ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 12, pp.76374-76376, December, 2018
DOI: https://doi.org/10.24941/ijcr.33582.12.2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

TIME WISE DOCUMENT SHARING AND LEAKAGE DETECTION SYSTEM WITH ENCRYPTION TECHNIQUE IN CLOUD

***Kajal S. Rathod and Mante, R.V.**

Department of Computer Science and Engineering, Government College of Engineering, Amravati, Amravati, India

ARTICLE INFO

Article History:
Received 20th September, 2018
Received in revised form
10th October, 2018
Accepted 19th November, 2018
Published online 31st December, 2018

Key Words:
Data Dissemination, Attribute-Based Encryption, timed-Release Encryption, Cloud Computing.

ABSTRACT

Cloud computing become more popular over the world. It provides services over the Internet. Cryptographic techniques provides protection for data of users in public cloud, but there are some issues, such as secure data group sharing and fine-grained access control of time-sensitive data. In this paper, we proposed a secure corporate cloud based data sharing system for employees in which multiple companies can use cloud document sharing system. In our system we proposed a novel technique of encryption in which we are combining broad cast encryption technique and Attribute based encryption technique with each other. Along with the security of the system we proposed auto leakage control system to prevent the document leakage before release time. Here, we are using identity based data group sharing scheme, in which data owner can send encrypted message over a group of receivers at one time by specifying these receivers' identities.

Citation: Kajal S. Rathod and Mante, R.V. **2018.** "Time wise Document Sharing and Leakage Detection System with Encryption Technique in Cloud", *International Journal of Current Research*, 10, (12), 76374-76376.

INTRODUCTION

Cloud computing become more popular around the world. Cloud storage service has more advantages on for convenient data sharing and cost reduction. There is no need of installation on user's computer and can be accessed from different places, cloud computing provide easy maintains. In our proposed system, we will discuss about time dependent data sharing over cloud efficiently. Qinlong Huang, Member, IEEE, Yixiang Yang and Jingyi Fu explained new technique for data sharing in which the document will be encrypted using broadcast encryption technique and the attributes will be embedded using Attribute-based encryption (ABE) technique on proxy server by using re-encryption on proxy. In existing system, there is one data disseminator admin who is responsible to re-encrypt the document using end user's attributes after release time. As the data disseminator (DD) admin is an honest but curious user, there is a possibility of data leakage from disseminator admin. To prevent data leakage we proposed an auto controlled mechanism which controls the data sharing before release time. One more limitation exposed in existing system, to share the documents with end users, the DD admin have to re-encrypt the document with new attributes and in case of attributes revocation as well as addition, the admin needs to perform decryption and encryption operations again and again which increases the computation overload on the system. We proposed a combined encryption technique containing broadcast encryption technique as well as ABE with constant cipher text, to overcome these issues. Qinlong Huang, Member, IEEE, Yixiang Yang and Jingyi Fu describe system in which broadcast encryption with attribute based encryption is proposed. The proposed technique is secure but need to re-encrypt the file again and again. This technique will replicate complete file with new attributes every time when any user wants to share document with new attributes. Due to which more server space will be occupied by the files. Therefore to reduce required server space we proposed new technique. In that system more server space is required while sharing the files. To reduce required space we proposed new technique. Existing algorithm need more computation time to re-encrypt the documents, to reduce computation time we proposed our system. In our proposed system, we will discuss about time dependent data sharing over cloud efficiently. In earlier paper, the author explained new technique for data sharing in which the document will be encrypted using broadcast encryption technique and the attributes will be embedded using Attribute-based encryption (ABE) technique on proxy server by using re-encryption on proxy. In existing system, there is one data disseminator admin who is responsible to re-encrypt the document using end user's attributes after release time. As the data disseminator (DD) admin is an honest but curious user, there is a possibility of data leakage from disseminator admin.

****Corresponding author:*** **Kajal S. Rathod,**
Department of Computer Science and Engineering, Government College of Engineering, Amravati, Amravati, India.

To prevent data leakage we proposed an auto controlled mechanism which controls the data sharing before release time. One more limitation exposed in existing system, to share the documents with end users, the DD admin have to re-encrypt the document with new attributes and in case of attributes revocation as well as addition, the DD admin needs to perform decryption and encryption operations again and again which increases the computation overload on the system. We proposed a combined encryption technique in which broadcast encryption technique and ABE with time release encryption is used. The main theme of work is to provide security of time sensitive data on cloud by combined time and attribute factor. We propose new technique to overcome the drawbacks of CP-ABE and KP-ABE. User uploads the document on cloud. The encrypted document will save on cloud. At the time of document encryption Release time allocated. Original file contains document information such as access attribute and release time. In our proposed combined technique, we will maintain the attributes and broad casting information on the header of the files instead of combining the attributes with file. The file is encrypted using separate key; the key will be maintained in the header of the document along with attributes and release time. If Admin need to share any document with other user, he will combine the attributes in header of the document insteadofcompletedocument.

