Subashri j, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System

Subashri j, Assistant Professor D.R.krithika
Department of Computer Application -PG
VISTAS, Chennai.

Abstract- Since cloud computing has been playing an increasingly important role in real life, privacy protection in many fields has been paid more and more attention, especially in the field of Personal Health Record (PHR). The traditional ciphertext-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with the ciphertext explicitly. However, the access policy will reveal the users' privacy because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems: (1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited, and (2) the cost of decryption is especially high since the access policy is embedded in ciphertext. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

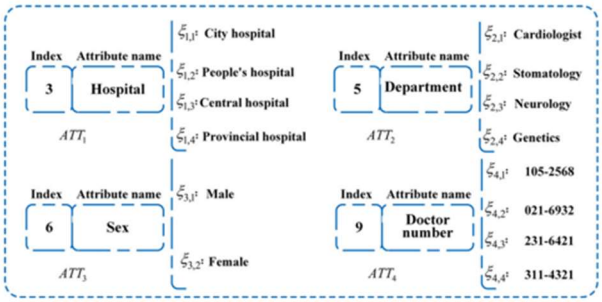
Keywords- Personal Health Record (PHR), Attribute-Based Encryption, Hidden Policy, Fast Decryption.impact.

I. INTRODUCTION

As an emerging technology in recent years, cloud computing provides a fast and efficient way to share data resources, and a mountain number of people access data through the network. For example, in the personal system health record system, a patient does not have to carry various paper versions of the test forms to make a diagnosis according to the traditional way, but he/she can store, retrieve and share the health record only by uploading his own personal health record to the PHR system. A patient has full control of his/her own PHR document and authorizes who can access their health data, such as friends, family, or healthcare providers. In order to achieve accurate access control of PHR, data owners urgently need a kind of encryption scheme that can realize fine-grained access control.

The hidden ciphertext policy attribute-based encryption scheme provides a good way to solve the problem, where it achieves privacy protection by hiding the access control policy. However, in the previous mechanisms [2], [3], [7], the access control policy is often sent along with the ciphertext explicitly, which makes it easy to reveal the users' privacy, since some attributes in the access structure carry crucial identity information of the legitimate users. In PHR, an access policy defined by a patient may contain some sensitive attributes such as cardiologist, central hospital, and so on [8], [31]. Therefore, for an unauthorized user, even if he cannot decrypt successfully, he can also infer from

the access policy in cleartext form that the encryptor suffers from some disease. The first hidden ciphertext-policy attribute-based encryption (HCP-ABE) was introduced in [16], where the access structure was embedded in the ciphertext and not sent directly. Subsequently, some other hidden CP-ABE schemes were also successively proposed in [17]– [19].



.FIGURE 1. Examples of attribute categories in PHR.

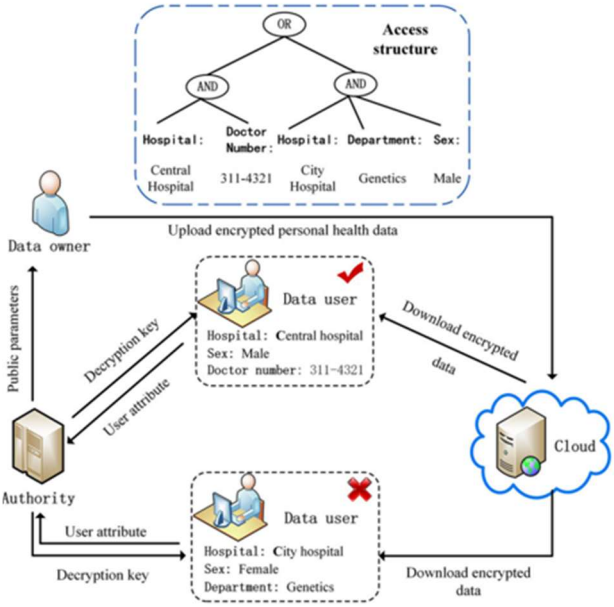


FIGURE 2. Example of PHR cloud storage.

MOTIVATION

In the context of personal health records (PHR), it is common practice to share health records (RHR) with healthcare providers. As the amount of information grows exponentially, users' personal information is often stored on third-party cloud servers. Traditional symmetric encryption relies on sensitive encryption keys and increases the risk of leaks. While public critical infrastructure provides greater security than other alternatives, there has been an explosion in the use of PHR by doctors due to the impact of developments that require security measures such as 4G and 5G.

To solve these problems, our proposed system adopts the Boneh-Franklin Identity-Based Encryption (IBE) method. Users can access the PHR using their physician ID or clinical unit ID. In a situation where the PHR is shared by multiple parties, recipients can jointly decrypt the ciphertext without having to regenerate the decryption key. Instead, when shared with a provider, they can use multiple devices for decryption to ensure that loss or damage to one device does not compromise the private key. Additionally, the decentralized decryption protocol has unequal participants. When physicians in a department need access to a patient's PHR, they can calculate the G group equivalent.

This method is especially suitable for lightweight wireless networks such as smartphones and tablets. Managers have greater computational and storage capacity and play an important role in the decryption process, allowing them to decrypt ciphertext with relative ease.

