Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Data Sharing Between Peer-to-Peer Using Trust Model

Mr.Janmejay Kale[1] and Prof.V.R.Chirchi[2]
[1]*Student, PG Department, MBES College of Engineering*
[2]*Asst.Professor, PG Department, MBES College of Engineering*

Abstract— Peer-to-Peer network information sharing environments are increasingly gaining the acceptance on the internet as they provide an infrastructure in which the desire information can be located and downloaded while preserving from both the requesters and Providers. Open nature of peer-to-peer network exposes them to malicious activity. Building trust relationships among peers can reduce 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 contiguity 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. The Aim of this Paper is reduces the malicious activity by using self-organizing Trust Model.

Keywords— Peer-to-Peer Networks, Trust Management, Reputation, Security

I. INTRODUCTION

PEER-TO-PEER (P2P) network rely on combination of peers to accomplish tasks. Ease of performing malicious activity is a threat for security of P2P networks. 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 calculate 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 trust-worthiness a challenge.

In the presence of an authority central server is considered way to stored and manage the trust information. The central servers securely store the trust information and define the trust metrics. Since, there is no central server concept in most P2P networks, Peers organized them to store and manage the trust information about each other [1], [2]. In pure P2P networks, peers act as equals, merging the roles of clients and server. In such networks, there is no central server managing the network, neither is there a central router. Typically, each client is able to act according to the momentary need of the network and can become part of the respective overlay network used to coordinate the P2P structure. Management of the trust information is dependent of structures P2P network. By far the most common type of structured P2P network is the distributed hash table (DHT), in which a variant of consistent hashing is used to assign ownership of each file to a particular peer, in a way analogous to a traditional hash table's assignment of each key to a particular array slot. In Distributed Hash Table (DHT) based requests, is peer become a trust holder by storing

feedback of other peers. Global trust information stored by the trust holder can be accessed through Distributed Hash Table efficiently.

An unstructured P2P network is formed when the overlay links are established arbitrarily. Such networks can be easily constructed as a new peer that wants to join the network can copy existing links of another peer and then form its own links over time. In an unstructured P2P network, if a peer wants to find a desired piece of data in the network, the query has to be flooded through the network to find as many peers as possible that share the data. In unstructured P2P networks each peer, stores the trust information about the peers in its neighbor or peer interacted in the past.

Aim of this paper to reduce malicious activity in P2P network by using self-organizing trust model by establishing trust relations among peer in the contiguity. No a priori information or a trusted peer is used to credit 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 contiguity and can isolate malicious peers. Since peers generally tend to interact with a small set of peers [7], forming trust relations in contiguity of peers helps to reduce attacks in a P2P system.

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: a)service and b)recommendation contexts. Information about past interactions and recommendations are stored in separate histories to assess competence and integrity of acquaintances in these contexts.

Trust Model defines three trust metrics.

1.1. REPUTATION METRIC is calculated based on recommendations. It is important when deciding about strangers and new acquaintances. Reputation loses its importance as experience with an acquaintance increases.

1.2. SERVICE TRUST METRIC- The service trust metric is used when selecting service providers.

1.3. RECOMMENDATION TRUST METRIC are primary metrics to measure trustworthiness in the service and recommendation contexts, respectively. The recommendation trust metric is important when requesting recommendations. When calculating the reputation metric, recommendations are evaluated based on the recommendation trust metric.

good peers can defend themselves against malicious peers without having global trust information. SORT's trust metrics let a peer assess trustworthiness of other peers based on local information. Service and recommendation contexts enable better measurement of trustworthiness in providing services and giving recommendations.

II. LITERATURE SURVEY

Generally malicious peers have more attack opportunities in distributed trust models due to lack of a central authority. Researchers are always being conducted to improve the accuracy and efficiency of the trust management in P2P networks. In addressing the above issues, we present a new trust based security model with risk management integration via trust, which repossesses the new feature of utility maximization. A formal trust model based on sociological foundations. A consignee uses own experiences to build trust relations and does not consider information of other consignee. Abdul-rahman and Hailes [12] evaluate trust in a discrete domain as an aggregation of direct experience and recommendations of other parties. They define a semantic distance measure to test accuracy of recommendations. Yu and Singh's model [13] propagates trust information through referral chains. Referrals are primary method of developing trust in others. Mui et al. [14] propose a statistical model based on trust, reputation, and reciprocity concepts. Reputation is propagated through multiple referral chains.

