American Journal of Applied Sciences, 10 (1): 1-7, 2013
ISSN: 1546-9239
©2013 Science Publication
doi:10.3844/ajassp.2013.1.7 Published Online 10 (1) 2013 (http://www.thescipub.com/ajas.toc)

Privacy Preservation for File Sharing Scheme Using Secured File Block ID with Binary Trees

[1]M. Balamurugan, [2]S. Chenthur Pandian and [3]J. Bhuvana

[1]Department of IT, Selvam College of Technology, Anna University, Tamilnadu, India
[2]College of Engineering and Technology, Anna University, Tamilnadu, India
[3]Department of MCA, Selvam College of Technology, Anna University, Tamilnadu, India

Received 2012-08-23, Revised 2012-08-31; Accepted 2013-01-28

ABSTRACT

Privacy, the security of information from unauthorized access is gradually needed on the Internet and yet progressively more important while each user acts as both consumer and producer. The lack of privacy is mainly employed for peer-to peer file sharing applications, in which users in the network shared file with each other and their actions are easily monitored by the unauthorized users. Several techniques have been presented to monitor the unauthorized access of files in the network. Our previous work described the secured file sharing using cryptographic key value pairs which shares the file among the users based on the key location of the file. But it does not provide an efficient privacy preservation scheme for file sharing concepts. To enhance the study progress, in this study, we proposed the design and implementation of secured file sharing through online by assigning a secured file block and a participant id that provides users with explicit, configurable control over their file. A File Security Packet (FSP) is developed to maintain a collection of users' file assigned with its respective file and block id without disclosing the users' privacy data to the public. Then the file sharing is done with file block id relating to the participant id using binary trees which represents the exact location of data present in the file to be shared. Binary trees keeps all those files to be shared with a relevant file and block id for each users' file in a form of tree pattern framework. The proposed secured file sharing using B-tree is optimized for systems that read and write large blocks of files in a chronological manner. An experimental evaluation is done with several user clients in terms of communication key round, number of participants and the size of the file for exchange to estimate the performance of the proposed privacy of file sharing using secured file block id using with Binary Trees [PFSBT].

Keywords: Privacy Preservation, File Sharing, Binary Trees, File Security Packet, Security

1. INTRODUCTION

Privacy is the fortification of files or data from illegal disclosure is an extensive reputation of computer system proposal. Privacy is gradually more insufficient on the Internet and yet ever more significant while every user acts as both customer and creator. The requirement of privacy is predominantly applied for peer-to-peer data sharing applications.

In the previous years, reputation of systems for mutual work and file sharing improved considerably. The requirement for efficient information sharing inside the set of documents in the privacy preservation framework processed further to endeavor data management systems, in addition to mutual platforms for P2P networks.

Enormous volumes of private data are repeatedly composed and examined by applications using data mining. Such data comprise shopping habits, illegal records, medical account and acclaim records, amid others. On the one hand, such records is an imperative advantage to business organizations and governments equally to decision building processes and to present communal benefits, such as medicinal examination, crime diminution, national safety. Alternatively, examining such data release new threats to privacy and self-sufficiency of the entity if not completed properly.

The hazard to privacy develops into genuine because data mining techniques are capable to obtain greatly

Corresponding Author: Balamurugan, M., Department of IT, Selvam College of Technology, Anna University, Tamilnadu, India

receptive knowledge from unspecified data that is not yet recognized to database holders. To attain privacy in an active environment, it is required to establish a secured relationships among peer nodes in the network. To enhance the privacy preservation scheme, it is necessary to adjust with the reliability of the peer based on its activities in the communication environment. The level of the privacy is also being measured by sharing and distributing the policies of a peer. Owing to security and network overload, rising amount of collaborative data sharing is being called. As the quantity and combination of data enclosing user-specific information raises, thrashing the requesters of data guides to research problems in privacy preservation scheme.