In summary, our method uses the Boneh-Franklin IBE concept to increase the security of shared PHR. It is suitable for situations where there are many buyers or a single doctor, providing convenience and security. The decentralized decryption process aggravates the efficiency of the equipment, with administrators assuming greater responsibility for providing secure and easy access to encrypted PHRs

II. PROPOSED CONTRIBUTION

In recent years, with the rapid development of the internet and cloud computing, a mountain number of Intelligent Medical Systems have been designed. However, in the previous mechanisms based on attribute encryption, access control policies are often sent along with the ciphertext, which makes it easy to reveal the sensitive information of users in the system. Especially, in PHR, the specific attribute values in an access policy carry much more sensitive information, such as the patient's pulse frequency, their family history of hereditary diseases, the result of the patient's laboratory test report, and so on. In

order to deal with the above problems, our contributions mainly include the following three part Access structure:

Each attribute in this paper contains two parts: the attribute name index and its attribute value. And each attribute has multiple candidate values. Every decrytor only knows the attribute name index of its own and its attribute value. Moreover, the values of the attributes in the access policy defined by the encryptor are hidden, and they are not sent with the ciphertext. Only the access matrix and the defined function ρ are sent to the decryptor along with the ciphertext. What's more, the proposed scheme can handle any access control policy that can be expressed as a linear secret sharing scheme.

Fast decryption:

Obviously, it is hard for a user to know whether his attribute set satisfies the access policy defined by the encryptor if the access policy associated with a ciphertext is fully hidden. Therefore, a decryptor has to do a lot of calculations to determine whether he is legal or not. In this paper, we present an efficient construction of Hidden Ciphertext Policy Attribute-Based Encryption that Supports Fast Decryption, where the number of bilinear pairing evaluations is reduced to a constant in the decryption phase.

Data verifiability

In most previous schemes, there are usually two practical problems that deserve to be considered. one is that the size of the public parameters increases linearly with the size of the universe. And the other is that the authorized user cannot determine whether the message he obtained through decryption is valid or not, because there is no verifiable link to the message. However, in the proposed scheme, the size of public parameters is constant, so the attribute universe in this scheme can be exponentially large and it also supports validation of decrypted messages, which can further improve the reliability of decryption. Furthermore, we also prove the full security of the proposed scheme in the standard model under static assumptions by using the dual system encryption method

Organization

The remainder of the paper is structured as follows. In section 2, some preliminary concepts are introduced, such as composite-order bilinear map, access structure, and complexity assumptions. We describe the definition of our proposed algorithm and its security model in Section 3. The specific structure of the proposed scheme is presented in section 4. Section 5 is a detailed description of the full security proof. Finally, we give a brief conclusion and performance analysis of the proposed scheme.

III. RELATED WORK

Title: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization.

Author: B. Waters. We propose a new way to implement Ciphertext Policy Associated Encryption (CPABE) in the standard model promise, and interaction-free cryptographic perspective. Our solution allows any domain author to define access controls based on access patterns for physical objects. On our most efficient machine, ciphertext size, encryption, and decryption time scale linearly with the complexity of the input model. The only previous study using these parameters was limited to evidence at international standards. We present our model in our framework. Our initial system has been shown to be secure under what we call the Parallel Bilinear Diffie-Hellman Decision Exponent (PBDHE) assumption, which can be viewed as the BDHE assumption. Our next two models provide trade-offs to ensure stability under the (weakly) deterministic-bilinear Diffie-Hellman exponential and deterministic-bilinear Diffie-Hellman assumptions, respectively.

Title: Fuzzy identity-based encryption.

Author: A. Sahai and B. Waters.

We introduce a new identity-based encryption (IBE) method, which we call fuzzy identity-based encryption. In Fuzzy IBE, we treat identity as a descriptive process. The concept of fuzzy IBE allows the private key of identity Ï to decrypt a ciphertext encrypted with identity Ï 0 if and only if the symbols Ï and Ï 0 are close to each other (in measure) - set overlap - measure distance. Fuzzy IBE schemes can be used to use biometric devices as tokens for encryption; The flaw in the breakdown of IBE plans is that they allow the use of biometric beacons designed to create some noise every time they are checked. We also show that Fuzzy-IBE can be used in a class of applications that we call "character-based

