An Attribute-Based Encryption Scheme in Cloud Computing

Vaishali Mahadeo Mane[1], Suraj Shivaji Redekar[2]
[1,2]*Dept. of Computer Science and Engineering, Ashokrao Mane Group of Institutions, Vathar Tarf Vadgaon, Tal- Hatkanangale, Dist.-Kolhapur, Maharashtra, India*

Abstract **- Lately, an ever-increasing number of users and enterprises have endowed information stockpiling and stage development to proxy cloud service providers (PCSP) through the cloud innovation. In this regard, attribute-based encryption (ABE) mechanisms can compensate for the shortcomings of traditional encryption with flexible and flexible anti-collusion access policies. However, there is a security problem in the access policy, which requires files to be updated in the practical application. At ABE there are problems with over- calculation, storage costs. In this paper, an effective cipher text strategy suggests an ABE scheme with policy updates and file updates in cloud computing. The cipher text component generated by the first encryption can be shared during policy updates and file updates. Reduce client's storage and communication costs as well as PCSP computing costs. Furthermore, the proposed scheme turns out to be valid assuming a Diffie-Hellman q-parallel bilinear exponential (BDHE) solution. Finally, experimental simulations show that the proposed scheme is very effective in terms of policy updates and file updates.**

Index Terms **- Attribute-based encryption (ABE), ciphertext policy (CP), Cloud computing, file update, policy update.**

I.INTRODUCTION

With the advent of the knowledge economy and the information age, cloud computing is an inevitable product of information technology and big data time, which can lower data storage costs and reduce storage platform pressure [1] - [4]. Attribute-based encryption (ABE) [5], [6] is a promising technology to ensure comprehensive data security in cloud computing, allowing users to customize access policies, encrypt data and flexibly implement access controls. However, data owners need to apply dynamic and frequent changes to the cipher text access policy after saving data from a cloud-based proxy provider (PCSP). It has become an important topic to explore the data together.

Traditional policy updates require data owners to decrypt, then encrypt and upload the updated cipher text to PCSP. Therefore, updating the rule must perform the encryption operation twice and the decryption operation once. At the same time, there are three main problems, high computing costs, excessive communication costs, and high memory consumption when data owner interacts with PCSP. It is effective to solve the above problem better. Outsourcing policy is proposed to update the ABE mechanism (CP-ABE) of the ciphertext policy based on the linear sharing of secrets Schematic (LSSS) matrix. In the proposed scheme, we use the cipher text parameters generated by the initial encryption to update Access Policy and then upload parameters to PCSP and PCSP will be swapped to complete the remaining steps policy updates, which can avoid secondary encryption. This will increase the effectiveness of policy updates.

Further, the document ciphertext normally wishes to be upto date dynamically and frequently in an actual situation. For example, we must modify the first version of a confidential document multiple times before we get the final version. However, when we need to update the file and the policy at the same time, the unchanged policy secret value may bring some security risks.

II.RELATED WORK

In 2005, fuzzy identity-based encryption (IBE) [8] was introduced by Sahai and Waters, which was the predecessor of

the ABE. The ABE can ensure end-to-end security in cloud,

that is, data owner encrypts data through the defined access

policy and uploads to the PCSP. The ciphertext associated with access policy can be decrypted if and only if there is a "match" between the users' attributes and access policy. Later, the ABE is divided into two categories, ciphertext-policy ABE (CP-ABE) [9]–[11] and key-policy ABE(KP-ABE) [12]. In the CP-ABE mechanism, the entire ciphertext will only be saved in the PCSP, and the local need not to back up it, which is more suitable for cloud environment. If we implement policy update in the CP-ABE mechanism, data owner generally decrypts the ciphertext, and reencrypts the plaintext with the update access policy, and then, uploads the updated ciphertext to the PCSP. However, it not only causes a large amount of computational and communication costs, but also leads the PCSP to have a large storage load. To better solve the aforementioned problems, some of the ABE schemes for the dynamic policy update have been proposed. For example, Goyal et al. [12] studied how to reduce the communication and computational costs and implement key policy updates. Sahai et al. [13] adopted the ciphertext authorization method to complete the policy update. However, those methods cannot satisfy the integrity and security, because the key update and ciphertext update are limited by the old access policy. Yang et al. [14] proposed a verifiable strategy update outsourcing model in the D-ABE mechanism [15], which converts the access structure into Lewko form (LSSS matrix [16]). Thus, it reduces the size of the ciphertext set by the conversion of the access policy and improves the efficiency of encryption and decryption. Belguith et al. [17] proposed an efficient access policy update scheme based on the key policy attribute and can also capture the attribute addition of the access policy. However, data owner needs to generate the whole of the updated ciphertext. Then, Huang et al. [18] proposed an access control scheme using the ciphertext update and computation outsourcing in the field of IoT fog computing. However, it needs multiple policies to finish the encryption and policy update. And the computational cost is high for data owner. Later, Ying et al. [19] proposed a lightweight personal health record (PHR) system based on the CP-ABE strategy update. In this scheme, PHRs owners only need to generate an updating key, then upload it to the CSP instead of retrieving the entire ciphertexts. However, the PCSP needs to identify and process the updated ciphertext components, which increases the computing overhead of the PCSP

