Secure Keyword Search And Data Sharing Mechanism For Cloud Computing.

Nukala.Mounika Suryakala, Smt.K.R.Rajeswari, Sri.V.Bhaskara Murthy
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this paper, we describe the notion of CPAB-KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison.

I. INTRODUCTION

C LOUD computing has been the remedy to the problem of personal data management and maintenance due to the growth of personal electronic devices. It is because users can outsource their data to the cloud with ease and low cost. The emergence of cloud computing has also influenced and dominated Information Technology industries. It is unavoidable that cloud computing also suffers from security and privacy challenges.

Encryption is the basic method for enabling data confidentiality and attribute-based encryption is a prominent representative due to its expressiveness in user's identity and data [1]–[4]. After the attribute-based encrypted data is uploaded in the cloud, authorized users face two basic operations: data searching and data sharing. Unfortunately, traditional attribute-based encryption just ensures the confidentiality of data. Hence, it does not support searching and sharing. Suppose in a Person Health Record (PHR) system [5]–[7], a group of patients store their encrypted personal health reports Enc(D1; P1;KW1); _ _ _ ;Enc(Dn; Pn;KWn) in the cloud, where Enc(Di; Pi;KWi) is an attribute-based encryption of the health report Di under an access policy Pi and a keyword KWi. Doctors satisfying the policy Pi can recover the record Di. However, they could not retrieve the specific record by simply typing the keyword. Instead, a doctor Alice needs to first download and decrypt the encrypted records. After decryption, she can use the keyword to search the specific

one from a bunch of the decrypted health records. Another inconvenient scenario is that Alice attempts to share a record with her colleague, in the case like she needs to consult the report with a specialist. In this situation, she must download the encrypted files, then decrypt them. Then, after she has acquired the underlying record, she encrypts the record using the policy of the specialist. As a result, this system is very inefficient in terms of searching and sharing.

Additionally, the traditional attribute-based encryption (ABE) technology used in the current PHR systems might cause another issue for keyword maintenance because the ABE algorithm could not scale well for keyword updates once the number of the records significantly increases. For example, after reviewing a health report with the patient self marked "contagious" tag, Alice from hospital A confirmed it is not the contagious condition and corrected the tag to "non- contagious". In order for Alice to share a health report that is encrypted with a tag "contagious" with another doctor from hospital B, she need to change the tag as "non-contagious" without decrypting the report. As the traditional attribute-based encryption with keyword search can not support keyword updating, Alice has to generate a new tag for all shared ciphertexts so as to keep the privacy of the keyword. From above scenarios, the traditional attribute-based encryp- tion is not flexible for data searching and sharing. Additionally, attribute-based encryption is not well scaled when there is an update request to the keyword. In order to search and share a specific record, Alice downloads and decrypts the ciphertexts. However, this process is impractical to Alice especially when there is a tremendous number of ciphertexts. The worse situation is the data owner Alice should stay online all the time because Alice needs to provide her private key for the data decryption. Thus, ABE solution does not take the advantages of cloud computing.

An alternative method is to delegate a third party to do the search, re-encrypt and keyword update work instead of Alice. Alice can store her private key in the third party's storage, and thus the third party can do the heavy job on behalf of Alice. In such an approach, however, we need to fully trust the third party since it can access to Alice's private key. If the third party is compromised, all the user data including sensitive privacy will be leaked as well. It would be a severe disaster to the users.

II. EXISTING SYSTEM

In an ABE, the users' identities are described by a list of attributes [1]. After ABE's pioneering work [1], several scholars extended the notion of ABE. For example, key policy attribute-based encryption (KP-ABE) [2], where the private key of a user is related to an access policy and the cipher text corresponds to an attribute set. In contrast, there is another example called cipher text-policy attribute-based encryption (CP-ABE) [3], where the private key is generated with an attribute set and the cipher text is related to an access policy. In both KP-ABE and CP-ABE, the cipher text length is linear with the size of the access policy. To reduce the cipher text length, Emura et al. [8] proposed a cipher text-policy attribute-based encryption scheme with constant cipher text length. Although it supports the AND-gates on multi attributes, it doesn't support the monotonic express on attributes. After that, a number of constructions have come out to enhance the efficiency, security and expressiveness [4], [9], [10]. To illustrate the ABE's application, Li et al. [11] adopted the notion of attribute-based encryption in the PHR system to achieve fine grained access control on personal health records.

