An efficient way to improve the security in Peer-to-Peer network using the Closed Trusted Community

V.Masthanamma, M.Narayanan

Abstract— Recently peer to peer systems are developing a lot. In the same way they are not secured. So am using the trusted community to develop the peers. By using this community they can develop a trusted relationship. Nowadays they were using the closed communities to secure and develop the peers. This closed community will be in large strength. But in the trusted community there will be the less strength and moreover it does not contain not more than three members. That means if the acknowledgement is received the information will be shared. So this is said to be trusted community. To implement this paper am using an algorithm called as trusted graph. The advantage in this paper is that we can check the trust level of the peer.
.

Index Terms— closed communities, CTS, trusted graph, trusted level, trusted relationship, P2P trusted community, valid acknowledgement

1 INTRODUCTION

Nowadays peer-to-peer networks becomes very insecured. And it can be secured using some closed communications, trusted communities etc. In this paper we are implementing the trusted communities to spot out the insecured P2P networks. By using this we can reduce the malicious activities in P2P systems. And moreover peers do not need to get the trusted data of all peers. Every Peer in the group will develop a individual concreta to make it trusted. Since every peer will generally meet a particular groups of peer in which that peer forms a more trusted relationships so that the nearness of space of the peer will make it easier to severe attacks in Peer-to-Peer systems. When we are using the trusted communities information can be shared. The advantage in this is cost can be reduced scalability ,reliability can be improved and autonomy is impoved. The main aim of this paper is to plan and prove the security, the group of people in the store shares the trust data which is fully controlled by peers.

This trusted data will also be helpful for commercial transaction applications which can be done electrically. So that consists of group of people who like and who congregate virtually to trade with each other. It can be used for buying and selling within the medium and that will be in the form of scales, and the bandy times will be depending upon the prevalent causes.

Since the stores are managed by the set of peers for some special purposes, so that will not be examined by the people who does not slog in the particular connection . As an alternative of the assure hold up related to the particular peers and reserved peer will be was used to assure the different ranges of assures which belongs to the circle of closed simlarity, particlar ranking and some kind of beliefs in the group.

The community trust stores(CTS) needs to be encourged to trust the related peers of the same group and so the peers can be reducing the recongized threats whle in the process of buying and selling of peers from every group. Because the peers must be accessed at anytime of the occasion the selling or buying may occur. And there process have to be saved in the assured data and that information must be believed. This will easily attained by helping the related personalities. However if a outlet saves the original or the individual opinion, that must be joined to a separate forum founder. So it can also able to address to issues of the safe evaluation to the assured information between the same group of peers. This can be able to solve the issues of the various types of peers that are residing online at various times.

i. The main advantage of trusted community is that proper controls for password and access can be set.
ii. set the password renewal
iii. prevent users by using the same passwords.

2 RELATED WORK

There are so many formal trusted model based on social logical foundations. That means an agent will built the own trusted applications and he will depend on other information of others. There are many different methods like propagating the trusted information through trusted referral chains. Referral means the major technique for rising assuring in the added processes and the next technique in which we can independent upon the assurity, prevalent causes, and exchange of ideas. That means it can be spreaded all through numerous referral

- *V. Masthanamma is currently pursuing UG program inSaveetha University, India, PH-9710696007. E-mail: masthana95@gmail.com*
- *M. Narayanan is currently pursuing Assistant Professor, Department of Computer Science, Saveetha University, Country, PH-938148513. E-mail: narayanan_baba@gmail.com*

chains. Third technique is based upon the oblique assurity between the relationships that might able to occur wrong assurity source. So the assured topologies must become very careful in executing before spreading assured data. These three methods can be done using the one trusted relationship. So that systems will meet the more further and additional faces or confront to meet any challenge comparing to commercial transaction platforms [1].

In this paper they are concentrating on trusted management systems. And these trusted management structure and basically it can classify as prevalent causes based trusted structures, social network based trusted systems and policy based trusted systems. The reputation based trusted system in which trusted evaluation will be based on measuring reputation. It will measure the trust in peer and trust in reliability. In this paper they are approaching can be able to address the issues of prevalent causes based trusted organization equally in the data running and also in the graphic stage. That means social networks are based are social relationship between the peers and policy based systems will prefer official document proof to be shown to establish trusted connection for the particular right to use and at the same time to manage it perfectly [2]. Botnet means it is a network of compromised computers called Zombie computers or bots, under the control of remote attacker. Bots are the useful tool. In this peer to peer botnets they presented a theoretical part (in the form of graph) model of the P2P botnets that analyses the elasticity of some botnets. It is valid for two resilience aspects:

1. Intellect gathering elasticity: In this elasticity it will evaluate the P2P botnets that are able to detect malware analysts by enumerate the bots into the network.
2. Interruption elasticity: It officially attacks and that can be used to disrupt P2P botnets [3].