III.PROPOSED SYSTEM

Our project proposes an efficient CP-ABE scheme for policy update and file update based on the LSSS matrix access structure, which can improve the efficiency of the policy update and realize file update dynamically. Meanwhile, this scheme solves some potential security problems when we need to update the file and policy. The main contributions of project are as follows.

1) Based on an outsourcing model, this article gives an efficient policy update scheme where the PCSP undertakes the major work of the policy update. In this method, the data owner takes advantage of the initial encryption information to generate update parameters that do not require redundant encryption to be performed. It aims to reduce the computing cost of data owner, communication expense, and storage consumption of the PCSP.

2) It shows a new file update scheme, which avoids the security risks caused by the invariable secret value of the access policy during the file update and policy update. It will enhance the security of the whole scheme in practical applications and reduce the computational overhead of the data owner.

3) It avoids the duplication of files on PCSP by calculating hash value using MD-5.

4) It gives the permission to access the file for a particular time given by data owner.

5) It avoids the shoulder surfing to provide better security.

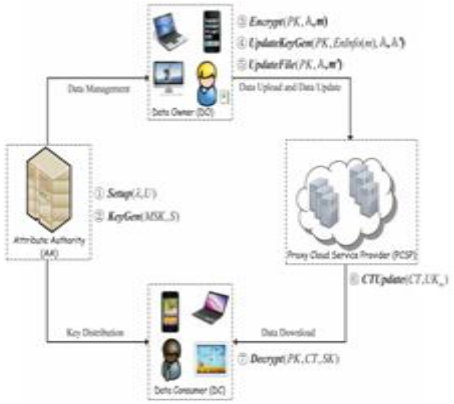
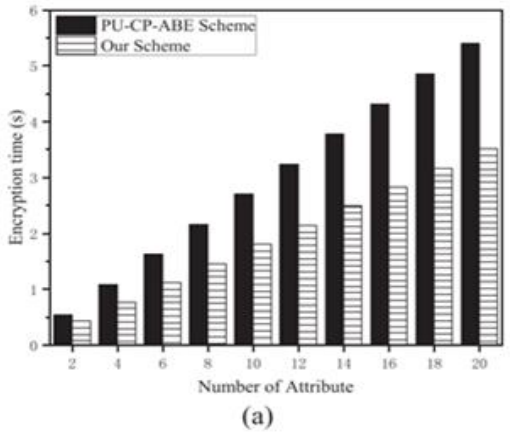


Fig 1. System model of the proposed scheme.

IV.PERFORMANCE ANALYSIS

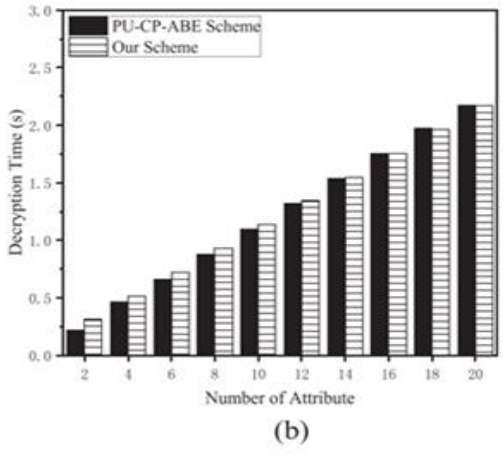
To validate theoretical analysis presented in previous sub section we implement scheme using by using ASP .NET MVC C# .NET on the Windows 10 with Intel Core processor at 3.40 GHz and 4.00-GB RAM and deploy on IIS server.

