodRQ method.

There are n no of Source, destination, Nodes are there Choose Source and Destination Address forward Packet to Selected node. Node selecting Based on Shortest Path. Then forward Packet to transmitter. Then find Attacker in that file if attacker found means Rectify that file then forward to destination else directly forward to destination . Destinations decrypt the encrypted received file.

XI. 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.

Individual, collaborative, and pseudonym changing attackers are studied in the experiments. Damage of collaboration and pseudo spoofing is dependent to attack behavior. Although recommendations are important in hypocritical and oscillatory attackers, pseudo spoofers, and collaborators, they are less useful in naive and discriminatory attackers. SORT mitigated both service and recommendation-based attacks in most experiments. However, in extremely malicious environments such as a 50 percent malicious network, collaborators can continue to disseminate large amount of misleading recommendations. Another issue about SORT is maintaining trust all over the network. If a peer changes its point of attachment to the network, it might lose a part of its trust network. These issues might be studied as a future work to extend the trust model.

Using trust information does not solve all security problems in P2P systems but can enhance security and effectiveness of systems. If interactions are modeled correctly, SORT can be adapted to various P2P applications, e.g., CPU sharing, storage networks, and P2P gaming. Defining application specific context of trust and related metrics can help to assess trustworthiness in various tasks.

REFERENCES

1. 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.

2. 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.

3. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in P2P Networks," Proc. 12th World Wide Web Conf. (WWW), 2003.

4. L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Ecommerce Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.

5. 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.

6. R. Zhou, K. Hwang, and M. Cai, “Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks,” IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.

7. J. Kleinberg, “The Small-World Phenomenon: An Algorithmic Perspective,” Proc. 32nd ACM Symp. Theory of Computing, 2000.

8. S. Saroiu, P. Gummadi, and S. Gribble, “A Measurement Study of Peer-to-Peer File Sharing Systems,” Proc. Multimedia Computing and Networking, 2002.

9. M. Ripeanu, I. Foster, and A. Iamnitchi, “Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design,” IEEE Internet Computing, vol. 6, no. 1, pp. 50-57, Jan. 2002.

AUTHORS PROFILE

Er.K.KAYALVIZHI, B.E., is pursuing her M.Tech in Computer Science and Engineering in PRIST University, Puducherry, India. She completed her B.E in Computer Science and Engineering in Annamalai University of Engineering and Technology, Chidambaram.

Ms.BHARATHI.R, Received The M.Tech In Computer Science And Engineering. Presently she is A Working Assistant Professor in Computer Science and Engineering at PRIST University, Puducherry Campus, and Puducherry, India.