World Journal of Engineering Research and Technology
WJERT
www.wjert.org

IMPLEMENTATION OF VOLATILE SECURE MODEL IN P2P SYSTEM: A DETAILED ANALYSIS

Amina N.*[1] and Prof. Dhaigude T. A.[2]

[1]Student, Department of Computer Engineering, DKGOI'FOE, Swami-chincholi, Daund, Pune, Maharashtra.

[2]Department of Computer Engineering, DKGOI'FOE, Swami-chincholi, Daund, Pune, Maharashtra.

Article Received on 10/05/2015 Article Revised on 02/06/2015 Article Accepted on 25/06/2015

***Correspondence for Author**
Amina N.
Student, Department of Computer Engineering, DKGOI'FOE, Swami-chincholi, Daund, Pune, Maharashtra.
aminanizamudeen@gmail.com
tanajidhaigude@gmail.com

ABSTRACT

In network domain system, the peer to peer systems shows an open access rather than other systems.P2P system defines each peer is able to share the information to other peer without the help of any centralized system. So there are more chances of malicious activities for better security one peer must send some trust parameters along with the recommendations from other peer. This system is fully based on priority, trust worthiness history and peer satisfaction, recommendation. Those peers who is having more recommendations and trustworthiness value, that peer will connect with other peers only. A trust model is derived by integrating the risk management and security, by applying this new method; it provides the utility maximization of peer to peer system. The main objective of the system is to make sure that the peer to peer communication is reliable and secure by the use of the trust model surrounded each and every peer in the system.

KEYWORDS: reputation, recommendation, Security, risk management, trusts management.

1. INTRODUCTION

Peer to Peer network is a collection of independent peers, without using any centralized system. These peers are capable of sharing information among them. Data security is the

main issue in P2P systems. There are chances of malicious activities occur in this system. Trustworthiness are maintaining in peers to avoid the malicious attacks. The most challenging task is to keeping trust on another peer. Because the opponent peers may be a malicious one. To define into the numerical format, the peer is very complex, as the trust is logical and social phenomenon. For the sharing of file between peers, classification of peer as trustworthiness or non-trustworthiness is a big issue and sometimes which is not so efficient. So for the calculation of peer trust, we are using matrices here.

In Peer-Peer communication the trustworthiness is not a sufficient approach. For that we are maintaining the recommendation matrix and reputation along with trustworthiness of the peer.[7, 8] To reduce the malicious activities in a peer to peer distributed system, the technique focuses to maintain the trust relations among peers in their surroundings. In this system, it does not try to collect trust information, While the peers which interacted in the past; each peer creates its own local computation of trust. As like this, good peers make a dynamic trust group which are evaluated from their surroundings and form a system, it can remove malicious peers.[3] Here we calculate the three matrices. The reputation metric, it is the first metric which is calculated according to the peer's recommendations. Among all peers it is important while deciding the strangers and new nodes. Second, the primary metrics to compute trust relation of the service and recommendation. Security measures alone can't measure the malicious behaviors in peer to peer system. There is another techniques used which integrate the risk and security to mitigate the malicious activities.

2. LITERATURE REVIEW

This describes the problems based on reputation trust management for both the data management and the semantic level.[1] We make sure that at both levels requires a scalable data structures and algorithms. No any central control system uses to assessing the trust by computing the reputation of an agent from its former interactions with other agents.[2] It proposes a method for P2P Security, in which the servants can communicate with each other, and pass the information about the reputation of their peers. The method Reputation sharing is based on peer to peer polling algorithm by which on the basis of when the provider before initiating to download, the resource requester can access the reliability of perspective providers.[3] This provides an algorithm which decreases the number of downloads of inauthentic files from a peer-to-peer file-sharing network which assigns that each peer a unique global trust value, based on the peer's history of uploads.[4] It presented a reputation

based trust supporting approach which included the coherent adaptive trust model for qualifying and comparing the trust worthiness of a peer based on a transaction based feedback system.[5] It proposed a reputation-based trust management system for P2P networks that aims to build confidence among the good members of the community and identify the malicious one

3. SYSTEM ARCHITECTURE

In Fig 1. In this model we use with utility maximization which explicitly by linking it with the operation of the underlying security models. It shows the utility, in fact, directly related to the outcome of interaction granted by the security operation.[9] It shows how the risk management can be integrated to security decisions for maximizing utility of the underlying system.