At a procedural level, privacy is simple to achieve with central solutions. If the user data is accumulated on a server in a data center, user commands about transmission can be simply imposed and data about user interests can be cautiously restricted or hindered on user request. Nevertheless, the authenticity is fairly diverse in practice. Many popular web services need users to mark away their separation and control rights as a state of service; sites frequently obtain advantage of this to gather, accumulate and distribute enormous amounts of individual data about their users.

Almost everybody on the Internet acts as a contented producer and a contented consumer, with an assorted set of restriction on accessing the users' privacy data. One could propose systems for every procedural model, e.g., one for unidentified publication, another for unidentified download, yet one more for forbidden sharing. A principle of the privacy scheme is to sustain a collection of data sharing circumstances proficiently inside a distinct framework.

In this study, we are going to implement a Secured file sharing concepts without disclosing users' privacy data. Using binary trees, an assignment of file block id is done for each file to be shared and the participants involved in the file sharing mechanisms are assigned with a relevant id.

1.1. Literature Review

Providing a secure and reliable data delivery over Internet is a challenging objective of the privacy preservation scheme and illustrate several presented ideas in the privacy design. More newly, have employed cryptographic techniques to make data sharing with permissions in a common web services without revealing contented to service providers (Baden *et al.*, 2009). Another technique, OneSwarm (Isdal *et al.*, 2010) supports permissions as well as permitting users to distribute data widely without acknowledgment. A key characteristic of the One-Swarm design is that users have precise supportive power above the quantity of trust they put in peers and in the division model for their data: the similar data can be shared widely, secretly, or with admission power, with both trusted and untrusted peers. The scrutinizing of the privacy preservation is also being finished with the respective semantic policies for data sharing provides users much better privacy described in (Kagal and Pato, 2010).

The privacy preserving can also be done in the form of document centric approach in dispersed environment. For document centric approach, users need to know about the location of relevant documents to access. The location of documents is identified thorugh indexing facility discusssed by (Zerr and Nejdl, 2008). Another useful tool for privacy preservation scheme is Support Vectors Machine (SVM) presented by (Lin, 2011). SVM take the data from training data set, discharging the data to SVM classifier for communal use to clients will reveal the confidential contented of support vectors. The SVM for privacy preservation scheme violates the privacy-preserving necessities for some authorized or viable reasons suggested by (Sun, 2010).

A safe and privacy-preserving opportunistic framework, called SPOC (Lu *et al.*, 2012), implemented in mobile Healthcare emergency for free distributed file sharing approach. With SPOC, elegant file transactions can be achived to practice the computing-intensive Individual Health Information (PHI). In recent times, (Vaidya and Clifton, 2009) have presented cryptographic techniques to facilitate data sharing using kth element over data set. Fong and Weber-Jahnke (2012), begins a privacy preserving approach with decision tree learning, without associated thrashing of accuracy. But, conservation of the privacy for collected data samples has a chance of being vanished. The troubles of Privacy-Preserving are Addressed effectively with Duplicate Tuple Matching (PPDTM) (Sang *et al.*, 2009a) and Privacy-Preserving Verge Attributes Matching (PPTAM). An analogous confront for privacy preservation is done with tuple matching (Sang *et al.*, 2009b), endeavors to mask conscious participants. In BitTorrent swarms (Zhang *et al.*, 2010) achieved privacy of file sharing based on the data obtained with it. In this study, binary tree representation is presented to enhance the privacy preservation file sharing mechanisms.

2. MATERIALS AND METHODS

2.1. Proposed Privacy of File Sharing using Secured File Block ID with Binary Trees

The proposed work is efficiently designed for providing a secured file transferring scheme among the networks in the system by assigning a secured file block id to each file maintained by the user and associated with each participant using binary trees. The proposed privacy of file sharing using secured file block id using with binary trees [PFSBT] is operated under two phases. The first phase is to assign a secured file block id using file security packet. The second operation is to provide a privacy preservation scheme of file sharing approach using binary trees. The architecture diagram of the proposed privacy of file sharing using secured file block id using with binary trees [PFSBT] is shown in **Fig. 1**.

