http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (5): 613-619, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.613.619
© 2012 Asian Network for Scientific Information

An Anonymous Authentication Scheme Based on Fully Homomorphic Encryption in P2P Networks

[1,2]Xiaoliang Wang, [3]Yuling Liu and [4]Hengfu Yang
[1]College of Information Engineering, Xiangtan University, Xiangtan, 411105, China
[2]School of Computer Science and Engineering,
Hunan University of Science and Technology, Xiangtan, 411201, China
[3]College of Information Science and Engineering, Hunan University, Changsha, 410082, China
[4]Department of Information Science and Engineering, Hunan First Normal University,
Changsha, 410205, China

Abstract: In P2P network, the existing researches focus on protecting the security of information transmission, or ensuring users' privacy. Security certification is a basic demand of P2P network, including the general authenticity, credibility, integrity and so on. Privacy protection for transactions is the high-level requirement of security, including confidentiality, copyright management, access control. One-sided pursuit of certification will affect the privacy rights of users while one-sided pursuit of anonymous will bring a series of anonymous abuse problems. However, little research has paid attention to urgency of this dilemma, leading to the emergence of a large number of problems in the applications. This study presents an anonymous authentication scheme based on homomorphic encryption, called FHET (Fully homomorphic encryption trust). FHET makes use of trust certificates and can also be combined with existing P2P reputation system which effectively prevents the selfish behavior of peers and ensures scalability, portability and practicality.

Key words: P2P, anonymity, authentication, traceability, homomorphic encryption

INTRODUCTION

Privacy is a fundamental right of citizens so that the anonymity has an extensive applications in present society (Liu, 2012; Shao *et al.*, 2008; Zaidan *et al.*, 2011). P2P software has become one of the most popular applications (Jiang *et al.*, 2009; Peng and Zheng, 2010; Xie *et al.*, 2009; Ye *et al.*, 2011) but the open environment of P2P communication and resource sharing also brings users more privacy concerns (Chen *et al.*, 2011; Modarresi *et al.*, 2008, 2009). For this concern, many researchers have studied anonymous mechanisms of P2P networks and achieved great successes (Freedman and Morris, 2002; Goldschlag *et al.*, 1999; Rennhard and Plattner, 2002).

How to design a secure authentication mechanism for P2P networks is also a research hotspot (Mekki and Fezza, 2009). In order to ensure an available response from resource owners, a lot of trust model (Damiani *et al.*, 2002; Kamvar *et al.*, 2003; Xiong and Liu, 2004) come into being. The trust model can effectively verify the identity of unknown peers. However, these identity-based trust models are based on a particular assumption: a peer must know the real identities of partner peers. This restriction leads to a dilemma that between trust mechanism and anonymous mechanism seems to exist contradictory.

So far, FBST (Wang and Sun, 2009) and CST (Wang *et al.*, 2010b) schemes are based on credential-based trust systems and can not fully integrate the existing P2P reputation system. In other words, although these trusts between peers can be built due to other peers' introduction but this certificate does not contain information about the reputation of partner peer which will lead to the system prone to free riders or other selfish behavior. Whether there exists a new anonymous authentication scheme which not only meets the anonymous, security and certification requirements and also compatible with the existing mature P2P reputation mechanisms to limit peers' selfish behavior (Wang *et al.*, 2010a). So in this study, FHET scheme is proposed.

HOMOMORPHIC ENCRYPTION BASED ON ALL ANONYMOUS AUTHENTICATION ALGORITHM

This section describes our anonymous authentication scheme FHET (Fully homomorphic encryption trust). In FHET, the system considers the distributed P2P network environment and uses the

Corresponding Author: Yuling Liu, School of Computer and Communication, Hunan University, Changsha, 410082, China
Tel: 86-731-58293779 Fax: 86-731-58293779

homomorphism of fully homomorphic encryption to ensure anonymity, authentication and traceability features in unstructured P2P networks.

Network structure: FHET scheme applies to super-peer model of unstructured P2P networks like PALMS-SP (Hoong and Matsuo, 2008). Firstly, all peers are divided into logical groups called Autonomous Domains (AD). Each autonomous domain chooses the best performance peer as the super-peer (SP). Other peers in the autonomous domain are called Normal Peers (NP). Super-peer keeps resource information of normal peers. Normal peers rely on super-peer when searching and accessing resource information, then directly contact the resources peers. This super-peer network architecture has many advantages, such as decreasing search time and bandwidth, self-management, load balancing, etc. (Oh *et al*., 2008).