In hybrid peer to peer system for distributed data sharing may consists of two parts.

i. That means combining the advantages of peer to peer networks.
ii. Minimizing their advantages.

The first one describes about the structured core network which contains overall backbone of hybrid system. The second one is made of various formless peer-to-peer networks. And each core in the network is attached to a node. In two tier hierarchy if the server is crashed the entire system are collapsed. If we set the public or private keys for data sharing, it will easily detect by intruder. If we use client-server model has load imbalance problem [4].

In this paper they were discussing that how to protect the people who use it can also get help from the circulated organizations using distributed CAs. At the same time even distributed CAs plays a vital role in it. They are assuming the distributed system with one or more central components. First is publics which can be a massive and huge classification that consists of a particular position of autonomously handled servers. Second is dynamic trust management which encapsulates the trust management in dynamic distributed environments, in which the members of the system assumes the frequently changing multiple roles. Third is the role-based access control associates permission with roles and not with users. Fourth is cryptographic binding enables an individual power to digitally sign a file without viewing the content of the file [5].In structured P2P strong consistency is provided by organizing replica nodes to an auxiliary structure on top of the overlay for update propagation. But in unstructured P2P it consists of two sorts of bordered reliability

i. **Adapted to bordered reliability**. In this the replica chains can be helpful to make sure that it gains the confident possibility.
ii. **Time bordered reliability** Push and pull techniques can also be used as another way to indicate the valid period for a replica copy [6].

In this paper they were discussing about the two kinds of networks. 1. Hybrid P2P networks 2.pure P2P networks. In hybrid P2P networks it consists of a server and each peer has to depend on another peer and it has to interact with it and should share its resources. In pure P2P networks it does not server and it has to find other peer and share its resources. And both have some disadvantages. To overcome that they were forming the communities so that it can solve many problems. And peers can also build their own communities. And these communities can provide co-operative and influential information [7]. In this paper they were discussing about the reputation trust management. Because in P2P networks it does not contain the fixed clients and servers. So every peer functions as both client and server. And it provides an open, limitless environment for sharing the content. This makes the attackers to easily spread the malicious content. So by using the reputation based systems we can able to create the trust within the members.

The advantage is it can able to prevent the spread of the malicious peers. And it will be highly useful to prevent the malicious content [8].

3. PROBLEM STATEMENT

The whole network learns about the trusted information through the search and the updates of the trusted information. While designing the algorithm first is to develop the searching methodology and the quality of the search. Second is it should contain the large number of files. Third is it should contain large storage capacity. Fourth is it should be able to protect the privacy peers.

These are works when implementing an algorithm.

The three main works are

i) Search
ii) Acknowledgement
iii) Feedback

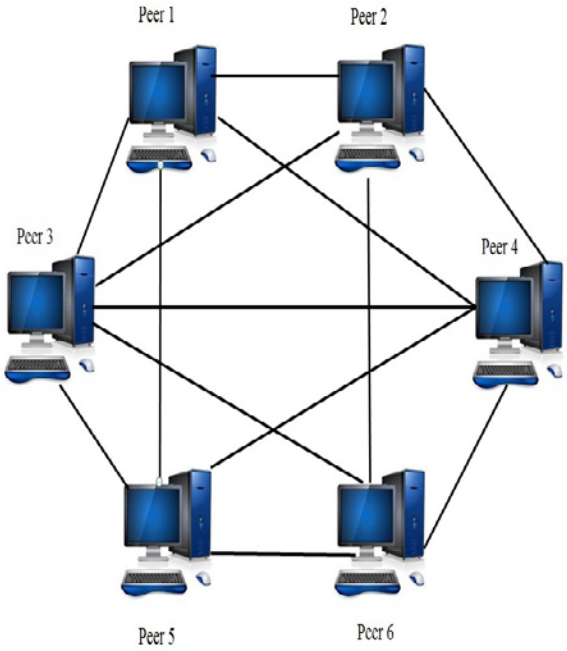
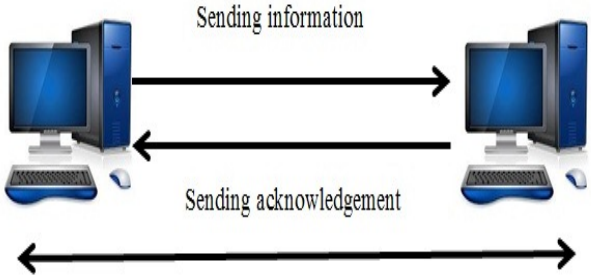