The first phase describes the process of evaluating the secured file block id scheme for every file sustained by the users using a file security packet. A File Security Packet (FSP) maintains a security relevant data for files in the form of FSP structure. Using FSP, a file block id is assigned and processed for file sharing mechanisms. The FSP data can be examined by users other than the security product. The FSP is mapped by file and block id, so others should not use this mapping to create or directly modify the FSP and should not make their own security or audit decisions based on the contents of the FSP.

The second phase describes the process of privacy preservation scehme for file sharing approaches using a secured file and block id for each users' file with binary trees. The privacy preservaton scheme of file sharing approaches is done with secured file and block id relevant to each participant Id using binary trees.

The above figure (**Fig. 1**) represents the entire process of the proposed privacy preservation scheme for file sharing approaches using binary trees by assigning a file and block id for each file maintained by the users' involved in the network. The assignment of each file id is done with the help of file security packet scheme.

2.2. Assigning File and Block id using FSP

A file security packet is a storage space system which assigns an id for each file and the participant and none other user can modify or use the data in the FSP without the knowledge of the owner of the respective file. A participant in the network has one or more files which are ready to be shared with the other users in the network. For each participant, it is necessary to assign an id by tracing the actions of that participant in the communication he has involved before.

When two peers attach, they substitute file list messages. File list messages are condensed XML counting attributes recounting the size, name, date shared and other meta-data for files for which a scrupulous participant has permissions. For each confidentially shared file the meta-data comprises a potential that is used as a symmetric encryption key for exercise during transfers.

Instead of sharing all data visibly with an active set of participants, file security packet clearly classify the trust level of a determined set of participants and files using their respective ids (by default peers are untrusted). Second, instead of integrating information about which users have which files, put isolated data sources by torrenting object lookups during the overlay. Third, instead of sources transferring data openly to receivers, data transfers are done using participant and file block identities.

A file security packet will maintain all the details about the participants and files. For a file, FSP comprises of Fid (File id), Pid (Participant id), Shared Pid, Bid (File block id) as shown in **Fig. 2**. The FSP maintains the information of participant about the participant id and number of files in which each participant has. It also maintains information of file about file id, block id, owner id of the respective file and the shared participant id for that shared file. The file security packet maintained valid information about the user and the participant and none other user can access or modify the data maintained by FSP, since it allowed an access to the file only the participants who have a valid id or valid member of the file security packet mechanisms.

2.3. Representation of Binary Tree for Privacy Preservation Scheme

After assigning the file and participant id for each participant and files which they maintained, now in this section1.4, we are going to see about how the files are shared in a secure manner without disclosing the private data of the participant using binary trees. For each participant involved in the communication will follow the binary tree pattern framework for each files they maintained. The other participant (User B) could share the file of participant (User A) using block id than file id. The file id provides information about the location of file. A block id refers to the location of the exact data content in the file. Rather than sharing with the file id, the file block id file sharing consumes less time to achieve the file sharing concepts since it specified the exact location of the data content to be shared.

The above figure (**Fig. 3**) describes the binary tree representation for the secured file sharing scheme. A user (P1, P2, P3) has one or many files (F1, F2, F3, F4, F5, F6) to be shared. For each file, a file id and block id is specified and this is represented as specified in **Fig. 3**. A straight line in **Fig. 3** represents the file id and block id a file have and a dotted line represent the sharing of the content of the file by another user. Using file id and block id, users can share their files with the other users in the network.