Safe assumption: As the discredited super-peer can not be entrusted under the fully homomorphic encryption, it is necessary to limit the credibility of the super-peer. In this scheme, there is a basic premise that super-peers must meet ''Honest but curious'' assumption.

- **Honest:** Super-peer must be able to faithfully perform all operations of system encryption process and will not deliberately discard packets
- **Curious:** Super-peer may want to peep into the data content, so the whole encryption process should not disclose any plaintext information to super-peer

''Honest but curious'' assumption applies to most situations but not to the weak security case.

Basic algorithm: The specific target of FHET is to protect the peer's identity, data content, privacy rights and trace of anonymous abuse peer, while also addressing the selfish behavior of P2P peers.

Phase 1 Initialization: In this phase, the system uses CDC partition algorithm (Ramaswamy *et al*., 2005) to divide every peer into a certain logical area. This logic area is called Autonomous Domain (AD). In every AD, system uses SOBIE (Liu *et al*., 2008) algorithm to select the best peer as the super-peer (SP). We assume in initialization phase the system is in the relative safety state.

In this phase, each super-peer uses integer-based homomorphic encryption (Van-Dijk *et al*., 2010) to generate a private key. This generation is as follows. Suppose super-peer of autonomous domain B is SP_B. SP_B selects an odd p as the his private key of homomorphic encryption, called sk_B. p is a binary sequence of length η, its value is odd. That is to say:

$$p \xleftarrow{\$} (2\mathbb{Z}+1)\cap[2^{\eta-1},2^{\eta})$$

Then system uses SO_B to generate the public key of homomorphic encryption in autonomous domain B, called pk_B. Detailed steps are as follows. According to the η bit odd p, SP_B designs the following function:

$$\Psi_{\gamma,\rho}(p)=\{\text{choose}\quad q \xleftarrow{\$} \mathbb{Z}\cap[0,2^{\gamma}/p),$$
$$r \xleftarrow{\$} \mathbb{Z}\cap[-2^{\rho},2^{\rho}):\ \text{output } x=pq+r\}$$

where, q is a large random integer and r is a small random integer. Notice that r should be very smaller so that it can make $2r+m \ll p$.

Public key pk_B is a sequence of bits, $\text{pk}_B = <x_0, x_1,\ldots, x_\tau$, where each number:

$$x_i \xleftarrow{\$} \Psi_{\gamma,\rho}(p),\ i=1,2,\ldots,\tau$$

After sorted, x_0 of the sequence is the largest number and also an odd, while $r_p\ (x_0)$ is an even. If selected number does not meet the above restriction, system continues to re-select it until x_0 is eligible to this requirement.

After this, every super-peer mutually exchange and store each other's public key of homomorphic encryption.

In addition, the normal peers within the same autonomous domain use anonymous multicast way to send their own identity information to local super-peer.

Phase 2 Resource index stored by the fully homomorphic encryption: Like general super-peer mode, the super-peer in FHET will collect the list of resources of each local peer and form the resource index for the retrieval operation. This mode will transfer calculation and resource research overload from normal peers to super-peers which reduces the burden of normal peers. However, this super-peer mode also brings some security risks: calculation process and resource index will disclose the peer privacy. Therefore, taking data privacy into account, the local normal peers upload their own resource indexes using fully homomorphic encryption. Suppose a normal peer, called u in autonomous domain A. Like initialization phase, u generates its public/private key pair pk_u and sk_u and then uses fully homomorphic encryption algorithm to encrypt resource index. Finally u anonymously sends encrypted index and public key pk_u to the local super-peer by multicast. The detailed homomorphic encryption algorithm will be introduced in the next section. As a result of multicast and homomorphic encryption process, although in the previous stage SP_A has stored all the peers identities but in the process of resource index phase it does not know the real identity of u and resource index content so that privacy of data and u have been protected. After SP_A has collected those related information, it will save the them and put pk_u into the local public key set.