Fig.1:P2P network closed community diagram

In Fig. 1: it contains number of peers. All the peers are connected in a closed community. If any person shares the information it will be sent to all the peers. Because all the peers are connected serially. And if any system fails, the whole network will be lost.or the whole network will be failed



Trusted community
Or
Trusted peer

Fig.2: trusted community

In Fig.2: it forms a trusted community. Suppose if any one system sends the information to another system. The other system will send an acknowledgement. If the acknowledgement is received by another system it forms a trusted community or trusted peer.

4. Algorithm for Constructing a Trusted Graph

```
ALGORITHM FOR CONSTRUCTING A TRUSTED GRAPH

Assume Peer Pr is Estimate the dependability of peer Pn
P is the set of peers being called.
FOR Every Peer Pi is 2 P and Pi has not been queried
        THEN DO
IF Depth (Pi) is Less than Depthbound THEN
                Pr Queries Pi
    IF (Pi is a witness of Pg) then
            Pi RETURNS the RATING about Pn to Pr
               ELSE
   FOR EVERY referral r = hPi ; Pji from Pi
   DO
              IF Pj 2 is Assigned to P THEN
            ADD r into R and ADD Pj into P
                 ELSE
            Disregard referral r
                End IF
          END FOR
        END IF
     END IF
END FOR
```

5. CONLUSION

In this paper we explained about the search technique that solves many troubles in the peer to peer network for example: no protection, less trust management etc. it also controls the malicious peers. Also provides more security. The advantage is that by using this algorithm it provides a trusted community. It can also be secured using P2P e-commerce. The disadvantage is that we cannot apply this method for the large peers. Because if it contains a large number of peers it is impossible to maintain a trusted community. So it is applicable only for the small communities. And it also increases the security level of the P2P networks. We are also interested to study about the standing mechanism in P2P systems with other topologies.

ACKNOWLEDGEMENT

The author likes to express their sincere thanks to Mr.M.Narayanan, Assistant Professor, Department of computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Thandalam, Chennai, Tamil Nadu, who had supported me and helped me to do this work. His valuable suggestions motivated me to do this paper in a successful manner.

REFERENCES

[1]. AhmetBurak Can, Bharat Bhargava, *" A Self-Organizing Trust Model for Peer-to-Peer Systems"*, IEEE Transactions on Dependable and Secure Computing, vol.10, no. 1, pp. 14-27,Jan.-Feb. 2013, doi:10.1109/TDSC.2012.74.

[2]. ChithraSelvaraj and Sheila Anand,*"A Role Based Trust Model for Peer to Peer Systems Using Credential Trees"*, International Journal of Computer Theory and Engineering, Vol. 3, No. 2, April 2011ISSN: 1793-8201

[3]. Berkeley, "*Modeling and evaluating the resilience of peer-to-peer botnets'*, May 19, 2013 to May 22, 2013ISBN: 978-1-4673-6166-8 pp.: 97-111

[4]. Min Yang, "*An Efficient Hybrid Peer-to-Peer System for Distributed Data Sharing*", IEEE Transactions on Computers, vol.59, no. 9, pp. 1158-1171, September 2010,doi:10.1109/TC.2009.175

[5]. Prashant Dewan, "*P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains*", IEEE Transactions on Knowledge & Data Engineering, vol.22, no. 7, pp. 1000-1013, July 2010, doi:10.1109/TKDE.2009.45

[6]. Yi Hu, Laxmi N. Bhuyan, Min Feng, "*Maintaining Data Consistency in Structured P2P Systems*", IEEE Transactions on Parallel & Distributed Systems, vol.23, no. 11, pp. 2125-2137, Nov. 2012, doi:10.1109/TPDS.2012.81

[7]. Yao Wang, "*Trust-Based Community Formation in Peer-to-Peer File Sharing Networks*", Department of Information and Computer Science, University of California, Irvine, CA 92697-3425, USA2VMware Inc., Palo Alto, CA 94304, USA2

[8]. A li Aydın Selcuk,Ersin Uzun,and Mark Resat Pariente,"*A Reputation-based Trust Management System for P2P Networks*", Department of Information and Computer Science, University of California, Irvine, CA 92697-3425, USA2VMware Inc., Palo Alto, CA 94304, USA