ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Secure Data Sharing in Peer to Peer Network Using Replication and DHT Algorithm

V.Ramkumar[1]

PG Scholar, Department of Computer Science and Engineering, Coimbatore Institute of Technology, Coimbatore, India [1]

ABSTRACT: Data sharing in the P2P became an important function in the trustworthy computing. Secure and trustworthy file sharing is vital to improve overall performance of peer-to-peer (P2P) file sharing systems. In this project, this study about the effectiveness of secure file sharing, searching and tracing system, which proves the necessity of proximity- and interest-aware clustering. Sharing the file in the P2P is became essential factor in the trustworthy network. Users of the network need to share the data anytime within the peer network. While transferring the file, security of the file is the most important one from malicious attackers. Malicious attackers can do two things they may damage our file and they may mismatch the file which have already exist in the network. So it will provide a great issue in the P2P network. for this issue this paper provide the effectiveness of secure file sharing mechanism and also it find out the malicious attackers with the help of the reputation value using follower- and cluster-based file replication algorithms to enhance file search efficiently in the peer network.

KEYWORDS: P2P Network, file sharing, malicious attackers, replication algorithm and secure transactions.

I. INTRODUCTION

Peer-to-peer file-sharing networks facilitate users to share files – several file like music, video, spreadsheets. P2P networks present a ready-made sharing transportation that is tricky to block and even harder to trail, provided that cover for spying and illicit activity [1].

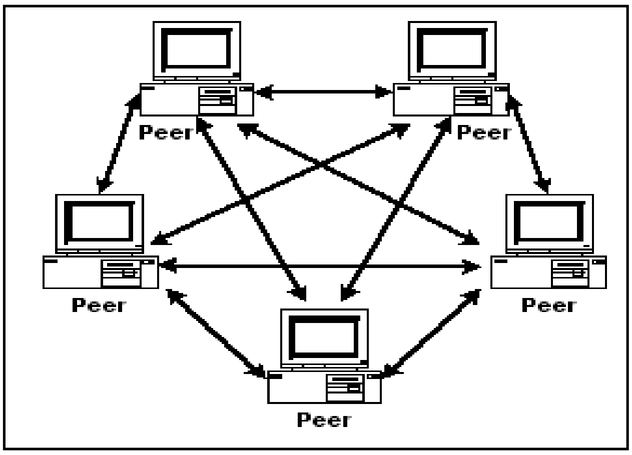

Figure 1: Peer to peer Networks

Peer-to-peer file distribution is a growing security risk for firms and persons. Users who partake in these networks to distribute music, pictures, and video are subject matter to many protection risks including inadvertent distribute of private information, exposure to viruses and worms, and the penalty of spyware. In this paper, it scrutinizes the peer-to-peer file sharing happening including an indication of the industry, its business models, and development. It portrays the information security hazard users' face including personal classification disclosure and leakage of proprietary business information. Security matter of peer in current P2P networks are calculated "publish" or to "share" data. The

DOI: 10.15680/IJIRCCE.2016. 0403177

user configures the client software to distribute items in a meticulous folder, and directs the client to move meticulous files and deposit them in that folder [2]. In regular operation, a P2P client purely writes files to disk as it downloads them and examine files from diskette as it uploads them. There are several routes for confidential data to get on to the network: a user unintentionally shares folders enclose the information, a user supplies music and other data in the same folder that is public, a piece of software the user has preferred to download and implement surreptitiously shares it (malware) and client software virus result in unintended distribution of file directories [3]. In P2P networks which share out resources of undecided authority, the issue of lack of obscurity becomes evident. For example, the BitTorrent file sharing system straight exposes the IP address of peers to each other in a crowd. This would allow peers in the swarm to know the distinctiveness of other peers who are downloading definite resources [4, 5]. They were lots of difficulty in the peer network. Hence our proposed work concentrate on avoiding malicious attackers with the help of the DHT (Distributed Hash Table) and also used the Trusted peer to peer concept to share the data in the peer network with secure access with the help of reputation model it provide the rank for every network which contains positive and negative ranks, using this model it calculate the positive and negative aspects. If it shows the positive aspects it will continue with that trusted peer network and if it shows negative aspects if does not provide the data sharing and data accessing in the network. So it helps to share the data in secure manner.