Phase 3 Anonymously research and download of resources: At the beginning of system, the search and exchange of peer resources are limited between the neighbor peers. All neighbor peers record others' reputation value according to every transaction and exchange each others' public key homomorphic encryption. Only after good reputation is built, a peer can search and exchange resource within non-neighbor peers. It must notice that P2P anonymous schemes are considered in the non-neighbor peers situation. Regardless of which mode adopted by anonymous P2P networks, previous peer's IP address is always known to successor peer, so the most of anonymous P2P schemes only consider multi-hop anonymity rather than adjacent neighbor peers' anonymity. We also follow the rule.

When a normal peer u needs to publish its query message within non-neighbor peers, it sends the query to SP_A by multicast, attaching its own public key pk_u and resource query q_u. Because of anonymity of multicast, SP_A does not know the real identity of u. Once receiving local multicast of u, SP_A verifies it with the public key encryption and judges whether u is in the local domain. This process relies on public key set which has already been uploaded by the resource peer in the phase 2. In other words, SP_A verifies whether pk_u is in the public key set. If not, it returns the non-accepting response to u. The aim is to prompt local peers to choose sharing resources instead of selfish behavior. If successful, it proved that this is a query from the local peer, so SP_A accepts the query of u and starts to look for related resource. There are two cases: local search and cross-domain search.

Local search: Firstly, SP_A searches resource in local domain. In this phase, it uses traditional Gerard vector space model (Salton *et al*., 1975) of information retrieval to express the query and computes similarity of query and local resource index. The process is as follows: SP_A changes this query into segmentations and stem of the word and obtains plaintext sequence of keywords and then uses different users' public key to encrypt those sequences respectively. Weight vector of keywords is used to represent resource. This weight is obtained by traditional information retrieval methods which is the normalized form of word frequency multiplied by logarithmic of inverted document frequency. By the use of encrypted word frequency and inverted document frequency, SP_A can get resource weight and then utilizes it to determine whether the required resource is in the local domain. For SP_A has stored resource indexes of local normal peers, it can judge whether the resource is kept in the local area. If the resource is locally stored, the query will be sent to the resource peer by multicast. Then the resource peer also uses the multicast to send resources within the domain to let u receive resources anonymously.

Cross-domain search: If the resource is external, SP_A signs the query and forward it to the neighboring autonomous domain.

If the query with signature passed by partner super-peer SP_B, SP_B broadcasts this query in his local domain. If not, SP_B also forwards the query to the next super-peer until query reaches the autonomous domain where the resource exists.

Suppose a peer in domain B, called v, has required resources. SP_B informs SP_A and asks SP_A a recommended credibility value of u as the trust certificate. Every domain has its own reputation threshold. We assume the reputation threshold of domain B is $Threshhold_B$, so if only the recommended credibility value of u exceeds $Threshhold_B$, the query of u can be met.

The generation process of trust certificate is shown in Fig. 1. To protect peer privacy, the generation of recommended credibility values uses fully homomorphic encryption. Owing to public key exchange of super-peers in the initialization phase, SP_A can publicly broadcast pk_B of SP_B and pk_u of u within the local autonomous domain and requires the neighbor peers of u to provide the recommended values of u.

Each peer checks received pk_u in its the neighbor public key set and if it find u is its neighbor peer, it will serve as a referee peer for recommended credibility values of u, called Referee Peer (RP).

Let's assume that a referee peer is called RP_i, $1 \le i \le k$. According to every historical transaction record of u, RP_i will compute a score for u within a certain range of integers. Finally, RP_i summarizes all the scores to calculate a mean value as recommended credibility value of u. The detailed process is as follows. rec_{RP_i} donates recommended credibility value of u. RP_i makes binary serialization of rec_{RP_i} , in which each bit uses the following full homomorphic encryption algorithm. RP_i chooses a random subset $S \subseteq \{2, \ldots, \tau\}$ and a random integer r within the range of -2^{ρ}, 2^{ρ}. Then a homomorphic encryption bit of recommended values is obtained:

