Document Sharing with New Encryption Technique and Leakage Detection System using Time Condition

Kajal S. Rathod
PG Scholar
Department of Computer Science and Engineering
Government College of Engineering, Amravati
Amravati, India

R. V. Mante
Assistant Professor
Department of Computer Science and Engineering
Government College *of Engineering, Amravati*
Amravati, India

***Abstract*— now a day's most of the user use cloud computing to store the data over the Internet. Cloud computing provide the services to the user rather than Product. Data security become a big issue in cooperate world. In this paper, we proposed a new encryption technique. Here we used broad cast encryption technique with Attribute based encryption technique.**

In our system, we are using Time based document sharing technique. Whenever any Employee or any company member upload document at that time he should also set the release time and date for that document. Because of this time based document sharing technique we provide more security to the data. If anyone tries to access document before release time then system send the notification to the branch manager.

Keywords*— *Data dissemination, attribute-based encryption, timed-release encryption, cloud computing.

I. INTRODUCTION

Cloud computing become more popular around the world. Cloud storage service has more advantages for convenient data sharing and cost reduction. Cloud provided a easy way to store and access data. 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 wise data sharing over cloud. 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 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 containing broadcast encryption technique as well as ABE with constant cipher text, to solve these issues.

Qinlong Huang, 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. 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 DD admin need to share any document with other user, he will combine the attributes in header of the document instead of complete document.

II. Literature Review

Currently, more and more users would store data to cloud service provider (CSP) for sharing. 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 can broadcast their encrypted data to a group of receivers. 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.

A. 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.

B. 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, which is known as Ciphertext-Policy Attribute-Based Encryption. Sahai and Waters (2005) introduced Attribute-based encryption (ABE). 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).

C. 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.

III. 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.

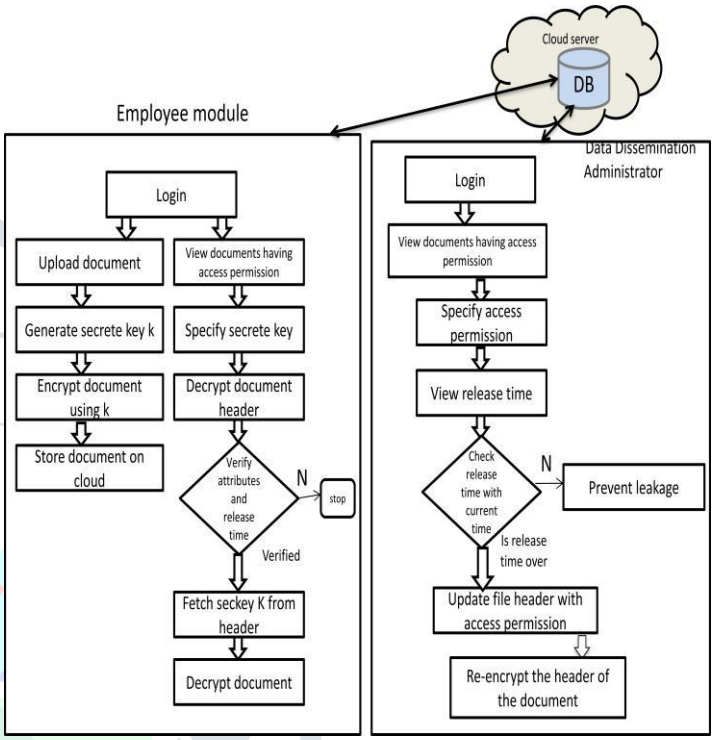

Figure: Proposed system model

Following are the modules which are used in our system:

- Cloud Admin
- Company Admin
- Branch Manager
- Employees
- Dissemination Admin
- Leakage Detection and Prevention

Firstly company has to register. After registration Admin approve the request. When admin approved the request, the user id and password will send to the company's mail id. Once company request is approved, company can login to system. After company login, company can register the Branch. At the time branch registration, a branch detail has to fill. Information required at time of registration such as branch name, branch code, mail, city and mobile number. Company admin also can upload and download documents.

Once Branch is registered, Branch manager can login using user id and password. Branch manager can

register the Employees. Branch manager can also upload and download documents. At the time of employee registration, information such as employee name, designation, gender and mail. At Employee Home, employee can upload the document. At the time of uploading document, document name, release time and date has to fill. Before Release date and time, no one can access the document. Employee can see the list of uploaded documents. Data Disseminator allows the authority to employees to access to the document. Data Disseminator decides the authority and access to employees that is which employee can access which document.

If any employee try to access the document before release date and time, then system generate the message and send notification to authorized person. At the time of downloading a document, when employee click on the download, the one-time secrete key will send to the employee's mail id. After that employee has to enter key, if key is verified successfully then employee can download the document.

IV. Conclusions

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

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

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

[3] Z. Wan, J. Liu, and R. Deng, "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, 2012.

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

[5] J. Weng, R. Deng, X. Ding, C. Chu, and J. Lai, "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, 2009.

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

[7] J. Hong, 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.

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

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

[10] K. Liang, M. H. Au, J. K. Liu, and W. Susilo, "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, 2014.

[11] M. Sepehri, S. Cimato, E. Damiani, and C. Yeuny, "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, 2015.

[12] C. Chu, J. Weng, S. Chow, J. Zhou, and R. Deng, "Conditional Proxy Broadcast Re-encryption," Proc. 14th Australasian Conference on Information Security and Privacy (ACISP 2009), pp. 327-342, 2009. [19] W. Liu, J. Liu, and Q. Wu, "Practical Chosen-ciphertext Secure Hierarchical Identity-based Broadcast Encryption," International Journal of Information Security, vol. 15, no. 1, pp. 35-50, 2016.

[13] K. Yang, Z. Liu, X. Jia, and X. Shen, "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, 2016.

[14] 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.

[15] D. Tran, H. Nguyen, W. Zha, and W. Ng, "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

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

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

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

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

[20] K. Liang, M. Au, J. Liu, W. Susilo, D. Wong, G. Yang, Y. Yu, and A. Yang, "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, 2015.

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

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