International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-1 E-ISSN: 2347-2693

Trust Model for Peer-To-Peer Systems

Dipti S. Borade*
Computer Department, University of Pune, India
dipti.borade@gmail.com

Kalpana S. Gulwe
Computer Department, University of Pune,India
gulwekalpana@gmail.com

Ganesh R. Chaudhari
Computer Department, University of Pune,India
ganesh21991@gmail.com

Satish N. Aghav
Computer Department, University of Pune,India
satishaghav100@gmail.com

Mayur A. Ahire
Computer Department, University of Pune,India
mr.mayurahire@gmail.com

www.ijcaonline.org

Received: Dec/22/2014 Revised: Jan/12/2015 Accepted: Jan/19/2015 Published: Jan/31/2015

***Abstract*—**In networked system, peer-to-peer systems are widely used in today's world. Widely growing networks and openness of networked systems brings some sort of insecurities in the interactions and operations. Hence, in this paper, we make a trust network first. In this trust network model, we make some trust relationships between systems or peers which are going to interact. So that, this helps peers to make decisions whether to interact with particular peer or system or not.

Keywords*—Peer-to-Peer Systems, Trust Management, Reputation, Security*

INTRODUCTION

In today's world, all of us are obsessed with the internet. World Wide Web has made us able to interact with any peer over the globe. But as openness increases, Insecurities also increases with that. There are many ways by which malicious peer systems can attack to other peers and make them disable.

Thus, it has become necessary to prevent peers from such type of attacks.Here we develop a Trust Model for peer-to-peer systems. It brings some sort of confidentiality and secureness in the networked systems and mitigates serious type of attacks.Each peer stores its own sign credentials to store trust information. Before interacting, each peer wants to know about strange peers. By using various trust metrics, peers determine whether the peer is a 'Good Peer' or not.

.

I. Computations Structure for Trust Model:

Computational Structure for trust model makes some assumptions. Such as, all the systems and all the peers are equal in computational power. To manage trust relationships, there is no any central or fully trusted peer.Peers frequently leave and join the network. Let us take an example of file uploading or file downloading.

A. Preliminary Notations:

P_i	i^{th} Peer
P_j	j^{th} Peer
A_i	$P_i's$ set of acquainstances
SH_{ij}	$P_i's$ service history with P_j
Sh_{ij}	Current size of service history
Sh_{max}	Upper bound for service history

Table 1: Preliminary Notations

If peer $P_i$interacted with peer $P_j$then$P_j$is stored in the set of acquainstances A_ii.e. P_jBecomes acquainstance of P_i.
Whenever any peer P_i interacts with any other peerP_j , then for each peer, separate service history is stored such asSH_{ij}.

B. Interaction Parameters

i. Satisfaction Value (S_{ij}^k)

Here k is any interaction between two peers *i* and *j*. And S_{ij}^k denotes $P_i's$ satisfaction value with P_j about k^{th}interaction.

ii. Weight Value (W_{ij}^k)

Weight value differs as per application. Let us take an example of application downloading.

In that, weight value can be calculated as follows:
-Speed for downloading
-authenticity of application
-transmission rate of packets
-time required for downloading

iii. Fading Effect (f_{ij}^{k})

$$f_{ij}^{k} = \frac{k}{Sh_{ij}} \qquad where \quad 1 \leq k \leq Sh_{ij}$$

Fading effect maintains the importance of new interactions so that peer cannot misbehave on the basis of old good history.

iv. Metrics to measure Trust Value

-Recommendation Value
-Reputation Value
-Service Trust Value

Algorithm to Get Recommendations:

1. $\mu_{rt} = \frac{1}{|Ai|}\sum_{pk\epsilon Ai} rt_{ik}$
2. $\sigma_{rt} = \frac{1}{|Ai|}\sqrt{\sum_{pk\epsilon Ai}(rt_{ik} - \mu_{rt})\text{^}2}$
3. $th_{high}=1$
4. $th_{low}= \mu_{rt} + \sigma_{rt}$
5. rset= θ
6. While $\mu_{rt-\sigma_{rt}}$<= th_{low} and |rset|< η_{max} do
7. For all $p_k \epsilon A_i$ do
8. If th_{low}<= rt_{ik}<= th_{high}then
9. rec = request recommendation (p_k , p_j)
10. rset= rset ∪ {rec}
11. end if
12. end for
13. $th_{high}= th_{low}$
14. $th_{low}=th_{low} - \sigma_{rt}/2$
15. end while
16. return rset

Before interacting with any strange peer, it asks for some recommendations from its set of acquainstances for stranger peer. After receiving good recommendations from most of the peers, it interacts with the stranger peer. This brings some sort of secureness between peers.

