ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Ensuring Secure and Timely Availability of Reputation Data in Peer To Peer Networks

S.Saranya[1], K.Kiruthika Devi[2]

P.G Scholar, Department of Computer Science and Engineering, Nandha College of Technology, Erode, Tamilnadu.

Assistant Professor, Department of Computer Science and Engineering, Nandha College of Technology, Erode, Tamilnadu.

***Abstract*- Peer to peer network is decentralized and distributed network, which is useful for file sharing via internet. Due to malicious activity, still it is insecure during file sharing. Depending on the past interaction and their recommendation, trustworthiness of a peer can be build. In order to measure the trustworthiness, two constraints are considered namely, services and recommendations. According to the recentness and peer satisfaction, both service and recommendations can be evaluated. While calculating these recommendations, we consider the trustworthiness of the recommender and confidence about a recommendation. Good peers can form the trust relationship by isolating the malicious peers. In this proposed model we provide cryptography provenance verification method for secure transmission of data and data auditing is performed for eliminate the malicious packets.**

Index Terms-Peer to Peer, Reputation, Trust management, security.

I INTRODUCTION

In Peer to Peer system, peers are connected via internet for file sharing without need of central control. Peer can act as both client and server. Each peer can request and each peer can response according to the request. In existing the central server is used to store the trusted information. Every client should request to central server for the trust information .example for central server is eBay. Since there is no need of the central server, the peer can organize themselves and stored the trusted Information. There are two types of peer to peer networks, structured peer to peer network and unstructured peer to peer where the file is searching from and where the files are stored. The Structured peer to peer networks use the Distributed Hash Table (DHT). Chord and tapestry are structured peer to peer system and it is sensitive to join/ leave/failure of peer behavior. In unstructured peer to peer network the peer knows about neighborhood peer. Gnutella and Limeware are example of unstructured peer to peer system which has high tolerant level with respect to peer failure.

In unstructured networks, there is no relationship between the source with other peers, except neighbor peer and its location. As the route has been established in the structured peer to peer system, there is no security issue. In unstructured Peer to Peer system, the peer is not aware of the file location. Due to this, security is lacking. To overcome this problem, SORT-Self Organizing Trust Model has been introduced. This model provides self certification and peer has been organize themselves for trustworthiness. And cryptography verification approach has been used for secure transaction.

This paper organized as follows. Section II describes about some existing approaches. Section III describes cryptography provenance method. Section IV describes about proposed solution. Section V describes about conclusion and future work.

II BACK GROUND AND RELATED WORK

Aberer and Despotovi (2001) proposed to address the problem of reputation trust management at both semantic level and data management level [9].provide decentralized and access the trusted information efficiently. The advantage of this proposal is by implementing this method in peer to peer environment, it scales well for huge participants in the network. The main drawback is communication cost is high.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Jøsang et al (2007) indicates that the trust and reputation system are vulnerable [7]. The basic idea of this paper is after completion of transaction the feedback ratings is evaluated. Based on that evaluation the peer can decided about the further transactions. The advantages of this paper are accuracy is maintained for long term performance and robustness. Drawback is when designing the new system, several constraints are taken into consideration.

Dellarocas (2000) proposed to encourage the trustworthiness during transactions by using the past behavior [5].Two mechanism had been proposed namely cluster filtering and controlled anonymity. By combining the both mechanism it provides the powerful technique which overcome the problem of unfair high and low ratings and discriminatory seller behavior. The advantages are it reduces the negative effects. It protects the online reputation system from malicious buyer and seller. Drawbacks are it does not involve complete evaluation.

Self Organizing Trust Model (SORT) is used to minimize the malicious activity in Peer to peer system [2]. This can be done by establishing trust relations among the peer. Here peer will not collect the trust information from all peers. Based on past interaction peer can develops their own local view. By this way peers can eliminate the illegitimate peers and good peers forms the dynamic trust group [6]. In Self Organizing Trust Model, at beginning the peers are considered to be stranger to each other. Then the peer should acquaintance of other peer by providing the services. By using the peer's service (called interaction) which can be calculated based on importance, past interactions and satisfaction. An acquaintance's feedback (called recommendation) which can be calculated based on confidence. level and recommender's acquaintance. A peer may be bad service provider but good recommender or vice versa. Based on the three metrics SORT can be defined [7]. The three metrics are Reputation metrics, service trust and recommendation trust. The reputation metric can be evaluated based on recommendation. It is used for deciding the stranger and new acquaintance. Services and recommendations are used to measure the trustworthiness. Service trust metric are used while prefer the service provider. Recommendation trust metrics plays an important role while requesting recommendation.