$$c_{RP_i} \longleftarrow [rec_{RP_i} + 2r + 2\sum_{i \in S} x_i]_{x_0}$$

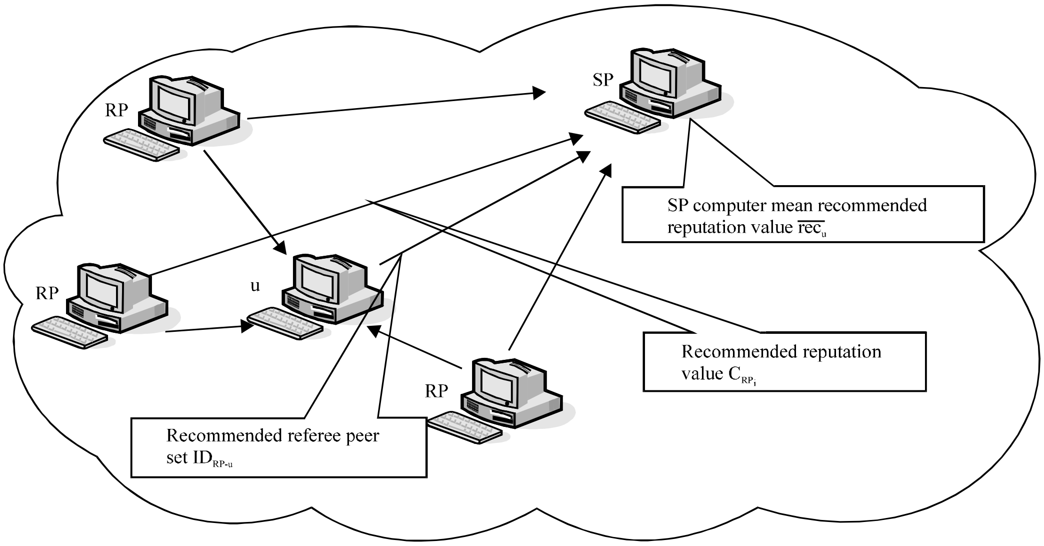
RP
SP
SP computer mean recommended reputation value $\overline{rec_u}$
RP
u
Recommended reputation value C_{RP_i}
RP
Recommended referee peer set ID_{RP-u}

Fig. 1: Trust certificate generation process

Similarly, RP_i can complete every bit of the recommended values and attain encrypted recommended values. Then, RP_i uses public key pk_B of SP_B to encrypt its own identity and obtains ID_{RP_i}. Finally, RP_i sends C_{RP_i} to SP_A as well as sending ID_{RP_i} to u. Here FHET simplifies the calculation of recommended value. But after the existing mature P2P reputation algorithms are improved, they can be also applied to FHET.

To get k neighbors' recommended credibility values, SP_A makes use of additive homomorphism of encryption to get the total reputation value of u:

$$rec_u = \sum_{i=1}^{k} (C_{RP_i}) = E\,(\sum_{i=1}^{n} rec_{RP_i})$$

where, k is the number of neighbor peers. Then SP_A uses multiplication to get all the mean reputation value:

$$\overline{rec_u} = \frac{1}{k} rec_u = \frac{1}{k} \sum_{i=1}^{k} (C_{RP_i}) = E\,(\frac{1}{k}\,(\sum_{i=1}^{n} rec_{RP_i}))$$

Owing to homomorphic encryption, although, SP_A does not know the private key of SP_B and can not decrypt recommended credibility values of u, it also summarizes recommended credibility values of u.

After u has obtained referee ID s from enough referee peers, it adopts fully homomorphic encryption to deal with ID s and obtains referee peers' identities set:

$$ID_{RP-u} = \prod_{i=1}^{k} (ID_{RP_i})$$

where, k is the number of neighbor peers. Then u sends ID_{RP-u} and pk_u to SP_A by multicast.

After these processes, SP_A owns a mean recommended credibility value of u, donated as $\overline{rec_u}$ and referee identities set ID_{RP-u}. Since it does not know the private key of SP_B, it do not know the credibility value of u as well as the referee identities, so that privacy of peers is protected. But SP_A meets the ''Honest but curious'' assumption, so SP_A will create a trust certificate of u so as to recommend u to SP_B. SP_A builds a triple including $\overline{rec_u}$, ID_{RP-u} and query q_u signed by its own private key signature.

The process of cross-domain anonymous access is shown in Fig. 2. If the required resource is in the foreign domain, SP_A will use Onion Routing approach (Goldschlag *et al.*, 1999) to contact super-peer SP_B attaching the above signed triple. After SP_B receives the signed triple, it verifies the signature and decrypts $\overline{rec_u}$ and then check whether it is greater than $Threshhold_B$. If successful, from the local public set SP_B finds the public key of u, then encrypts query q_u and multicasts it in the local domain.