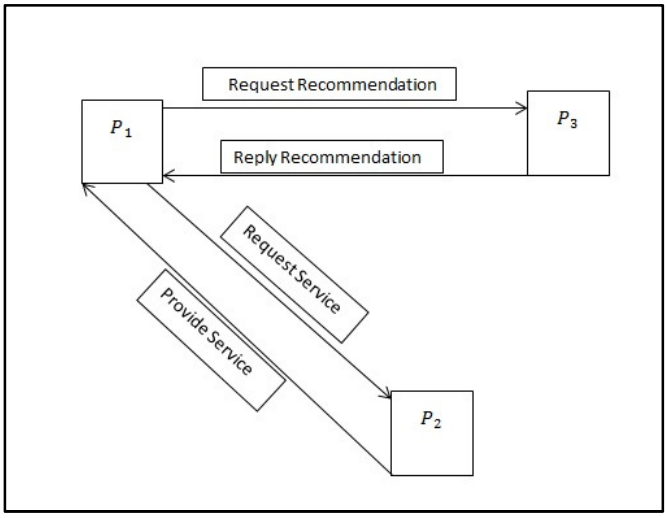

Figure1: Receiving Recommendations

P_1 : Peer1

P_2 : Peer2 as acquainstance of P_1

P_3 : Peer3 as stranger to P_1

II. EXPERIMENTS AND ANALYSIS

In SORT analysis some points studied in the experiments: attacks handler, attacks mitigated, recommendations are not helpful in correctly identifying malicious peers, and which attackers are most harmful.

1. Method

Cycles are run in simulation it represent period of time. It provides the facility of uploading and downloading file. Downloading and uploading file it called session. File is uploaded and downloaded by any user check integrity. Antivirus software are installed in to all peer for detect infected file. Trust calculation methods effect is analysis by following four methods:

1) For uploader selection trust is not used it use bandwidth is called no trust.
2) For uploader selection trust information is used but recommendation information is not calculated from other peer.
3) In this method sort information is calculated.
4) In this method sort equation is used query is flooded in whole network. For mitigating the attack this method is helpful.

2. Attacker Model

Attacker performs two type of attack service based and recommendation based attack. In malicious network good and malicious peer are present. If peer does not having any idea about each other and perform attacks independently it called individual attacker .Individual attackers having different attack behaviour is naive, discriminatory, hypocritical and oscillatory.

Percentage of Service Based Attacks Prevent for Individual Attackers:

10 percent malicious:

Attacker behavior	NoRQ	SORT	FloodRQ
1 .Naive	65.3	73.4	73.5
2. Discriminatory	72.2	78.9	79.9
3. Hypocritical	36.4	61.1	65.2
4. Oscillatory	34.3	63.7	69.6

Table2: 10 percent malicious

50 percent malicious:

Attacker behavior	NoRQ	SORT	FloodRQ
1 .Naive	63.5	65.3	64.7
2. Discriminatory	68.7	72.1	72.7
3. Hypocritical	27.5	43.0	47.5
4. Oscillatory	16.3	37.0	44.0

Table3: 50 percent malicious

III. Conclusion

Trust model is made of Peer two Peer network. In a trust model peer develop a trust network in its proximity. In this network peer develop trust relationship with good peer.Attackers changing nature are studied in the experiments Individual, collaborative, and pseudonym attacker nature check. Peer can isolate malicious peers, in malicious environments such as half of malicious network, collaborators can continue to expand large amount of misleading recommendations. Trust all over the network is maintained in Self-Organizing Trust model. Peer changes It position of attachment with a network, it may be lose a part of its own trust network. These issues are used to study as a future work to extend the trust model. In peer to peer systems Trust information are not solve all security problem but enhance security and effectiveness of systems.

REFERENCES

[1] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-PeerInformation System," Proc. 10th Int'l Conf. Information and KnowledgeManagement (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-BasedTrust 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-BasedTrust Management System for P2P Networks," Proc. IEEE/ACM