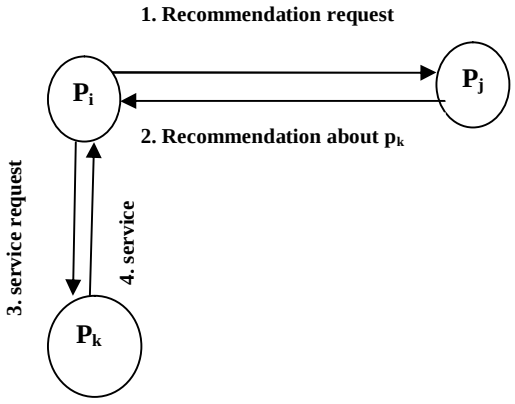

Fig 1 Receive the recommendation and interacted with each other

III CONSTRUCTION FOR PROPOSED SCEHME

To avoid malicious packets, the SORT and cryptography provenance verification method with data auditing under training set is done. The data auditing has been performed by using Bayesian classifier. By using these above techniques we perform the secure transmission without any malicious activity.

Cryptography provenance method as robust mechanism that ensures true origin of the data produced by an entity such as a system stored data [3][4]. Therefore, we aim to detect the two specific behaviors (traffic-checkpoint bypassing and fake data injection) under the assumption that our detection system is not compromised at the run time. Three operations are defined for data-provenance verification which are setup, sign, and verify.

- *Setup:* The data producer(sender) which is generate signing key k and the data consumer(receiver) which is generate verification key k' for the secure purpose which can prevent the malware from accessing the keys.
- *Sign (d, k):* The sender sign data d with a secret key k, and then the output is d along with its proof sig.
- *Verify (sig, d, and k'):* The sender uses key k' to verify the signature sign of received data and data is rejected if the verification fails [5].

The important participation of proposed model is

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

1. A self-certification-based identity system protected by cryptographically blind identity mechanisms.

2. A light weight and simple reputation model.

3. An attack resistant cryptographic protocol for generation of authentic global reputation information of a peer.

In addition SORT, peers send reputation queries only to peers interacted in the past using DHT, which reduces network traffic comparing to flooding-based approaches.

Bayesian Probability Technique is used for data auditing and this can be done by using several steps which are Preparation of Testing/classifying Set, .Preprocessing, Generating word list, Generating word maps, Classifying an file.

IV PROPOSED SCEHME

The proposed scheme involves forming the unstructured network and file has been searched based on Distributed Hash Table(DHT).then asymmetric cryptography approach is used for the cryptography verification method .Digital signature is generated at both sender and receiver side to prevent the occurrences of falsy data injection. And finally data auditing is done to drop the malicious packets.

a. Distributed Hash Table

Since unstructured network is dynamic, any number of peers can be joining or may leave from the network. Such networks can be easily constructed as a new peer that wants to join the network can copy already existing links of another node and then form its own links. In an unstructured Peer to Peer network, if a peer wants to find a desired piece of data in the network, the query should flooded through the network for sharing the file to find as many peers as possible that share the data[8]. Each peer known only their neighbor peer that's represents unstructured Peer to Peer network. In the unstructured Peer to Peer networks, interested peers share the content they have and forward the queries plays an important role during the content search process. Each and every peer in the network must maintain this table which is used to forward the peer request to the apt peer instead of its neighbor peer. The proposed system uses the distributed hash table where each and every peer has the separate hash table.

The information stored in the hash table is based on Reputation management (tracking peers past activity).It helps to perform the file searching operation efficiently. The self certificate is used for ensuring secure and timely availability of the reputation data of a peer to other peers. For reliable and elective reputations, each peer stores its own reputation locally; they have to be updated and stored securely to prevent malicious peers from the reputation system.

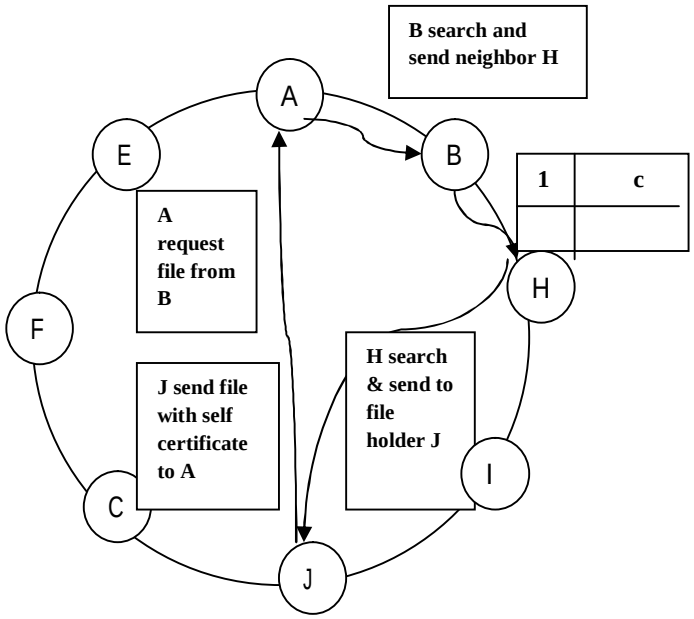

Fig 2 Communication in P2P networks with self certification

b. Asymmetric cryptography approach

Peers generate universally unique identifications locally and store them along with their public key, their current IP address. Implementation of Self Certification and Digital Signature for Secure Communication is focused in this module. RSA is used to generate public key and for data encryption and decryption. MD5 is used to generate the digital signature on the basis of encrypted file.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

C.Digital signature matching system

Each and every peer has the unique identity, based on this, the peer is identified and the transaction is begined. The certification is attached with identity of the peer [3]. The certification uses the concept of RSA and DS. Where the algorithm generates the private key and public key, these identities are attached with reputation of the given peer. The sender sends the information which is associated with its private key and signature, at receiver side receives the file and generates the signature, it will be matched with the attached signature if true conclude no more presence of malicious peer else proceed next module steps[7].