In this section, we analyze and compare the encryption time, decryption time, and policy update time between our scheme and the PU-CP-ABE scheme using following Figs. However, our theme is made by adopting the improved encryption and decryption operations.



Comparisons between our scheme and the PU-CP-ABE scheme. (a) Comparison of the encryption time cost

As illustrated in Fig. a, the period of time of the encryption operation is clearly but the PU-CP-ABE theme.



Comparisons between our scheme and the PU-CP-ABE scheme. (b) Comparison of the decryption time cost

In Fig. b, with the rise of the quantity of attributes, the coding time of our theme is gradually higher than the PU-CP-ABE scheme.

V.CONCLUSION

An effective CP-ABE scheme, it can support policy updates and file updates in cloud computing. The policy update is obtained by using the initial encrypted data to generate update parameters. It can effectively reduce the communication cost, storage cost and calculation cost of the system. At the same time, a file update model has been constructed to improve system security and reduce the calculation cost of data owners. In addition, we prove the recommendation under the assumption that q-parallel BDHE is judged, this scheme is safe. In addition, the proposed system raises some interesting open questions. For example, how to further reduce the time cost of file update and how to use blockchain technology to solve strategy update and file update.

VI.ACKNOWLEDGMENT

We are thankful to those people who help us a lot in making of this paper. This will help us to grow both academically and professionally.

VII.REFERENCES

[1] R. Li et al., “A lightweight secure data sharing scheme for mobile cloud computing,” IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344–357, Apr./Jun. 2018.

[2] J. Li et al., “Industrial Internet: A survey on the enabling technologies, applications, and challenges,” IEEE Commun. Surv. Tuts., vol. 19, no. 3, pp. 1504–1526, Thirdquarter 2017.

[3] H. Qiu et al., “A user-centric data protection method for cloud storage based on invertible DWT,” IEEE Trans. Cloud Comput., to be published, doi: 10.1109/TCC.2019.2911679.

[4] J. Li, L. Huang, and Z. Ming, “Computation partitioning for mobile cloud computing in big data environment,” IEEE Trans. Ind. Inform., vol. 13, no. 4, pp. 2009–2018, Aug. 2017.

[5] H. Xiong and J. Sun, “Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing,” IEEE Trans.

Dependable Secure Comput., vol. 14, no. 4, pp. 461–462, Nov./Dec. 2017.

[6] S. Wang et al., "An efficient file hierarchy attribute-based encryption scheme in cloud computing," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1265–1277, Jun. 2016.

[7] J. Zamite et al., "Group-based discretionary access control in health related repositories," J. Inf. Technol. Res., vol. 7, no. 1, pp. 78–94, 2014.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology-EUROCRYPT 2005, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[9] J. Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, 2007, pp. 321–334.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Workshop Public Key Cryptography, 2011, pp. 53–70.

[11] S. Wang et al., "Attribute-based data sharing scheme revisited in cloud computing," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 8, pp. 1661–1673, Aug. 2016.

[12] V. Goyal et al., "Attribute-based encryption for finegrained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[13] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Advances in Cryptology-CRYPTO 2012. Berlin Germany: Spring, 2012, pp. 199–217.

[14] K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec. 2015.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 26, no. 2, pp. 96–99, 1978.

[16] Z. Liu, Z. Cao, "On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption," IACR Cryptol. ePrint Arch., vol. 2010, pp. 374–390, 2010.

[17] S. Belguith, N. Kaaniche, and G. Russello, "PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT," in Proc. IEEE Comput. Soc. 11th Int. Conf. Cloud Comput., 2018, pp. 924–927.

[18] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," IEEE Access, vol. 5, pp. 12941–12950, 2017.

[19] Z. Ying et al., "A lightweight cloud sharing PHR system with access policy updating," IEEE Access, vol. 6, pp. 64611–64621, 2018. [20] A. Beimel et al., "Linear secret-sharing schemes for forbidden graph access structures," in Theory of Cryptography Conference. Cham, Switzerland: Springer, 2017, pp. 394–423.