A Novel Attribute based Encryption Scheme for Efficient File Hierarchy in Cloud

Mr.Dileep Kumar Murala[1], Pabba Sai Sharanya[2], Thatipally Ravali[3], Uppala Sahana[4]
[1]*Assistant Professor*, [2,3,44] *B.TECH*
Department of Information Technology, Malla Reddy Engineering College for Women

Abstract **-** From the recent years the usage of healthcare information has raised drastically. So the scientists, programmers and organizations have kept their ideas to develop e-health applications. This idea raised science and data interchange between health details in web applications. This type of data is exchanged between applications of e-health and Health Information System. By this exchange of data the security issues were occur for sensitive data. In this paper, we proposed a FH-CP-ABE (File hierarchy Cipher text-policy attribute based encryption) to provide efficient file sharing in cloud computing. These hierarchical files are encrypted using symmetric algorithms before sharing data into the cloud so that both the cipher text storage cost and time for encrypting data can be reduced. In this paper we use one secret key for decrypting the encrypted information.

I. INTRODUCTION

To provide security and to avoid leakage of data we are sending the encrypted data for the storage area. Controlling the access is the supreme to prevent the data from unapproved persons from accessing the data. Thriving of network technology and mobile devices the exchange of data has become an addiction such as whatsapp, facebook, twitter and online shopping. One of 5the most sharing of data is through the cloud as a platform. To provide data privacy realizes fine-grained, one-to-many, and non interactive access control we are using attribute based encryption from past few years. Cipher text-policy attribute based encryption (CPABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications. The cloud service provider (CSP), who offers and controls the cloud resources, has full access to any data or computations brought into the cloud.

Second, because CSPs multiplex their limited resources to multiple consumers for efficiency reasons, there is the threat of other cloud consumers, with whom cloud resources are divvied up, breaking the isolations imposed by the CSP. The right to encrypt and upload the generated cipher text is given to Data owner. The downloaded interested cipher text files from CSP are done by the user. The shared files usually have hierarchical structure. That is, a group of files are divided into a number of hierarchy subgroups located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of cipher text and time cost of encryption could be saved.

A. Our Contributions - The contributions of our scheme are three aspects.

(i) Firstly, we propose the layered model of access structure to solve the problem of many ordered files sharing. Only one integrated structure can be used to encrypt the files.

(ii) Secondly, we also formally provide the guard of FH-CPABE scheme that can successfully thwart chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie Hellman (DBDH) assumption.

(iii) Thirdly, we conduct and implement whole experiment for FH-CP-ABE scheme, and the simulation outcome shows that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption.

II. LITERATURE REVIEW

Sahai and Waters [3] proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE. Latterly, a variant of ABE named CP-ABE [4], [5], [6] was proposed. IBE[7] and CP-ABE. Wan et al. [8] proposed hierarchical ABE scheme. Later, Zou [9] gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A cipher text policy hierarchical ABE scheme with short cipher text is also studied in [10]. In these schemes, the parent authorization domain governs its child authorization realm and a top level authorization domain creates secret key of the next level realm. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened. At present, there are three types of access structures AND gate, access tree, and linear secret sharing scheme (LSSS) used in existing CP-ABE schemes. At present, there are three types of access structures AND gate, access tree, and linear secret sharing scheme (LSSS) used in existing CP-ABE schemes. Cheung and Newport first used AND gate access structure to achieve CP-ABE scheme. Later, some improved schemes are proposed.

III. EXISTING PROBLEMS

In this we use various cloud services and models like Saas, Iaas, Paas and public, private and hybrid. It leads to various security issues, each model is associated atleast one issue. Security issues are considered as two types firstly the service provider who insures that services provided by them should be secure and also manages the customer's identity management. Other view is customer view that ensures that service that they are using is secure enough.

A. Multi-tenancy - In this only one instance of software can run on a server and serves many tenants. A tenant is a collection of users who share a common access with specific privileges to the software instance.

B. Elasticity - It is the system of degree which is able to handle the changes in the work load by provisioning and insane in self-regulating manner, So that they can reach the current demand at any time.

C. Insider attacks - Cloud model is the multitasking based model the is under the single management realm. This is the major problem that arises in the firm. Here we are not using any hierarchical standards so that hackers can easily stole the data from the firm. And can sell the information to the competitive firms.