II. LITERATURE REVIEW

N. Naoumov et al [6] from this paper proposes a secure and useful reputation based distributed trust administration model which uses Self-certification, an identity management method, and a cryptographic protocol that make possible making of secure repute data in a P2P network, in order to accelerate uncovering of scoundrel This paper discusses the reputations managed in the network, the corresponding reputation information specified to peers and recognition of malicious nodes. Once the malicious nodes are acknowledged based on their download's ratios and behavior in the network, as an alternative of banish the selfish peer entirely, the planned system make available services at lower bandwiDHT and its occurrence can boost up network routine. The projected model is more protected, vigorous and successful on harass from various malicious peers, counting peers with malicious behaviors and peers with defense threats, and shows more enhancement in the protection feature of the trust administration.

D. Schoder, [7] from this paper author analyzes the trust model for P2P networks is accessible, in which a peer can extend a trust network in its immediacy. A peer can separate malicious peers approximately itself as it develops conviction relationships with good peers. Two situations of trust, service and suggestion contexts are definite to determine capabilities of peers in provided that services and generous recommendations. Communications and recommendations are measured with happiness, weight, and evaporation effect parameters. A recommendation encloses the recommender's own understanding, information from its connections, and level of assurance in the suggestion. These limitations afford us a better measurement of dependability. Individual, mutual, and assumed name changing attackers are intentional in the experiments. Damage of association and simulated spoofing is reliant to attack behavior. Although suggestion is important in duplicitous and oscillatory attackers, pseudo spoofers, and associate, they are fewer useful in naive and unfair attackers. SORT alleviates both service and recommendation-based harass in most experiments. Using belief information does not solve all refuge problems in P2P systems but can augment security and helpfulness of systems.

Prashant Dewan and Partha Dasgupta [8] Peer-to-peer (P2P) networks are defenseless to peers who cheat, proliferate malicious code, parasite on the network, or simply do not assist. The traditional security techniques urbanized for the federal distributed systems like client-server networks are deficient for P2P networks by the good quality of their federal nature. The nonappearance of an innermost authority in a P2P network poses exclusive challenges for reputation management in the network. These brave include uniqueness administration of the peers, secure reputation data management, Sybil attacks, and above all, accessibility of reputation data. In this paper, we present a cryptographic procedure for make sure protected and timely accessibility of the reputation data of a peer to other peers at enormously low costs. The past performance of the peer is summarize in its digital reputation, and is consequently used to predict its prospect actions. As a result, a peer's standing motivates it to collaborate and desist from malicious activities. The cryptographic procedure is coupled with self-certification and cryptographic mechanisms for uniqueness organization and counter Sybil attack. We illustrate the safety and the competence of the system systematically and by means of simulations in an entirely decentralized Gnutella-like P2P network.

Ahmet Burak Can and Bharat Bhargava [9] presents distributed algorithms used by a stare to motive about dependability of other peers based on the accessible limited information which enclose past relations and recommendations established from others. Peers collaborate to found trust among each other without using a priori information or a belief third party. A peer's reliability in given those services, e.g., uploading files, and giving suggestion is evaluated in service and recommendation circumstance Three main faith metrics, examine trust, reputation, and recommendation trust, are defined to specifically measure trust-worthiness in these contexts. An interaction is appraised based on three parameters: happiness, weight, and fading effect. When appraise a suggestion, as well as to these parameters, recommender's trustworthiness and confidence about the information supply are considered. Observations make obvious that malevolent peers are identified by good peers. The attacks are alleviating even if they gain high reputation. Mutual recommendation-based attacks might be victorious when malicious peers make favoritism between good peers. But the identity altering is not a good harass strategy.

III.PROBLEM DEFINITION

In existing work we find the problem of security issues in the peer network. While transferring the file in peer network, the security of the file is the most important one from malicious attackers. They were malicious attackers are inside the network and can do the un-wanted thinks for blemish the user action [10, 11]. Those malicious attackers can do two things they may damage our file and they may disparity the file which have already survive in the network. So it will provide a large issue in the P2P network. However, in extremely malicious environments such as a 50 percent malicious network, collaborators can persist to broadcast large amount of misleading suggestion Another issue about SORT is preserve trust all over the network. If a peer modifies its point of accessory to the network, it may lose a part of its trust network.