Phase 4 Resources access: Upon v receives the encrypted query of u from the local super-peer SP_B. v checks whether the query resource is own resource. If not, it shows that resource has been updated and v informs SP_B. SP_B adjusts the related index stored in its catalogs and re-forward the query.

If v has the required resources, v sends resource to SP_A via onion routing. Finally, SP_A multicasts it in local domain to allow u to anonymously access this resource.

Phase 5 The discovery of malicious peers: In FHET scheme, if anonymous abuse exists, we assume the malicious peer is u, u attacks v by anonymous mechanism.

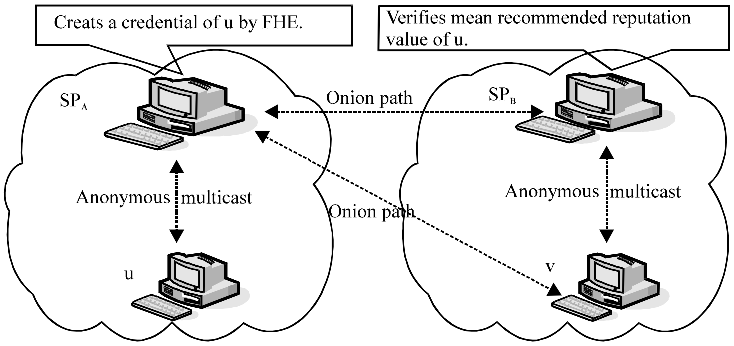
Creats a credential of u by FHE.
Verifies mean recommended reputation value of u.
SP$_A$
SP$_B$
Onion path
Onion path
Anonymous multicast
Anonymous multicast
u
v

Fig. 2: Anonymous Access Cross-domain

In this case, v will apply to SP$_B$. SP$_B$ contacts SP$_A$ and sends the ID$_{RP-u}$ of u to SP$_A$. Since the number of peers in a domain is not large and in the initialization phase all the peers identities already have stored in super-peer, so SP$_A$ can use exhaustive method to find out the identities of referee peers recommending u. After this, SP$_A$ can cooperate with those RPs and link this malicious transaction with u so that malicious peer is tracked. It should be noticed that the exhaustive method owns high computational complexity to ensure the trace mechanism will not be abused in the general case.

ALGORITHM ANALYSIS

- **Authentication security analysis:** Since recommended values and referee peers identities are included in packet encrypted by full homomorphic encryption, the authentication mechanism is ensured. The ability of authentication depends on the security of the full homomorphic encryption algorithm used in the FHET. Because of space constraint, this section simplifies the formal homomorphism proof of the above algorithm. Some parameters restrictions and strict proof are in the reference (Van-Dijk *et al*., 2010). We assume there are two plaintext bits, m$_1$ and m$_2$. After the homomorphic encryption algorithm is done, $c_1 = q_1p+2r_1+m_1$, $c_2 = q_2p+2r_2+m_2$. For addition operation, there is $c_1+c_2 = (q_1+q_2)p+2(r_1+r_2)+(m_1+m_2)$. By the selection of parameters, we can make $2(r_1+r_2)+(m_1+m_2)$ much smaller than p, so we can get $c_1+c_2 \bmod p = 2(r_1+r_2)+(m_1+m_2)$, which proves that this algorithm is additive homomorphism. For multiplication operation, $c_1\times c_2 = (c_1q_1+q_1c_2+q_1q_2)p +2(2\ r_1r_2+r_1m_2+m_1r_2)+m_1m_2$. Also by the selection of paranieters, we can make $2(2\ r_1r_2+r_1m_2+m_1r_2)+m_1m_2$ much smaller than p, so we can get $c_1\times c_2 \bmod p = 2(r_1r_2+r_1m_2+m_1r_2)+m_1m_2$, which proves that this algorithm is multiplication homomorphism. Moreover, after SP$_B$ obtains triple, the reputation of u can be verified. Finally, the signature of SP$_A$ provides the proof for the credibility value of u and other peers can verify this signature. In fact, recommended credibility value of u provides u an access to external resources
- **Anonymity and privacy:** In FHET, u uses pk$_u$ as public key of full homomorphic algorithm to encrypt all the resources of its, while anonymously multicasting them to the local super-peer SP$_A$ which makes the external peers not directly know the detailed index content so as to protect the privacy of remote storage