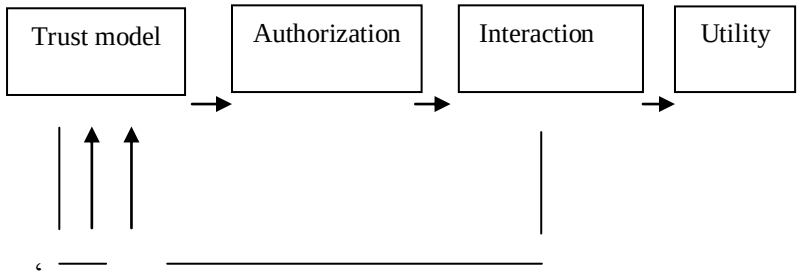


Fig.1. Working of Trust enhanced Authorization

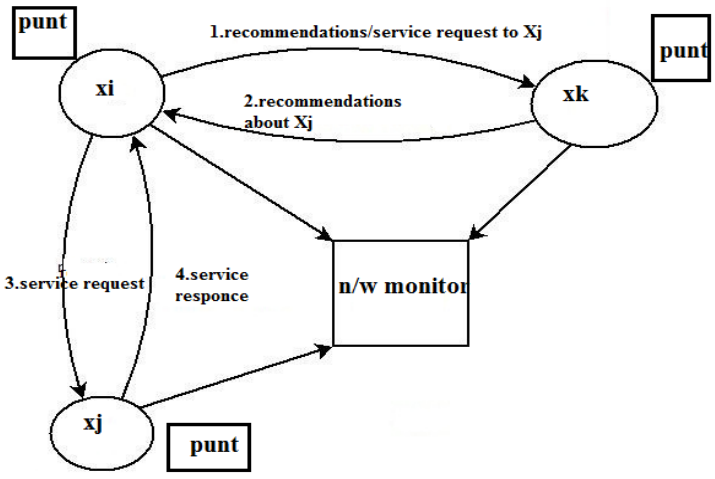


Fig. 2. Working Flow of the system

Now this model presents the conceptual trust enhanced security model that maximizes the utility as depicted in Figure 1. It consists of four blocks: trust model, authorization, interaction and utility. The trust model manages the trust information in the system and

makes trust decisions with risk management consideration; the authorization block, Which performs the standard authorization process with risk consideration; the interaction block which manages the mapping between behavioral evidences and the resulting up-dated trust value; the utility block is used to calculate the system utility at the end of each interaction.[6] The basic idea used here is to use trust information, which is managed by the trust model with risk management consideration, to fine tune the authorization decisions, such that malicious entities are detected through past interactions and will be "weeded out", and benevolent entities will get the appropriate access permissions according to the risk levels, which are done by removing the malicious entities and control interactions with benevolent entities.[10] This way it has to improve the system authorization performance and the maximization of system utility. Then we have to describe the main building blocks of the model as follows.[5] As mentioned earlier, as an example, we are using a mobile agent system and focus it on to its trust based authorization decisions with risk management abstracting away the details of authorization mechanisms. Also to be noted is that the trust model presented in this work is a simplistic one and is used for the sake of clarity in illustrating the new approach. We added a new technique that "punt" block, which calculate the probably un-trustable nodes which are participating the communication. In Fig2., If Xi wants to communicate with Xj, Xi send recommendation request to Xk about Xj, after getting the proper recommendation, then only Xi communicate with Xj. If Xk doesn't contains the information about Xj,Xi consider Xj as a stranger node and give a dummy request to Xj that how fast Xj is responding. According to the response time, its rating can be calculated.

4. ALGORITHM

Reputation metrics

1. thi< =1
2. thl< =μr t+σr t
3. rset< =ø
4. while μr t-rσr t <= thl and
|rset| < μmax do
5. for all dk ε bi do
6. if thl <= rtik <= thi then
7. rec <=RequestRecommendation(pk ,pj)
8. rset <= rsetU rec ,end if, end for
9. thi <= thl

10. thl (<=thl-μrt/2)

