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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Review Paper on Privacy Preservation for File Sharing Scheme Using Secured File Block Id with Binary Trees and Encryption

Navdeep Singh, Dr. Rahul Malhotra

PG Student, Dept. of ECE, Guru Teg Bahadar Khalsa Institute of Engineering & Technology, Chapia Wali Malout, India

Director, Dept. of ECE, Guru Teg Bahadar Khalsa Institute of Engineering & Technology, Chapia Wali Malout, India

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.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.

I. 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 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

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. sing 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. Some methods for privacy factor utilize certain amount of transformations involved on the part of data to achieve privacy. Cache obtains well-explored idea from dispersed systems, explicitly caching and finally relating it in the framework of privacy. One of the few applications involved in visual cryptography is secure multiparty copy right protection. The prime objective of secure multi party computation is to enable parties to mutually compute a function over their inputs, at the same time keeping these inputs as private. In current years, Color image visual cryptic filtering method is presented for deblurring effect of the non-uniform distribution of visual cryptic share pixels. Texture overlapping filters decide which part of input image to be patched with output texture. Privacy of the owners is preserved using cache mechanism with visual cryptography for distributed digital document. While employing filter mechanism, though pixels were considered the image quality was enhanced using texture overlap and Fourier filtering, this remove the noise present in the image using CMY color model. All information of the users is preserved for distributed digital document using cache mechanism, who shared the secret parts of digital document which has been split using visual cryptography for digital document sharing, between the peer users. The distributed file for distributed data sharing using visual cryptography model further enhances the process of security by deploying distributed key model and binary spanning tree.

II. LITERATURE REVIEW

[1]privacy preservation for file sharing scheme using secured file block id with binary trees,2013:
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

[2] Secured Privacy Preserving Mechanism for Distributed Digital Documents,2014: The increasing availability of internet and digital imaging knowledge has given rise to the secret image sharing and visual cryptography. The unauthorized nature of data and sharing control systems, breach their privacy. To address this issue, a very efficient and robust visual cryptography scheme called, securitizing visual cryptography using error transmission technique. First, an efficient color image visual cryptic filtering scheme to improve the image quality on restored original image from visual cryptic shares. Fourier transformation and texture overlapping is applied to normalize the unevenly transformed share pixels on the original restored image. Second, privacy preservation using cache-cache mechanism which maintains cache inside a cache to preserve details about the users who shared the secret parts of digital document which has been split using visual cryptography is presented. Third, to enhance security for distributed file sharing in visual cryptography, binary spanning trees are used. Privacy of file sharing is performed with file block id relating to the participant id using binary trees. Finally, providing security and to achieve good quality of reconstructed image, error transmission technique is introduced. Experimentation carried out with bench mark data sets of real and synthetically generated data sets estimate the performance of Secured Privacy Preserving Mechanism for distributed digital document (SPPM) in terms of visual quality, time taken to read the text, security level.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

[3] Efficient and Secure Data Storage Operations for Mobile Cloud Computing,2012:
In a mobile cloud computing system, lightweight wireless communication devices extend cloud services into the sensing domain. A common mobile cloud secure data service is to inquiry the data from sensing devices. The data can be collected from multiple requesters, which may drain out the power of sensing devices quickly. Thus, an efficient data access control model is desired. To this end, we present a comprehensive security data inquiry framework for mobile cloud computing. Our solution focuses on the following two research directions: First, we present a novel Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) to protect sensing data. Using PP-CPABE, light-weight devices can securely outsource heavy encryption and decryption operations to cloud service providers, without revealing the data content. Second, we propose an Attribute Based Data Storage (ABDS) system as a cryptographic groupbased access control mechanism. Our performance assessments demonstrate the security strength and efficiency of the presented solution in terms of computation, communication, and storage.
[4] **Trust-Based Privacy Preservation File Sharing Scheme for Peer-to-peer Network,2013**
Privacy preservation in a peer-to-peer system tries to hide the association between the identity of a participant and the data that it is interested in. We propose a trust-based privacy preservation method for peer-to-peer data sharing. It adopts the trust relation between a peer and its collaborators. 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.

III. PROBLEM DEFINITION

In existing paper they have used ofFSPAfter assigning the file and participant id for eachparticipant and files which they maintained, now in this they are going to see about how the files areshared in a secure manner without disclosing the privatedata of the participant using binary trees. For eachparticipant involved in the communication will followthe binary tree pattern framework for each files theymaintained. The other participant (User B) could sharethe file of participant (User A) using block id than fileid. The file id provides information about the location offile. A block id refers to the location of the exact datacontent in the file. Rather than sharing with the file id,the file block id file sharing consumes less time toachieve the file sharing concepts since it specified theexact location of the data content to be shared. Usingfile id and block id, users can share their files with theother users in the network.
In this technique sharing the block id in the network with other person can be in-secured. Because blockid can misused by any person in between.Any body can read the data lying at specific blockid. We can protect it by providing the encrypted block id. And body who has legal decryption key will be considered as legal person who can read specific block id contents.

IV. OBJECTIVES

1. providing the participant id to each participant.
2. Providing the file id to each file.
3. Providing the block id each file block to specific participant who accessed the data often.
4. Using encryption key to specific blockid.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

5. Use appropriate decryption key to decode the data.

V. TOOL USED TO IMPLEMENT IT

1. NetBeans 7.0
2. Mysql server.
3. Encryption standard tools.

VI. METHODOLOGY

1. building the network of specific no. of persons.
2. Allotting the participant id to each person part of the network
3. Allotting the block id to data often used by specific participant id under specific file id
4. Providing encryption key and decryption key to the recipient.

REFERENCES

[1]Baden, R., A. Bender, N. Spring, B. Bhattacharjee and D. Starin, 2009. Persona: privacy preservation for file sharing scheme using secured file block id with binary trees. Proceedings of the ACM SIGCOMM 2013
[2]Fong, P.K. and J.H. Weber-Jahnke, 2014.Secured Privacy Preserving Mechanism for Distributed Digital Documents. IEEE Trans. Knowl. Data Eng., 24: 353- 364. DOI: 10.1109/TKDE.2010.226
[3]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
[4]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
[5]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:
[6]A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency.IEEE Trans. Parallel Distrib. Syst. DOI: 10.1109/TPDS.2012.146
[7]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
[8]Sang, Y., H. Shen and H. Tian, 2009a.Privacypreserving tuple matching in distributed databases. IEEE Trans. Knowl. Data Eng., 21: 1767-1782. DOI: 10.1109/TKDE.2009.39 Sun, J., 2010.
[9]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
[10]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
[11]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.
[12]Zhang, C., P. Dhungel, D. Wu, Z. Liu and K.W. Ross, 2010.BitTorrentdarknets. Proceedings of the INFOCOM, Mar. 14-19, IEEE Xplore Press, San Diego, CA.,pp: 1-9. DOI: 10.1109/INFCOM.2010.5461962