Literature review: Currently, more and more users would store data to cloud service provider (CSP) for sharing. However, the CSP which deprives data owners' direct control over their data is assumed to be honest-but-curious, that may prompt security concerns. These security matters existing in public cloud motivate the requirement to appropriately keep data confidential. Cryptographic mechanisms used for security problems. In order to guarantee secure data group sharing, identity-based broadcast encryption (IBBE) scheme is employed in public cloud. Cecile describes the first IBBE with constant size ciphertexts and private keys. In broadcast encryption schemes, message will be encryprted and transmits to user's group and private keys will used to decrypt message. The data owners could broadcast their encrypted data to a group of receivers at one time and the public key of the user can be regarded as email, unique id and username. Using the id of users the data owner can send the data to another user. Attribute-based encryption (ABE) is a encryption technique which is used in cloud to provide security for data group sharing.

Identity-based encryption: An IBE scheme is a encryption technique in which parameters can be taken as public key. Names, dates, and email addresses, for example, may serve as public keys in an IBE system. This feature is valuable because it reduces the interaction and infrastructure required to send data securely. In particular, is possible to perform encryption using public key of a selected entity without performing a certificate lookup or other interaction.

An IBE system consists of four randomized algorithms, which we roughly summarize as follows:

- **Setup:** The function setup is executed by the PKG (public key generation) on input consisting of a security parameter k. The output includes params, a set of data comprising a message space, a ciphertext space, and other parameters to be published by the PKG.
- **Key-gen:** T Given input params, master key, and some string (public-key) ID, the function key-gen returns dID: the private key corresponding to ID.
- **Encrypt:** Given input params, the string (public-key) ID, and a message M, the function encrypt yields a ciphertext C.
- **Decrypt:** The Given input params, the string (public-key) ID, and the correct corresponding private key dID, the function decrypt returns the message M.

Attribute Based Encryption: Attribute-based encryption (ABE) is a encryption technique which is used in cloud to provide a secure data group sharing. In many of the systems a user can access data if a user set a attributes. In ABE the user can send the encrypted message to another user by using his attributes. While sending the encrypted message, user should mention the attributes of another user to whom he want to send that message. John Bethencourt, Sahai and Brent Waters present a system in which they describing about access control on encrypted data that is known as Ciphertext-Policy Attribute-Based Encryption. Attribute-based encryption (ABE), introduced by Sahai and Waters (2005), offers an expressive way to define asymmetric-key encryption schemes for policy enforcement based on attributes. Here both a user secret key and ciphertext are associated with sets of attributes. There are two technique in ABE i.e. cipherrtext-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE).

Ciphertext-Policy Attribute-based Encryption: CP-ABE is a cryptography prototype for one-to-many secure communication. In a CP-ABE based scheme, besides the storage platform, the system consists of three basic parties: the authority, the owner and the user. The authority is introduced to publish system parameters and issue secret keys for the users. The owner shares files to the intended users by designating an access policy and encrypting the file under the policy.

Timed-Release Encryption: The concept of timed-release encryption is for scenarios that someone wants to securely send a message to another one in the future. In detail, the owner encrypts his/her message for the purpose that intended users can decrypt it after a designated time. From the security aspect, TRE satisfies that: 1) Except the intended users, no one is able to get any information of the message; 2) Even the intended user cannot get the plaintext of the message before the designated releasing time. In order to support an accurate timed release mechanism, a trusted time agent is required to manage the clock of the system. At each time point T, the agent releases a time token TKT, which is an important notion in TRE. When encrypting the message, the ciphertext is generated with the public key of the intended user and the designated releasing time T. The ciphertext holds the feature that only with the corresponding users secret key and time token TKT, can a user correctly get the plaintext of the message; otherwise, if without either of the two components, the user cannot successfully conduct the decryption.

PROPOSED METHODOLOGY

In our proposed system, we proposed secure time wise data sharing on cloud; in this system all the users will upload documents. Data Disseminator (DD) admin have rights to disseminate the data to other users.

We proposed auto controlled mechanism to prevent data leakage before time. Along with this, we proposed combined encryption technique (Broadcast encryption + ABE). We will maintain the attributes and broad casting information on the header of the files instead of combining the attributes with file. If DD admin need to share any document with other user, he will combine the attributes in header of the document instead of complete document. This technique will reduce computation cost.

Conclusion

Study of various encryption techniques, ABE, IBBE is presented in this paper. In our proposed system, we proposed a combined encryption technique which reduces the time required for re-encryption. The paper shows the advantage of our new encryption technique over the existing encryption techniques.

REFERENCES

Bethencourt, J., Sahai, A. and Waters, B. 2007. "Ciphertext-policy Attribute- based Encryption," Proc. the 28th IEEE Symposium on Security and Privacy (S&P 2007), pp. 321-334.