Most existing P2P networks are built on traditional security models, including the two most widely used models the mandatory access control (MAC) and the discretionary access control (DAC)

models [5]. While these models aim at the enforcement of access control of system resources, they are not concerned about the system utility on which they do have a direct impact. This is because malicious behaviors can happen even after the authorization stage [9].

The notion of utility and its application in distributed computing is not new. Marsh introduced the notion of utility as a member of a set of input parameters used for constructing his trust model for distributed systems, where utility was actually used as one of the input parameters for the trust calculation used for cooperation decisions [14]. The notions of utility and trust have also been used by other researchers in security context for grid based computing [13]. However, risk management has not been considered in these Studies. Sonntag. Have proposed a payment based scheme for mobile agent based e-commerce applications.

Yu and Singh's model [13] propagates trust information through referral chains. Referrals are primary method of developing trust in others. Mui et al. [14] propose a statistical model based on trust, reputation, and trade concepts. Reputation is propagated through multiple referral chains. Jøsang et al. [15] discuss that referrals based on indirect trust relations may cause incorrect trust derivation. Thus, trust topologies should be carefully evaluated before propagating trust information. Terzi et al. [16] introduce an algorithm to classify users and assign them roles based on trust relationships. Zhong [17] proposes a dynamic trust concept based on McKnight's social trust model [18]. When building trust relationships, uncertain proofs are evaluated using second-order probability and Dempster-Shaferian framework.

In e-commerce platforms, reputation systems are widely used as a method of building trust, e.g., flipkart, shopclues, Amazon. A central authority collects feedbacks of past customers, which are used by future customers in shopping decisions. Resnick et al. [19] discuss that ensuring long-lived relationships, forcing feedbacks, checking honesty of recommendations are some difficulties in reputation systems.

III. PROPOSED SYSTEM

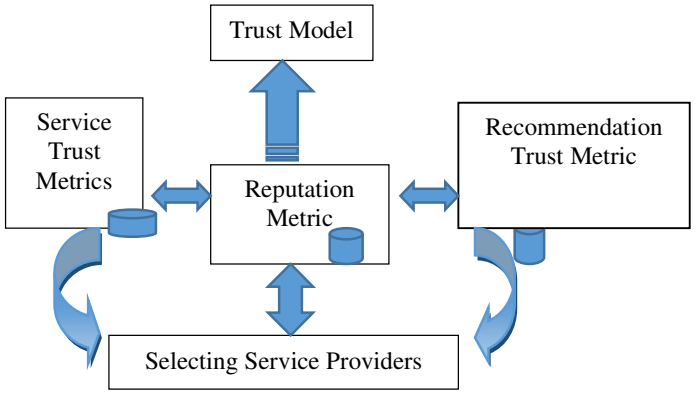

Fig.1. Operations in Proposed System with the Help of peer-to-peer network

We define secure routing and outline our solution. Throughout this paper, most of the analyses and techniques are presented in terms of this model and should apply to other structured overlays except when otherwise noted. We define an abstract model of a structured Distributed routing overlay, designed to capture the key concepts common to overlays such as CAN, Chord, Tapestry and Pastry. The protocol routes messages with a given key to its associated root. To route messages efficiently, all nodes maintain a routing table with the node IDs of several other nodes and their associated IP addresses. Moreover, each node maintains a neighbor set, consisting of some number of nodes with node IDs nearest itself in the id space. Pastry node IDs are assigned randomly with uniform distribution from a circular 128-bit id space. Given a 128-bit key, Pastry routes an associated message toward the live node whose node ID is numerically closest to the key. Each

Pastry node keeps track of its neighbor set and notifies applications of changes in the set. Secure routing ensures that (1) the message is eventually delivered, scorn nodes that may corrupt, drop or misroute the message; and (2) the message is delivered to all legitimate replica roots for the key, despite nodes that may attempt to impersonate a replica root. Secure routing can be combined with existing security techniques to safely maintain state in a structured Distributed overlay. For instance, self-certifying data can be stored on the replica roots, or a Byzantine-fault-tolerant replication algorithm [10] can be used to maintain the replicated state. Secure routing guarantees that the replicas are initially placed on suitable replica roots, and that a lookup message reaches a replica if one exists. Similarly, secure routing can be used to build other secure services, such as maintaining file metadata and user quotas in a distributed storage utility.