,end while

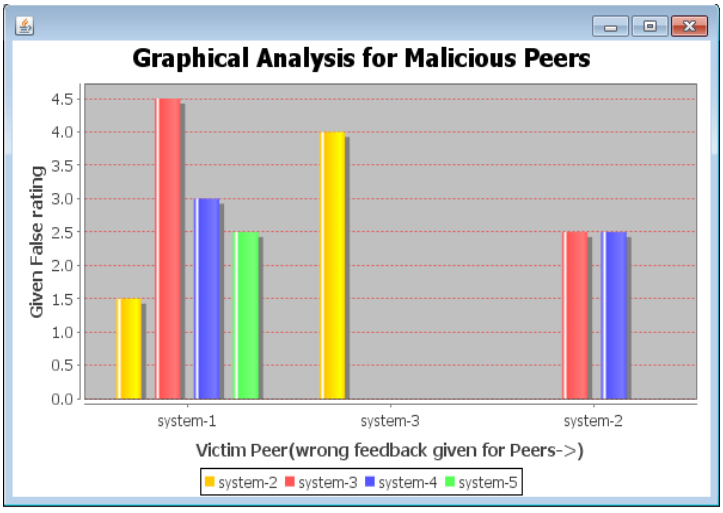
11. return rset

5. RESULT

Table 1. Service Based Trust Calculation

Sr. No	Sender	Receiver	Time required	Feedback (rating)	Analysis (Trustability)
1	System-1	System-2	1 sec.	1.5	Malicious
3	System-1	System-3	2 sec.	3.5	Malicious
5	System-1	System-4	1 sec.	3	Malicious
6	System-1	System-5	O sec.	2.5	Malicious
7	System-3	System-2	1 sec.	3.5	Malicious
8	System-2	System-3	1 sec.	2.5	Malicious
9	System-3	System-2	1 sec.	4.5	Malicious
10	System-2	System-4	0 sec.	2.5	Malicious
11	System-3	System-2	2sec.	4.5	Malicious
12	System-2	System-1	1 sec.	7.5	Trustable
13	System-1	System-2	0 sec.	8.5	Trustable
14	System-3	System-5	2 sec.	8	Trustable
15	System-1	System-2	1 sec.	9	Trustable
16	System-4	System-5	1 sec.	9	Trustable

The experiments are conducted on a file sharing application to determine how the system of this secure model who mitigates the attacks. The Table 1. shows that how much recommendations are (or not) helpful in correctly identifying malicious peers,how this secure model handles attacks and how much attacks can be mitigated. The number of service based attacks with respect to time is the most important output parameter.It shows that this model is successful about this type of attacks.In a malicious network service and recommendation based attacks affect the reputation of the peer.



6. CONCLUSION

This new approach is very useful in trust calculation and its relationship. This is introduced a way of thinking about security. It maximize the utility and provide a good economical benefits. Here recommendations are the important to find the attackers. It mitigate the both service and recommendatiuon based attacks in most experiments.

7. ACKNOWLEDGMENT

This is to acknowledge and thank to one and all that played defining role to prepare this paper. All Faith and honor to GOD for his grace and inspiration. I take this opportunity to express my sincere thanks to my Guide, Department head, PG coordinator and all my family members and friends to support me to prepare this paper.

REFERENCE

1. Ahmet Burak Can, Bharat Bhargava.”‘SORT: A Self -Organized Trust Model In Peer-Peer system”’, IEEE Transaction for 2001 Dependable January-February 2013.
2. Despotovic.” Managing Trust in a Peer-2-Peer information System, Proc. 10th Intl Conf. information and Knowledge Management (CIKM) 2001.
3. F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, Choosing Reputable Servents in a DISTRIBUTED Network, Proc. 11th World Wide Web onf. (WWW), 2002.
4. S. Kamvar, M. Schlosser, and H. Garcia-Molina. ”The(Eigentrust)Algorithm for Reputation Management in DISTRIBUTED Networks.” Proc. 12th World Wide Web Conf. (WWW), 2003.
5. L. Xiong and L. Liu. ”Peertrust: Supporting Reputation-Based Trust for Distributed Ecommerce Communities.” IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.
6. B. Yu and M. Singh. ”A Social Mechanism of Reputation managementin Electronic Communities.” Proc. Cooperative Information Agents(CIA), 2000
7. Z. Despotovic and K. Aberer. ”Trust-Aware Delivery of mposite Goods.” Proc. First Intl Conf. Agents and Distributed Computing, 2002.
8. F. Cornelli, E. Damiani, S.C. Vimercati, S. Paraboschi, and P. Samarati. ”A reputation-based approach for choosing reliable resources in Distributed networks.” In CCS02, Washington DC, USA 2002.

9. K. Aberer, A. Datta, and M. Hauswirth. ”P-Grid: Dynamics of Self- Organization Processes in Structured DISTRIBUTED Systems.” Distributed Systems and Applications, vol. 3845, 2005.
10. R. Zhou and K. Hawang. ”Power trust A Robust and Scalable Reputation System for Trusted Distributed Computing.” IEEE transaction Parellel and distributed system, vol.18, no.4 apr 2007.