Blaze, M., Bleumer, G. and Strauss, M. 1998. "Divertible Protocols and Atomic Proxy Cryptography," Proc. Advances in Cryptology Eurocrypt 1998 (EUROCRYPT '98), pp.127-144.

Chu, C., Weng, J., Chow, S., Zhou, J. and Deng, R. 2009. "Conditional Proxy Broadcast Re-encryption," Proc. 14th Australasian Conference on Information Security and Privacy (ACISP 2009), pp. 327-342.

Delerablée, C. 2007. "Identity-based Broadcast Encryption with Constant Size Ciphertexts andPrivateKeys," Proc. the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007), pp. 200-215.

Hong, J., K. Xue, W. Li, and Y. Xue, "TAFC: Time and Attribute Factors Combined Access Control on Time-Sensitive Data in Public Cloud," Proc. 2015 IEEE Global Communications Conference (GLOBECOM 2015), pp. 1-6, 2015.

Huang, Q., Yang, Y. and Fu, J. 2017. "PRECISE: Identity-based Private Data Sharing with Conditional Proxy Re-encryption in Online Social Networks," Future Generation Computer Systems, doi: 10.1016/j.future.2017.05.026

Hur, J. 2013. "Improving Security and Efficiency in Attribute-Based Data Sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271-2282,

Liang, K., Au, M. H., Liu, J. K. and Susilo, W. 2014. "A DFA-based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing," IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667-1680.

Liang, K., Au, M., Liu, J., Susilo, W., Wong, D. G. Yang, Y. Yu, and A. Yang, 2015. "A Secure and Efficient Ciphertext-policy Attribute-based Proxy Re-encryption for Cloud Data Sharing," Future Generation Computer Systems, vol. 2015, no. 52, pp. 95-108.

Liu, W., Liu, J. and Wu, Q. 2016. "Practical Chosen-ciphertext Secure Hierarchical Identity-based Broadcast Encryption," International Journal of Information Security, vol. 15, no. 1, pp. 35-50.

Liu, W., Liu, J. and Wu, Q. 2016. "Practical Chosen-ciphertext Secure Hierarchical Identity-based Broadcast Encryption," *International Journal of Information Security*, vol. 15, no. 1, pp. 35 -50.

Qin, Z., Xiong, H., Wu, S. and Batamuliza, J. 2016. "A Survey of Proxy Reencryption for Secure Data Sharing in Cloud Computing," IEEE Transactions on Services Computing, doi: 10.1109/TSC.2016.2551238.

Qinlong Huang, Member, IEEE, Yixiang Yang and Jingyi Fu," Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud", IEEE Transactions on Services Computing TSC.2018.

Sepehri, M., Cimato, S., Damiani, E. and Yeuny, C. 2015. "Data Sharing on the Cloud: A Scalable Proxy-based Protocol for Privacy-preserving Queries," Proc. 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2015), pp. 13571362.

Shao, J., Wei, G., Ling, Y. and Xie, M. 2011. "Identity-based Conditional Proxy Re-encryption," Proc. 2011 IEEE International Conference on Communications (ICC 2011), pp. 1-5.

Tran, D., Nguyen, H., Zha, W. and Ng, W. "Towards Security in Sharing Data on Cloud-based Social Networks," Proc. the 8th International Conference on Information, Communications and Signal Processing (ICICS2011), pp. 1-5, 2011

Wan, Z., Liu, J. and Deng, R. 2012. "HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754.

Weng, J., Deng, R., Ding, X., Chu, C. and Lai, J. 2009. "Conditional Proxy Re-Encryption Secure Against Chosen-ciphertext Attack," Proc. the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (CCS 2009), pp. 322 -332.

Xu, P., Jiao, T., Wu, Q., Wang, W. and Jin, H.2016. "Conditional Identity-based Broadcast Proxy Re-encryption and its Application to Cloud Email," IEEE Transactions on Computers, vol. 65, no. 1, pp. 66-79.

Yang, K., Liu, Z., Jia, X. and Shen, X. 2016. "Time-domain Attribute-based Access Control for Cloud-based Video Content Sharing: A Cryptographic Approach," IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 940-950.

Zhang, J., Zhang, Z., Guo, H. 2017. "Towards Secure Data Distribution Systems in Mobile Cloud Computing," IEEE Transactions on Mobile Computing, doi: 10.1109/ TMC.2017.2687931

Zhao, J., Feng, D. and Zhang, Z. 2010. "Attribute-based Conditional Proxy Re-encryption with Chosen-ciphertext Security," Proc. 2010 IEEE Global Communications Conference (GLOBECOM 2010), pp. 1-6.

Zhou, Y., Deng, H., Wu, Q., Qin, B.and Liu, J. 2016. "Identity-based Proxy Re-Encryption Version 2: Making Mobile Access Easy in Cloud," Future Generation Computer Systems, vol. 62, pp. 128-139.

****