D. Outsider attacks - It is the major issue which leaks the sensitive data to the other organization directly. Clouds are public networks and they have more interfaces compare to other networks so it gives the chance for attackers t**o hack the data.**

E. Deficiency of data - As cloud is a public network it is not providing any safety, integrity, security, authorization measures, it effects financial and in economical environment in the organization.

IV. THE PROPOSED FH-CP-ABE SCHEME

In this section, the detailed construction of FH-CP-ABE scheme is first presented. Then, based on the scheme, an improved encryption process about FH-CP-ABE scheme is proposed in order to reduce computational complexity. In addition, a brief discussion about FH-CP-ABE scheme's feature is also provided.

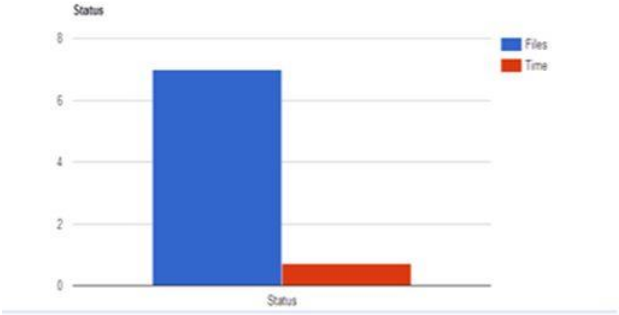
A. Scheme Construction - Let e: G0 × G0 → GT be a bilinear map, and G0 be bilinear group of prime order p with generator g. For any k ∈ Zp and an attribute set S = {S1, S2, Sm ∈ Zp}, the Lagrange coefficient k, S = π∈ S,l_=k (x − l)/(k − l). Two hash functions H : {0, 1}* → G0 and H2 : {0, 1}* →GT are used in the proposed scheme. An universe of attribute set is defined as A = {a1, . . . ,an}.

B. FH-CP-ABE Scheme With Improved Encryption - To facilitate the presentation in the below, we denote the above FH-CP-ABE scheme as BasicFH-CP-ABE. We now show how to modify the encryption process of BasicFH-CPABE scheme in order to reduce computational complexity. In ciphertext CT, some transport nodes are removed from CT if they don't carry any information about level node, where the information denotes leaf node, non-leaf node, level node, or transport node in hierarchical access tree. That is, these transport nodes are removed from CT if they do not directly or indirectly contain level node.

C. Scheme Discussion - We now provide a brief discussion about FH-CP-ABE scheme's features for the entities data owner and user. Here we suppose that data owner needs to share k hierarchical files with k access levels in cloud computing as we set before. Improve the part C (x,y), j about transport node in CT. All other operations execute exactly as in Basic FH-CP-ABE. In order to make a clear description, we use an example to further illustrate the improved encryption process in the step of ˆC (x,y), j of cipher text.

V. PERFORMANCE ANALYSIS

In this section, the results of theoretical analysis and experimental simulation are given. The experimental results show that the proposed scheme is highly efficient, particularly in terms of encryption and decryption.



VI. CONCLUSION

In this paper, we have suggested a mechanism of efficient encryption and decryption based on FH-CP-ABE algorithm to encrypt the original plaintext and then encrypt the secret key of symmetric algorithm. The results of experiment shows the time required for encryption and decryption is reduced. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.

VII. REFERENCES

[1]. T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "k-times attribute-based anonymous access control for cloud computing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[2]. J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Finegrained two factor access control for Web-based cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484–497, Mar. 2016.

[3]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT, pp. 457–473, May 2005.

[4]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," IEEE Symposium on Security and Privacy, pp. 321– 334, May 2007.

[5]. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," Proceedings of the 14th ACM conference on Computer and communications security, pp. 456–465, October 2007.

[6]. A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," Information Sciences, vol. 276, pp. 354–362, August 2014
[7]. C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," Advances in cryptology-ASIACRYPT, pp. 548–566, December 2002.
[8]. Z. Wan, J. Liu, and R. H. 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, April 2012.
[9]. X. Zou, "A hierarchical attribute-based encryption scheme," Wuhan University Journal of Natural Sciences, vol. 18, no. 3, pp. 259–264, June 2013.
[10]. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," Information Security Practice and Experience, vol. 5451, pp. 13–23, April 2009
[11]. An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing 1Neehal Jiwane, 2Namrata Deshmukh, 3 Pooja Shrivastav, 4 Prajakta Walde
[12]. F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, pp. 763–771, May 2014.
[13]. T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," Applied Cryptography and Network Security, vol. 5037, pp. 111–129, June 2008.