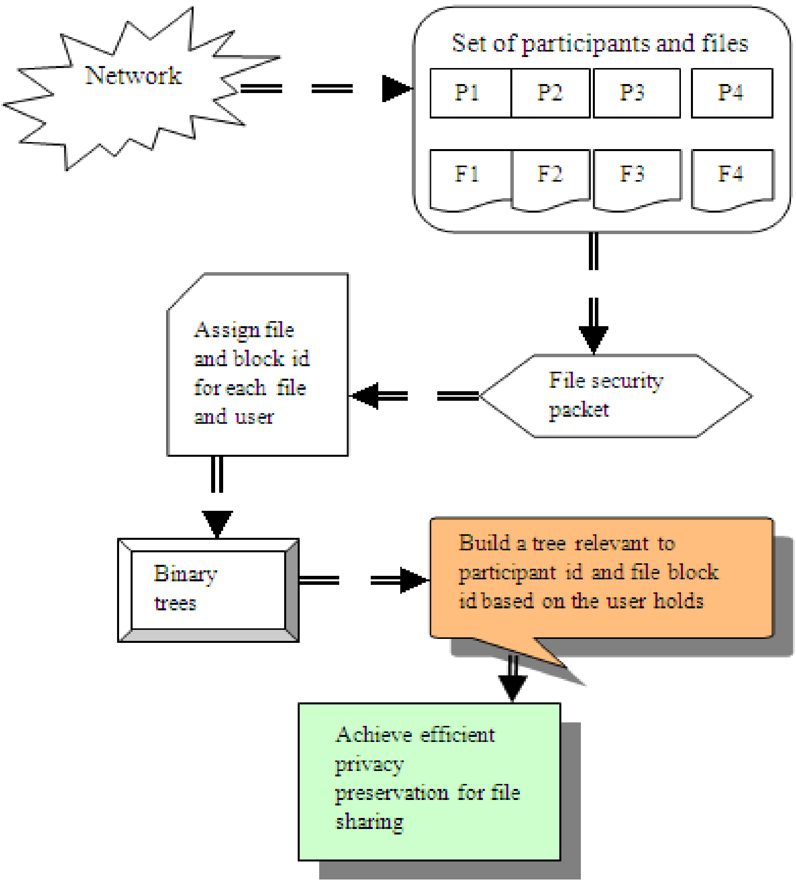
Network
Set of participants and files
P1
P2
P3
P4
F1
F2
F3
F4
File security packet
Assign file and block id for each file and user
Binary trees
Build a tree relevant to participant id and file block id based on the user holds
Achieve efficient privacy preservation for file sharing

Fig. 1. Architecture diagram of the proposed PFSBT

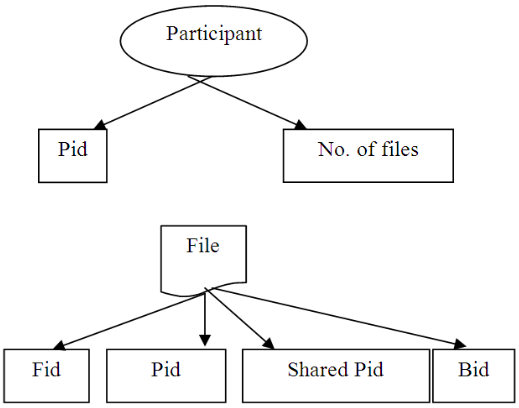

Fig. 2. Process of File security packet

A file id specifies the location of file in the file security packet and the block id refers to the specified data location on the file security packet. So, it is easy for the user to choose the file block id to share retrieve the content from the file in a secure way.