When communicating with non-neighbor peers, normal peer u sends query to SP$_A$ by multicast. Because of anonymity of the multicast, SP$_A$ does not know the real identity of the partner peer and the privacy of the anonymous peer is protected. On the other hand, because that summation of the credibility value is used by full homomorphic algorithm, although, SP$_A$ can obtain average recommendation credibility $\overline{rec_u}$ and referee identities set:

$$ID_{RP-u} = \prod_{i=1}^{k}(ID_{RP_i})$$

it still can not know the detailed content and confidentiality of credibility value is protected. The reason is as follows. If a certain peer wants to peek into encrypted credibility value of u, it must deduce private key of u from its public key. The complexity of cracking encryption is equal to attacking approximate integer gcd which is difficulty (Van-Dijk *et al*., 2010).

For the different super-peer SP$_B$, it can not deduce the referee identities from encrypted credibility value of u without collaboration of SP$_A$, which play a very good privacy protection for referee peers.

For the Man-in-the-Middle attacker, the transmission of information in the transaction process uses multicast or onion routing, so they can not break communication anonymity of transaction.

Finally, v communicates with SP_B by multicast so that SP_B who owns public key of v can not link resources with the identity of v.

- **Traceability analysis:** In FHET, if anonymous abuse happens, v will apply to SP_B. Then SP_B contacts SP_A and with the help of the public key they can cooperate to track the malicious peer. This is because pk_u exists in the generation of credibility value and anonymity is limited in the transaction. If malicious attack appears, the credibility value can be used to track the real identity of u
- **Prevent selfish behavior of peer:** In FHET, for local search phase, without sharing resource, the public key of u should not exist in public key set of SP_A, so u can not query resources among non-neighboring peers which limits its selfish behavior and encourages it to actively sharing its own resources. For the cross-domain search related to reputation threshold , SP_B needs to verify the credibility value of u which makes u will change selfish behaviors, such as ''reap without sowing" and ''free riders", to actively sharing resources in order to obtain a higher reputation value among neighbor peers.

CONCLUSION AND FUTURE WORK

Since P2P networks need duouble requirements of security and privacy, this study presents an anonymous authentication trust (Fully homomorphic encryption trust, FHET) based on full homomorphic encryption. This proposal improves FBST (Wang and Sun, 2009) and CST (Wang *et al*., 2010b) schemes which are based on credential-based trust systems and can not fully integrate the existing P2P reputation system. It owns much stronger privacy protection for P2P networks users. FHET not only meets the anonymous, security and certification requirements but also is compatible with the existing mature P2P reputation algorithm which can limit the selfish behavior of peers. Therefore, FHET is more scalable and practical.

ACKNOWLEDGMENTS

This study is supported by Natural Science Foundation of Xiangtan University (No. 10XZX16, 11QDZ41), Scientific Research Fund of Hunan Provincial Education Department (No. 11C1215), Scientific Research Fund of Hunan Science and Technology Department (No. 2011GK3205), Hunan Provincial Natural Science Foundation of China (No. 10JJ4041), National Natural Science Foundation of China (No. 61073191, 61103215).

REFERENCES

Chen, H., H. Xu, C. Wang and K. Zhou, 2011. Incentive mechanism for P2P networks based on Markov chain. Infor. Technol. J., 10: 2242-2251.

Damiani, E., S.D.C. di Vimercati, S. Paraboschi, P. Samarati and F. Violante, 2002. A Reputation-Based Approach for Choosing Reliable Resources. In: Association for Computing Machinery, Selcuk, A.A., E. Uzun and M.R. Pariente (Eds.). IEEE Computer Society, Washington, DC., USA, pp: 207-216.

Freedman, M.J. and R. Morris, 2002. Tarzan: A peer-to-peer anonymizing network layer. Proceedings of the 9th ACM Conference on Computer and Communications Security, November 18-22, 2002, Association for Computing Machinery, Washington, DC, USA., pp: 193-206.

Goldschlag, D., M. Reed and P. Syverson, 1999. Onion routing for anonymous and private internet connections. Communications ACM., 42: 39-41.