IV. ADVANTAGES OF PROPOSED SYSTEM

4.1 Limited Cost

The implementation of our reputation service required certain amount of resources, in terms of both storage capacity and bandwidth, but this cost is limited and justified in most situations. The amount of storage capacity is proportional to the number of servants with which the servant has interacted.

4.2 Reliability

This performance metric is used to evaluate the ability of the peer-to-peer network to handle errors. Use the number of retransmissions to characterize this ability. A peer-to-peer network with higher reliability will have a smaller number of retransmissions, and thus higher throughput. The redundant links can greatly improve the reliability of the peer-to-peer network with little overhead.

4.3 Concentration of servents

Servants will have a high probability of exhibiting a sufficient number of votes supporting their reputation in the portion of network that a node in a particular instant sees only if they have a considerably greater number of votes globally.

4.4 Overload avoidance

Our Reputation service presents a considerable risk of focusing transfer request on the servant that have a good reputation, reducing the degree of network availability.

4.5 Integration with intermediate P2P solutions

Intermediate P2P solutions(like fastTrack nodes) identity nodes of the network characterized by an sufficient amount of CPU power and network bandwidth,assigning to them the role of indexing what is offered on the network.

V. APPLICATION AND USES

Using trust information does not solve all security problems in P2P Network but can enhance security and effectiveness of systems. If interactions are modeled correctly, Trust Model 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

VI. CONCLUSION

A trust model for P2P networks is presented, in which a peer can develop a trust network in its contiguity. 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

REFERENCES

[1] A.B.Can and B.Bhargava,"SORT: Self ORganizing Trust Model for Peer-to-Peer Systems," IEEE Transactions on Dependable and Secure Computing,vol.10,no.1,pp.14-27,Jan.2013
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] R. Zhou, K. Hwang, and M. Cai, "Gossip trust for Fast Reputation Aggregation in Peer-to-Peer Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.
[8] J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp. Theory of Computing, 2000.
[9] S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proc. Multimedia Computing and Networking, 2002.
[10] 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.
[11] S. Marsh, "Formalising Trust as a Computational Concept," PhD thesis, Dept. of Math. and Computer Science, Univ. of Stirling, 1994.
[12] S. Saroiu, K. Gummadi, R. Dunn, S.D. Gribble, and H.M. Levy, "An Analysis of Internet Content Delivery Systems," Proc. Fifth USENIX Symp. Operating Systems Design and Implementation (OSDI), 2002.
[13] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. 33rd Hawaii Int'l Conf. System Sciences (HICSS), 2000.
[14] B. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000.
[15] L. Mui, M. Mohtashemi, and A. Halberstadt, "A Computational Model of Trust and Reputation for E-Businesses," Proc. 35th Hawaii Int'l Conf. System Sciences (HICSS), 2002.
[16] A. Jøsang, E. Gray, and M. Kinateder, "Analysing Topologies of Transitive Trust," Proc. First Int'l Workshop Formal Aspects in Security and Trust (FAST), 2003.
[17] E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, "An Algorithm for Building User-Role Profiles in a Trust Environment," Proc. Fourth Int'l Conf. Data Warehousing and Knowledge Discovery (DaWaK), vol. 2454, 2002.
[18] Y. Zhong, "Formalization of Dynamic Trust and Uncertain Evidence for User Authorization," PhD thesis, Dept. of Computer Science, Purdue Univ., 2004.
[19] D.H. McKnight, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2001.
[20] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation Systems," Comm. ACM, vol. 43, no. 12, pp. 45-48, 2000.
[21] Z. Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc. First Int'l Conf. Agents and Peer-to-Peer Computing, 2002.
[22] A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.
[23] C. Dellarocas, "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior," Proc. Second ACM Conf. Electronic Commerce (EC), 2000.
[24] B. Yu and M.P. Singh, "Detecting Deception in Reputation Management," Proc. Second Int'l Joint Conf. Autonomous Agents and Multiagent Systems, 2003.
[25] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of Trust and Distrust," Proc. 13th Int'l Conf. World Wide Web (WWW), 2004.
[26] J. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to Peer Systems (IPTPS), 2002.