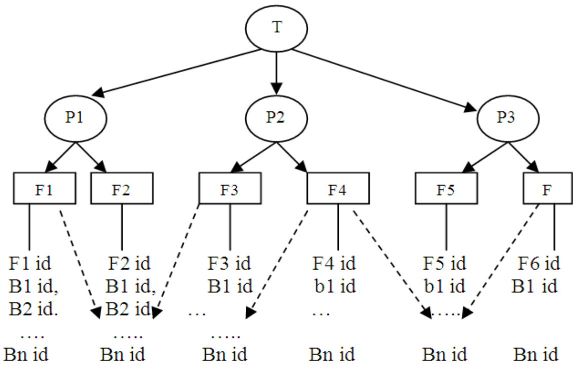

Fig. 3. Binary representation for privacy preservation scheme using FSP

When sharing data with binary tree representation using FSP, disclosure is limited by familiar mechanisms: strong identities, capabilities and end-to-end encryption. So, the privacy of the data content in the file stored in a secure way and only the authorized user can access it in a reliable manner. The pseudo code below describes the performances of the proposed privacy of file sharing using secured file block id using with binary trees [PFSBT]:

```
Input:  Set of users U, Set of files F
Step1:  Each user might have one or more F
Step2:  Apply FSP // Assigning secured File Block id
Step3:  For each user U
Step4:  Assign Uid
Step5:  Count the number of files he has (n)
Step6:  End For
Step7:  For each file F
Step8:  Assign Fid
Step9:  Assign Bid
Step10: Find the Uid of the respective file F
Step11: End for
Step12: FSP maintains all the above mentioned details
        in it i.e., it maintains only the authorized data //
        Privacy Preservation using Binary tree
        representation
Step13: Form a binary tree structure based on U and F
Step14: For each U (Uid)
Step15: There might be some F (Fid)
Step16: For each F, there might be some Bid (Block id)
Step17: End For
Step18: End for
Step19: Allow the users to share their file based on Bid
        using their own Uid, since bid refers to the
        exact location of the data content of the
        respective file
Step20: End (Privacy preservation achieves)
```

The algorithm above describes the process of the proposed privacy of file sharing using secured file block id with Binary Trees [PFSBT]. The first process is to assign a secured file block id to the files and participants whoever involved in the communication process. The File Security Packet (FSP) maintains the entire file and participant id in it and acts as like a file allocation table. After assignment of secured file block id, the binary tree representation is done by splitting the file and block id for each file maintained by the respective participant. Through the tree framework, the files can be accessed in a secure manner without disclosing its privacy data.

2.4. Experimental Evaluation

The proposed privacy of file sharing using secured file block id with Binary Trees [PFSBT] is efficiently designed and used for providing a secured way of file sharing approach using binary tree representation. The implementation of the proposed PFSBT is done with Intel P-IV machine with 2 GB memory and 3 GHz dual processor CPU. At first setup, the secured file block id is assigned using file security packet scheme and the representation of binary trees are used to form a secured file sharing approach by using file block id. Compared to an existing cryptographic key value pairs, the proposed PFSBT provides a secure file sharing mechanism in a reliable manner by implementing file security packet and binary tree representation. The binary tree is formed with the tree pattern framework by simply assigning the corresponding file and block id to its respective participants.

3. RESULTS

The performance of the proposed privacy of file sharing using secured file block id with binary trees is measured in terms of:

- FSP efficiency
- Tree Building time
- File sharing time

FSP efficiency describes the effectiveness of secure transformation of the files over the network the user has:

FSP efficiency = No. of files transferred securely/
Total no. of files

The above table (**Table 2**) describes the time taken to build the binary tree for achieving the privacy preservation scheme. The outcome of the proposed privacy of file sharing using secured file block id with binary trees is compared with an existing Cryptographic Key Value Pairs (CKVP).

Figure 5 describes the binary tree building time pattern framework based on the number of sequential files a user have. Since the proposed followed the representation of binary tree, the privacy preservation is highly achievable and it allows the participants for an easy access of the file contents the participants have. The binary tree is built based on participant id and file block id scheme. The tree building time is measured in terms of seconds. Compared to an existing cryptographic key value pairs, the proposed privacy of file sharing using secured file block id with binary trees, efficiently built the tree, with the file block evaluated from file security packet and the variance is 20-30% low in the proposed PFSBT.

The above table (**Table 3**) describes the time taken to share the file in a short interval of time for achieving the privacy preservation scheme. The outcome of the proposed privacy of file sharing using secured file block id with binary trees is compared with an existing Cryptographic Key Value Pairs (CKVP).