IV. SECURE FILE TRANSACTION USING REPLICATION AND DHT

Data sharing in the P2P develop into an important purpose in the reliable computing. Protected and trustworthy file distribution is vital to progress overall recital of peer-to-peer (P2P) file distribution systems. Most of the user needs protected way of transaction in every network. For the user require this paper study about the usefulness of secure file sharing, penetrating and tracing system, which establish the necessity of proximity- and interest-aware clustering and proposes dissimilar approach to guide nodes to frontward a file query to friends that are supplementary trustworthy and more possible to resolve the question or forward the query to file possessor [12]. This also proposes follower- and cluster-based file duplication algorithms to enhance file investigate efficiency. This effectively finds the users curiosity and behavior in P2P, which helps to compute the standing value. Based on the reputation value, the system allocates services. The results of proposed system P2P display the higher efficiency, dependability, and dynamism-resilience of SOCNET determine up to with other systems. and it provide various compensation likes search efficiency, Tracks file admission in Peer groups, identifies malicious performance in peer groups, Calculates reputation attain based on the behavior, Fast search alternative using DHT and also afford services based on the score it also enclose the clustering method which helps to group up the positive and negative aspects. They were lots of troubles in the peer network. So here we used distributed hash tables to store and retrieve the frequently used contents or files in the peer network and also used the reputation model to calculate the value of most appropriate one in the peer networks.

a. Distributed hash tables

Distributed hash tables are similar to dispersed data structures that are used in P2P submission to store and retrieve data competently. In a classic hash table, hash table objects are amass in dissimilar buckets according to each object's confusion value which is obtained by applying a hash function to the data being stored. Since the information search for mechanism is logarithmic, the systems that make use of DHTs are tremendously scalable. When the number of nodes in the network doubles, only one additional hop is needed to discover any given node [13, 14]. In DHT P2P networking, every node in the system has a globally exclusive identifier. It provides decentralized process, devoid of the need to preserve a federal server to organize the P2P network.

b. Reputation model

This model is autonomous of the topology of the P2P network, addressing method for its nodes, bootstrap mechanisms, combination and departure protocols of peers, and the name service. In other words, the choice of any of this machinery has no impact on the reputation representation and vice versa. If the system allows the peers to issue both positive and negative recommendations to other peers, some peers might get victimized by bad orifice i.e., a petitioner can

DOI: 10.15680/IJIRCCE.2016. 0403177

potentially issue a negative recommendation to the contributor even if the contributor deserved a positive recommendation for a given transaction. On the other hand, if only positive suggestion is allowed then it would be hard to differentiate a relatively new peer from a chronic bad peer [15]. Therefore, here we make an supposition that both positive and negative recommendations are allowed and a given peer will stop interrelate with peers who frequently issue negative recommendations.

V. EXPERIMENTAL RESULT

Our proposed system helps a lot in the peer network to maintain the trust. Hence our proposed work concentrate on avoiding malicious attackers with the help of the DHT (Distributed Hash Table) and also used the Trusted peer to peer concept to share the data in the peer network with secure access with the help of reputation model it provide the rank for every network which contains positive and negative ranks, using this model it calculate the positive and negative aspects. If it shows the positive aspects it will continue with that trusted peer network and if it shows negative aspects if does not provide the data sharing and data accessing in the network. So it helps to share the data in secure manner. This experimental result shows the difference of existing and the proposed system progress.

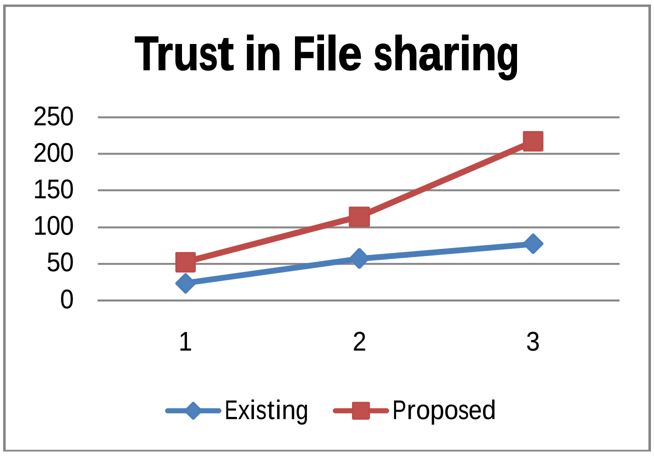

Chart 1: Trust in File sharing among peer network

Here this chart represents the comparative of trust in the peer network while sharing the file in the network. When compared to the existing system our proposed one provide more trust when compared to existing one.