A cipher text policy attribute-based encryption with hidden policy [12] was proposed to hide the access policy which may leak the user's privacy in the PHR system. The concept of outsourcing decryption attribute-based encryption was introduced to enable a computation-constrained mobile device to outsource most of the decryption work to a service provider [13]. However, there is no guarantee that the service provider could return the correct partial decryption cipher text. To overcome this issue, Lai [14] and Li [15] proposed attribute-based encryption with verifiable outsourced decryption schemes respectively.

Proxy re-encryption was designed to delegate the decryption [16]. Prior work has focused on the scheme's functionality, efficiency, and security model [17] [18] [19], [20]. Later, Liang et al. [21] presented an attribute-based proxy re-encryption (AB-PRE) scheme by using proxy re-encryption to a attribute based setting. Meanwhile, another AB-PRE scheme was proposed to support "AND" gates on positive and negative attributes [22]. Following their work, Liang et al. [23] proposed a cipher text-policy attribute-based proxy re-encryption (CPABPRE) scheme supporting a monotonic access formula in the selective model. Later, the security has been improved in an adaptive model [24]. Ge et al. [25], [26] presented two KPABE schemes that are secure in the selective and adaptive model respectively. Liang et al. [27] proposed a deterministic finite automata (DFA) based PRE scheme, where the access policy is viewed as a DFA. Unfortunately, the privacy could not be preserved in keyword search in all of these schemes.

DISADVANTAGES

- In the existing work, the system does not provide Data integrity proof.
- This system is less performance due to lack of strong encryption techniques.

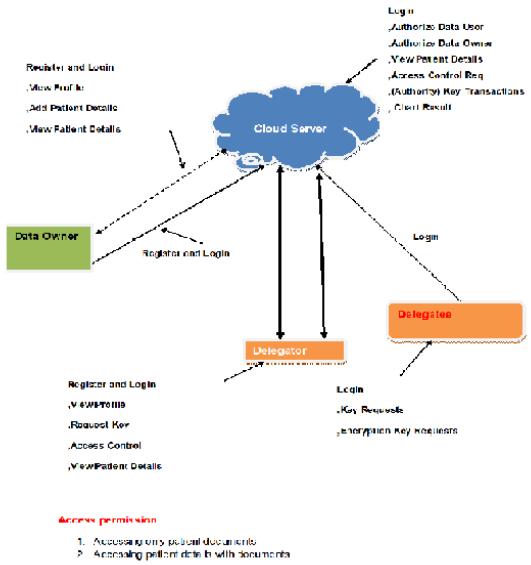
III. PROPOSED SYSTEM

The proposed system first introduces a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The searching and sharing functionality are enabled in the ciphertext-policy setting. Furthermore, our scheme supports the keyword to be updated during the sharing phase. After presenting the construction of our mechanism, we proof its chosen ciphertext attack (CCA) and chosen keyword attack (CKA) security in the random oracle model. The proposed construction is demonstrated practical and efficient in the performance and property comparison.

ADVANTAGES

- allows the data owner to search and share the encrypted health report without the unnecessary decryption process.
- supports keyword updating during the data sharing phase.
- more importantly, does not need the exist of the PKG, either in the phase of data sharing or keyword updating.
- the data owner can fully decide who could access the data he encrypted.

IV. ARCHITECTURE DIAGRAM



V. IMPLEMENTATION

- Data Owner

  In this module, the provider requests for symmetric encryption key permission from OWNER and upload the patient details in ABE with the key. View & delete the uploaded patient details, and view the clinical report from the user.