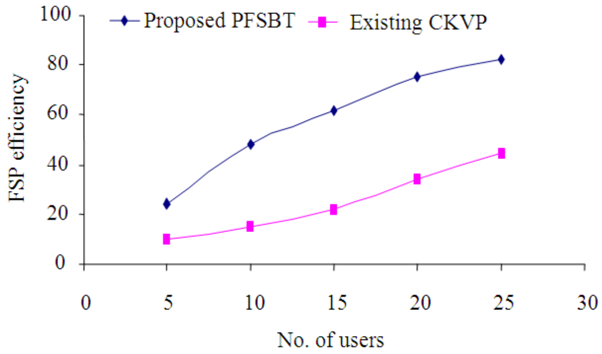

Fig. 4. No. of users Vs FSP efficiency

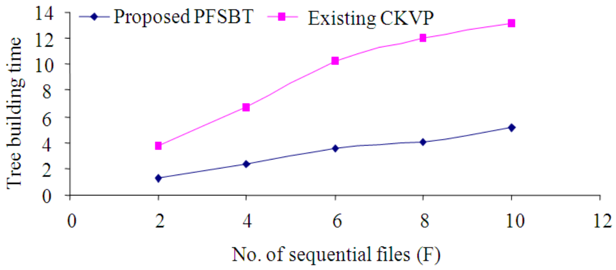

Fig. 5. No. of sequential files Vs Tree building time

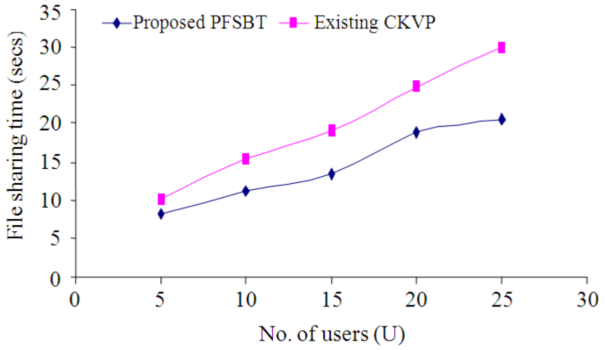

Fig. 6. No. of users Vs File sharing time

Table 1. No. of users Vs FSP efficiency

	FSP efficiency	
No. of users	Proposed PFSBT	Existing CKVP
5	24	10
10	48	15
15	62	22
20	75	34
25	82	45

Table 2. No. of sequential files Vs Tree building time

	Tree building time (secs)	
No. of sequential files	Proposed PFSBT	Existing CKVP
2	1.3	3.8
4	2.4	6.8
6	3.6	10.2
8	4.1	12.0
10	5.2	13.1

Table 3. No. of users Vs File sharing time

	File sharing time (seconds)	
No. of users	Proposed PFSBT	Existing CKVP
5	8.2	10.2
10	11.1	15.4
15	13.3	19.2
20	18.9	24.8
25	20.5	30.0

Figure 6 describes how long it will take to share the file among the users involved in the communication based on the number of users present. In the proposed PFSBT, the file sharing is done with a secured file block id. The binary tree has set of participants and each participant might have a set of files specified as file id and block id. The file id specified the location of file in the file security packet and the file block id specified the exact location of the content of the file to be shared. The proposed PFSBT shared the file in the network using file block id, so the consumption of time to share the file among the users will become less. The file sharing time is measured in terms of seconds (secs). Compared to an existing cryptographic key value pairs, the proposed privacy of file sharing using secured file block id with binary trees, efficiently share the file without disclosing its privacy data and the variance is 10-30% low in the proposed PFSBT.

4. DISCUSSION

Compared to an existing cryptographic key value pairs, the proposed PFSBT provides a secure file sharing mechanism in a reliable manner by implementing file security packet and binary tree representation. An experimental evaluation is processed with several user clients in terms of communication key round, number of participants and the files utilized for exchange to estimate the performance of the proposed PFSBT.

At last, it is being observed that the proposed privacy of file sharing using secured file block id with binary tree efficiently achieved the privacy scheme by implementing a file security packet and the representation of binary tree based on the FSP and shared the respective file with the users based on file block id. The proposed PFSBT allowed the users to share the file in a short interval of time without releasing its privacy data.