D. Data auditing under training sets

Each receiver maintains trained data sets which are used whether signature verification fails. Each content or word must be compared with trained data set and find the similarity if the similarity is much more then it concludes the content must be malicious to the peer so on the attack basis it just warns the peer else the file will be received successfully and safe.

Bayesian Probability Technique

Each receiver maintains trained data sets which are used whether signature verification fails [10]. Each content or word must be compared with trained data set and find the similarity if the similarity is much more then it concludes the content must be malicious to the peer so on the attack basis it just warns the peer else the file will be received successfully and safe.

i.Preparation of Testing/classifying Set

All received files in the testing set are pre classified based on the user requirements .After the data classification, resulting data are mixed together to form as a set**.**

ii.Preprocessing

All the words in the above classifying set are preprocessed as separate words in the trained file

iii.Generating word list

A tokenizer is used to organize the file contents into word lists. A stop word list is needed to remove the unwanted words(which is called stop words) from word lists.

iv.Generating word maps

A word map is a list of words that appear both in a given. One word map contains words that appear in the received file. Another word map contains words that appear in the unwanted Vocabulary table. These two word maps can be different from each other since some words appear in unwanted files may not appear in ordinary files according to the training set

v. Classifying an file

And finally, According to the word maps, probabilities of *W* word map to determine if a word is an unwanted word.

VI .CONCLUSION AND FUTURE WORK

The proposal model presents self-certification, reputation model, an identity management mechanism, and a cryptographic protocol that ensures the generation of global reputation data in a P2P network, in order to rapid detection of attacks. A reputation system for peer-to-peer networks can be thwarted by a group of malicious nodes. Such a group may maliciously raise the reputation of one or more peer of the group. The global reputation data are protected against any malicious modification by the third party peer and are immune to any malicious modifications by their owner. By using the self certification and cryptography provenance verification reduces the number of malicious transactions and less consumption of bandwidth per transaction than the other reputation systems proposed in its category. Presented an unstructured P2P network with rigorous performance guarantees to enhance search efficiency, effectiveness and trustworthiness. It also handles the problem of highly erratic availability pattern of the peers in P2P networks.

In Peer to Peer network, the peers which are participating in the network are miscellaneous with storage space, network bandwidth and computational capability. It will be quite interesting for our future work to investigate how miscellaneous affects our proposal.

REFERENCES

[1] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1:1-1:31, 2009.

[2] Ahmet Burak Can and Bharat Bhargava,"SORT-Self Organizing Trust Model", IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 1, January/February 2013.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

[3] Kui Xu, Huijun Xiong, Chehai Wu and Deian Stefan," Data-Provenance Verification For Secure Hosts," IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, March/April 2012.

[4] A. A. Selcuk, E. Uzun, and M. R. Pariente, "A reputation-based trust management system for p2p networks," in *Proceediizgs of the 4th IEEE/ACM I~ztenzatio~zaSly ~nposiumo n Cluster Conzputing and the Grid (CCGRID)*, 2004.

[5] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in Proceedings of tlze 2ndACM colzference on Electl-onic comlnerce (EC),2000.

[6] A.B. Can, "Trust and Anonymity in Peer-to-Peer Systems," PhD thesis, Dept. of Computer Science, Purdue Univ., 2007.

[7] 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.

[8] R. Zhou and K. Hwang, "Power trust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473,Apr. 2007.

[9] K. Aberer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in Proceedings of the IOtlz ir7terlzarional colzference on I~zfonnation and knowledge ma~zagenient (CIKM),2001.

[10] Y. Wang and J. Vassileva, "Bayesian Network Trust Model in Peer-to-Peer Networks," Proc. Second Workshop Agents and Peer-to-Peer Computing at the Autonomous Agents and Multi Agent SystemsConf. (AAMAS), 2003.

[11] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-Resilient Online Content Voting," Proc. Sixth USENIX Symp. Networked Systems Design and Implementation (NSDI), 2009.

[12] A. Habib, D. Xu, M. Atallah, B. Bhargava, and J. Chuang, "A Tree-Based Forward Digest Protocol to Verify Data Integrity in Distributed Media Streaming," IEEE Trans. Knowledge and Data Eng., vol. 17, no. 7, pp. 1010-1014, July 2005.

[13] 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.

[14] K. Aberer, A. Datta, and M. Hauswirth, "P-Grid: Dynamics of Self-Organization Processes in Structured P2P Systems," Peer-to-Peer Systems and Applications, vol. 3845, 2005.

[15] B. Yu, M.P. Singh, and K. Sycara, "Developing Trust in Large-Scale Peer-to-Peer Systems," Proc. IEEE First Symp. Multi-Agent Security and Survivability, 2004.