- Delegator

  In this module,Delegator register and logs in and request access control from the healthcare server and view the access control (1-access only the patient details and 2-accessing both patient details with the document), if the user has both the access permissions, user can provide the clinical report for the corresponding patient details.

- CLOUD SERVER

  The Cloud Server authorizes both user and owner, view all the uploaded patient details and give the access control permissions to the corresponding requested user. View the response from the OWNER about the key requested. After the clinical report is generated by the user forward it to the corresponding patient. And view the patient disease in chart.

- Delgatee

  In this module, the Delegatee will generate the key requested by User. And also generates the symmetric encryption key and provides permission requested by the users.

VI. CONCLUSIONS

In this work, a new notion of cipher text-policy attribute- based mechanism (CPAB-KSDS) is introduced to support keyword searching and data sharing. A concrete CPAB-KSDS scheme has been constructed in this paper and we prove its
CCA security in the random oracle model. The proposed scheme is demonstrated efficient and practical in the performance and property comparison. This paper provides an affirmative answer to the open challenging problem pointed 96 out in the prior work [36], which is to design an attribute based encryption with keyword searching and data sharing without the PKG during the sharing phase. Furthermore, our work motivates interesting open problems as well including designing CPAB-KSDS scheme without random oracles or proposing a new scheme to support more expressive keyword search.

REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Annual International

Conference on the Theory and Applications of Crypto982 graphic Techniques, pp. 457–473, Springer, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp984 tion for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98, Acm, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute988 based encryption," in Security and Privacy, 2007. SP'07. IEEE Sympo989 sium on, pp. 321–334, IEEE, 2007.

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

[5] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," International Journal of Information Security, vol. 14, no. 6, pp. 487–96 497, 2015.

[6] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryp999tion," Future Generation Computer Systems, vol. 52, pp. 67–76, 2015.

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Interactive conditional proxy re-encryption with fine grain policy," Journal of Systems and Software, vol. 84, no. 12, pp. 2293–2302, 2011.

[8] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "Aciphertext-policy attribute-based encryption scheme with constant ci1005 phertext length," in International Conference on Information Security Practice and Experience, pp. 13–23, Springer, 2009.

[9] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public-Key Cryptography–PKC 2013, pp. 162–179, Springer, 2013.

[10] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in Advances in Cryptology–CRYPTO 2012, pp. 180–198, Springer, 2012.

[11] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute1015 based encryption," IEEE transactions on parallel and distributed sys1016 tems, vol. 24, no. 1, pp. 131–143, 2012.

[12] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system," IEEE Access, vol. 7, pp. 33202–33213, 2019.

[13] M. Green, S. Hohenberger, B.Waters, et al., "Outsourcing the decryption of abe ciphertexts.," in USENIX Security Symposium, vol. 2011, 2011.

[14] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on informa1024 tion forensics and security, vol. 8, no. 8, pp. 1343–1354, 2013.

[15] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2013.

[16] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic 1028 proxy cryptography," in International Conference on the Theory and 1029 Applications of Cryptographic Techniques, pp. 127–144, Springer, 1998. 1030

[17] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy 1031 re-encryption schemes with applications to secure distributed storage," 1032ACM Transactions on Information and System Security (TISSEC), vol. 9, 1033 no. 1, pp. 1–30, 2006. 1034

[18] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure 1035 proxy re-

encryption," IEEE Transactions on Information Theory, vol. 57, 1036 no. 3, pp. 1786–1802, 2011. 1037
[19] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in 1038 Applied Cryptography and Network Security, pp. 288–306, Springer, 1039 2007. 1040
[20] C. Ge, W. Susilo, J. Wang, and L. Fang, "Identity-based conditional 1041 proxy re-encryption with fine grain policy," Computer Standards & 1042 Interfaces, vol. 52, pp. 1–9, 2017. 1043