5. CONCLUSION

An incredible growth in internet made us to share everything through online. To share a file each other online, without disclosing the private data, this study efficiently described the process of sharing of file in a secure manner using file security packet mechanism with binary tree representation. To improve the secured sharing of file among the users', the study presented a File security packet scheme. The FSP played an important part of the privacy file sharing mechanism, since it has maintained all the privacy data of the user and files. By using file security packet, the file sharing is being done reliably for many users using the representation of binary trees. With the binary trees, we can easily identified the location of file and the user who holds the respective file. The experimental evaluation presented here described the performance of the proposed PFSBT carried out with the number of participants and the files they hold for privacy file sharing mechanism. The results shown that compared to existing CKVP, the proposed PFSBT provides an efficient secure file sharing mechanism in the network. The adversary rate in the proposed FSP with binary tree representation is low and the efficiency rate is 80% high contrast to the existing cryptographic key value pairs mechanism.

6. REFERENCES

Baden, R., A. Bender, N. Spring, B. Bhattacharjee and D. Starin, 2009. Persona: An online social network with user-defined privacy. Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication, Aug. 16-21, ACM Press, New York, pp: 135-146. DOI: 10.1145/1592568.1592585

Fong, P.K. and J.H. Weber-Jahnke, 2012. Privacy preserving decision tree learning using unrealized data sets. IEEE Trans. Knowl. Data Eng., 24: 353-364. DOI: 10.1109/TKDE.2010.226

Isdal, T., M. Piatek, A. Krishnamurthy and T. Anderson, 2010. Privacy-preserving P2P data sharing with OneSwarm. Proceedings of the ACM SIGCOMM 2010 Conference, Aug. 30-Sep. 03, ACM Press, New York, pp: 111-122. DOI: 10.1145/1851182.1851198

Kagal, L. and J. Pato, 2010. Preserving Privacy based on semantic policy tools. Security Privacy IEEE, 8: 25-30. DOI: 10.1109/MSP.2010.89

Lin, K.P., 2011. On the design and analysis of the privacy-preserving SVM classifier. Proceedings of the IEEE Transactions on Knowledge and Data Engineering, (TKDE' 11), IEEE Xplore Press, pp: 1704-1717. DOI: 10.1109/TKDE.2010.193

Lu, R., X. Lin and X. Shen, 2012. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Trans. Parallel Distrib. Syst. DOI: 10.1109/TPDS.2012.146

Sang, Y., H. Shen and H. Tian, 2009b. Privacy-preserving tuple matching in distributed databases. Proceedings of the IEEE Global Telecommunications Conference, (IGTC' 09), IEEE Xplore Press, pp: 1767-1782. DOI: 10.1109/TKDE.2009.39

Sang, Y., H. Shen and H. Tian, 2009a. Privacy-preserving tuple matching in distributed databases. IEEE Trans. Knowl. Data Eng., 21: 1767-1782. DOI: 10.1109/TKDE.2009.39

Sun, J., 2010. A privacy-preserving scheme for online social networks with efficient revocation. Proceedings IEEE INFOCOM, Mar. 14-19, IEEE Xplore Press, San Diego, pp: 1-9. DOI: 10.1109/INFCOM.2010.5462080

Vaidya, J. and C.W. Clifton, 2009. Privacy-preserving Kth element score over vertically partitioned data. IEEE Trans. Knowl. Data Eng., 21: 253-258. DOI: 10.1109/TKDE.2008.167

Zerr, S. and W. Nejdl, 2008. Privacy preserving document indexing infrastructure for a distributed environment. Proceedings of the VLDB Endowment, (VLDBE' 08), ACM Press, USA., pp: 1638-1643.

Zhang, C., P. Dhungel, D. Wu, Z. Liu and K.W. Ross, 2010. BitTorrent darknets. Proceedings of the INFOCOM, Mar. 14-19, IEEE Xplore Press, San Diego, CA., pp: 1-9. DOI: 10.1109/INFCOM.2010.5461962