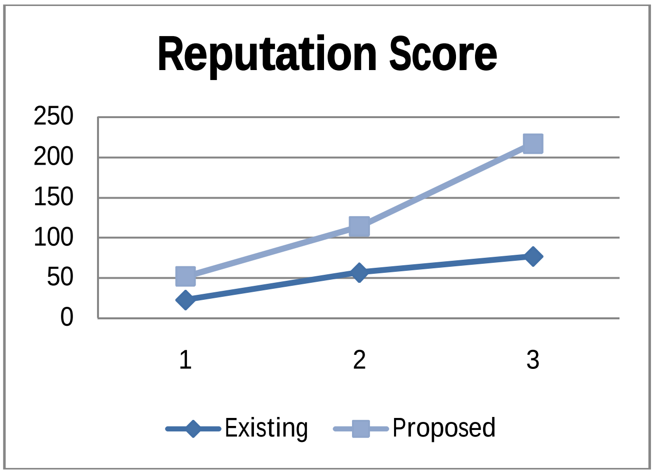

Chart 2: Reputation score calculation

DOI: 10.15680/IJIRCCE.2016. 0403177

This chart represents the reputation score for the existing and proposed method in existing it didn't well worked with the reputation values but in our proposed system it shows better result for finding the positive and negative aspects. When compared to the existing system it works well. It find the malicious attackers and it deny their actions and also it does not share any file with that network so it will be the great advantages for our proposed one.

VI. CONCLUSION

Secure transaction is an important factor in any fields. Peer network is a connection of many systems and used for sharing the file within that network. While sharing malicious attackers may arise for misbehavior the file. They may do 2 things firstly they will duplicate the file and secondly spoil the file. So the user of the peer network may lock into trouble. For avoiding those troubles from the malicious attackers this paper propose the cluster-based file replication algorithms to enhance file search efficiency and secure way of transferring the file in peer network. So it helps to share the data in secure manner.

REFERENCES

[1]. J.Risson, T. Moors. "Survey of Research Towards Robust Peer-to-Peer Networks: Search Methods." Technical Report, University of New South Wales, Sydney, Australia. 2004.

[2]. Crocker. "Host Software." RFC 1. 1969. http://www.faqs.org/ftp/rfc/rfc1.txt

[3]. "P2P or Peer-to-Peer Safety, Privacy and Security." Federal Trade Commission. 2004.

[4]. M. Suvanto. "Privacy In Peer-to-Peer Networks." Helsinki University of Technology. 2005.

[5]. "P2P Networks Hijacked for DDoS Attacks." Netcraft. 2007.

[6]. N. Naoumov, K. Ross. "Exploiting P2P Systems for DDoS Attacks." International Workshop on Peer-to-Peer Information Management. 2006.

[7]. D. Schoder, K. Fischbach. "Core Concepts in Peer-to-Peer (P2P) Networking."

[8]. Prashant Dewan and Partha Dasgupta, "P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains".

[9]. Ahmet Burak Can and Bharat Bhargava, "SORT: A Self-ORganizing Trust Model for Peer-to-peer Systems".

[10]. Guoxin Liu, "An Efficient and Trustworthy P2P and Social Network Integrated File Sharing System".

[11]. Castro, Costa, Rowstron. Performance and dependability of structured peer-to-peer overlays. *December 2003.*

[12]. M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," Proc. Fifth Symp. Operating Systems Design and implementation, pp. 299-314, Winter 2002.

[13]. Timo Tanner, "Distributed Hash Tables in P2P Systems - A literary survey"

[14]. Li, Stribling, Gil, Morris, Kaashoek. Comparing the performance of distributed hash tables under churn. *February 2004.*

[15]. E. Damiani, D. di Vimercati, S. Paraboschi, P. Samarati, and F.Violante, "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks," Proc. Conf. Computer and Comm. Security (CCS '02). pp. 207-216, 2002.