Hoong, P.K. and H. Matsuo, 2008. Push-pull two-layer super-peer based P2P live media streaming. J. Applied Sci., 8: 585-593.

Jiang, X., S. Jiang and T. Peng, 2009. A multi-channel multimedia content distribution strategy using multiple description coding. Inform. Technol. J., 8: 1084-1093.

Kamvar, S.D., M. T. Schlosser and H. Garcia-Molina, 2003. The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th International Conference on World Wide Web, May 20-24, 2003, ACM Press, New York, USA., pp: 640-651.

Liu, J., Z. Chen, D. Li and H. Liu, 2008. Towards a self-adaptive super-node P2P overlay based on information exchange. Proceedings of the 9th International Conference for Young Computer Scientists, November 18-21, 2008, Zhang Jia Jie, Hunan, China, Inst. of Elec. and Elec. Eng. Computer Society, pp: 410-415.

Liu, J., 2012. Privacy preserving data publishing: Current status and new directions. Inform. Technol. J., 11: 1-8.

Mekki, R. and R. Fezza, 2009. A sample chat application based on JXTA. J. Applied Sci., 9: 3912-3916.

Modarresi, A., A. Mamat, H. Ibrahim and N. Mustapha, 2008. Measuring the performance of peer -to-peer systems with social networks characteristics. J. Applied Sci., 8: 3895-3902.

Modarresi, A., A. Mamat, H. Ibrahim and N. Mustapha, 2009. Modeling and simulating semantic social overlay peer-to-peer systems. J. Applied Sci., 9: 3547-3554.

Oh, B.T., S.B. Lee and H.J. Park, 2008. A peer mutual authentication method on super peer based peer-to-peer network. Proceedings of the International Symposium on Consumer Electronics, April 14-16, 2008, Institute of Electrical and Electronics Engineers Inc., Vilamoura, Portugal, pp: 487-490.

Peng, T. and Q. Zheng, 2010. Resource occupation of peer-to-peer multicasting. Inform. Technol. J., 9: 438-445.

Ramaswamy, L., B. Gedik and L. Liu, 2005. A distributed approach to node clustering in decentralized peer-to-peer networks. Proc. IEEE Transactions Parallel Distributed Systems, 16: 814-829.

Rennhard, M. and B. Plattner, 2002. Introducing MorphMix: Peer-to-peer based anonymous internet usage with collusion detection. Proceedings of the ACM Conference on Computer and Communications Security, November 21, 2002, Association for Computing Machinery, Washington, DC., USA., pp: 91-102.

Salton, G., A. Wong and C.S. Yang, 1975. A vector space model for information retrieval. Commun. ACM. 13: 613-620.

Shao, F., H. Duan, G. He and X. Zhang, 2008. A unified model for privacy-preserving support vector machines on horizontally and vertically partitioned data. Inform. Technol. J., 7: 850-858.

Van-Dijk, M., C. Gentry, S. Halevi and V. Vaikuntanathan, 2010. Fully Homomorphic Encryption Over the Integers. In: Lecture Notes in Computer Science, Rabin, T. (Ed.). Springer Verlag, France, PP: 24-43.

Wang, X. and X. Sun, 2009. Fair blind signature based authentication for super peer P2P network. Inform. Technol. J., 8: 887-894.

Wang, X., L. Yang, X. Sun, J. Han, W. Liang and L. Huang, 2010a. Survey of anonymity and authentication in P2P networks. Inform. Technol. J., 9: 1165-1171.

Wang, X., X. Sun, G. Sun and L. Dond, 2010b. CST: P2P anonymous authentication system based on collaboration signature. Proceedings of the 5th International Conference on Future Information Technology, May 21-23, 2010, IEEE Computer Society, Busan, Korea, pp: 1-7.

Xie, M., G. Wei and Y. Ling, 2009. Analysis and application on rate-distortion model oriented scalable video sequences. Inform. Technol. J., 8: 188-194.

Xiong, L. and L. Liu, 2004. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowledge Data Eng., 16: 843-857.

Ye, L., H. Zhang and Q. Dai, 2011. Identifying P2P application with DHT behaviors. Inform. Technol. J., 10: 565-572.

Zaidan, B.B., A.A. Zaidan and M.L.M. Kiah, 2011. Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. Int. J. Pharmacol., 7: 382-387.