encryption." In this paper, we propose the construction of two fuzzy IBE schemes. Our structure can be viewed as an identity-based encryption of messages of various qualities that make the identity (fuzzy). Our IBE concept is both fault- and crash-tolerant. Also, our simple structure does not use random oracles. We demonstrate the security of our offering based on the chosen identity security model
Title: Ciphertext-policy attribute-based encryption.
Author: J. Bethencourt, A. Sahai, and B. Waters
In some deployments, users should only be able to access data if they have certain credentials or attributes. Currently, the only way to implement such a policy is to use a trusted server to store information and control access. However, if a server storing data is compromised, the confidentiality of the data may also be compromised. In this article, we want a process for using complex access to encrypted data, which we call encryption based on ciphertext policy behaviour. Using our technology, encrypted data can be kept private even if the storage is not trusted; Additionally, our methods are safe from accidents. Previous attribute-based encryption systems used attributes to identify encrypted data and establish authority for the user's key. In our system, attributes are used to identify the user's credentials, and the party encrypting the information decides who can decrypt it. Therefore, our approach is conceptually closer to traditional access control methods such as role-based access control (RBAC). We also provide system implementation and performance evaluation.
Title: Security and privacy in smart health: Efficient policy- hiding attribute-based access control.
Author: Y. Zhang, D. Zheng, and R.H. Deng.
With the rapid development of the Internet of Things (IoT) and cloud computing technology, smart health (health) is expected to improve the quality of healthcare services. However, data security and user privacy issues have not yet been fully addressed. As a well-received quality control solution, Ciphertext Policy Attribute-Based Encryption (CPABE) is capable of ensuring data security in the case of health. However, there are two disadvantages to directing CPABE in healthcare. On the other hand, the right of access is clear text and disclosure of health-related information in encrypted health records (SHRs). On the other hand, it often favours small objects in the world, which leads to an unacceptable limitation of the use of CPABE because the size of its population does not increase linearly with the size of the responded world. To solve these problems, we introduce PASH, a privacy-aware healthcare management system where the main object is a macrocosmic CP-ABE whose access policy can be partially hidden. In PASH, the code to access the useful character is hidden in the encrypted SHR and only reveals the name of the character. In fact, character values carry more sensitive information than list names. In particular, PASH uses a good SHR decryption test that requires bile line matching. While the main character may be size, the size of the population is small and not regular. Our security tests show that PASH is completely secure in the standard format. Performance comparison and experimental results show that PASH is more effective and more meaningful than previous solutions.

IV. FUTURE WORK

In Hidden Cipher Policy Attribute- Grounded Encryption(HCP-ABE) for Personal Health Records(PHRs) includes enhancing decryption effectiveness through optimized algorithms and scalability advancements for large-scale systems. sequestration advancements should concentrate on minimizing information leakage and supporting dynamic access control mechanisms.

V. CONCLUSION

This paper proposed a new technology called "multivalued linear secret sharing" that aims to improve access to information. It is worth noting that each property is divided into two parts: the property name and its corresponding value. This unique feature provides clear benefits as it allows hiding of valuable behaviour and ensures optimal protection of user privacy in Personal Health Information (PHR). The proposed strategy keeps the size of the population fixed and constant with the decryption cost limit for both operations. In addition, this paper uses the dual system encryption method to ensure the full security of the original theory as well as the proposed scheme in the standard model. While the

proposed strategy achieves partial obfuscation, the interesting challenge lies in using solutions that provide full obfuscation while also encrypting quickly. This remains an interesting area for future research, indicating a continued commitment to improving privacy, especially in the context of PHRs.

Acknowledgement

We would like to extend our sincere gratitude to our guide, Associate Professor Dr. M. Sravan Kumar Reddy, MTech, whose unvarying guidance, support, and moxie have been necessary in the successful publication of this specialized Technical paper.
He fidelity to nurturing our exploration chops and his perceptive feedback have been inestimable throughout this trip. I'm also deeply thankful to the entire Computer Science and Engineering Department at RGMCET for furnishing a conducive terrain for academic growth and for the inestimable benefactions of its speakers. Their stimulant and mentorship have played a significant part in shaping our scholarly hobbies.

REFERENCES

1. B. Waters, "Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions," in Advances in Cryptology CRYPTO (Lecture Notes in Computer Science), vol. 5677, S. Halevi, Eds. Berlin, Germany: Springer, Aug. 2009, pp. 619–636.
2. M. Qutaibah, S. Abdullatif, and C.T. Viet, "A Ciphertext-Policy Attribute-Based Encryption Scheme With Optimized Ciphertext Size And Fast Decryption," in Proc. 2017 ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS), Apr. 2017, pp. 230–240.
3. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography PKC(Lecture Notes in Computer Science), vol. 6571. Berlin, Germany: Springer, Mar. 2011, pp. 53–70.
4. V. Goyal, O.Pandey,A.Sahai, and B. Waters,"Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf.Comput. Commun. Secur. (CCS), Nov. 2006, pp. 89–98.
5. J. Lai, R.H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," in Proc. 7thACMSym. Infor., Comput, Commun. Secur., May. 2012, pp. 18–19.
6. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Eds.Berlin, Germany: Springer, May 2005, pp 457–473.
7. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy(SP), May 2007, pp.321– 334.
8. Y. Zhang, D. Zheng, and R.H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018
9. H. Cui, R.H. Deng, G. Wu, and J. Lai, "An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures," in Provable Security PROVSEC (Lecture Notes in Computer Science), vol. 10005, L. Chen, Eds. Berlin, Germany: Springer, Nov. 2016, pp.19–38.
10. C.Y. Umesh, "Ciphertext-policy attribute-based encryption with hiding access structure," in IEEE Inter.Adv.Comput. Conf. (IACC), Jul 2015, pp. 6–10.
11. L. Zhang and Y. Hu, "New Constructions of Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Computing," KSII Transactions Internet J., vol. 7, no. 5, pp. 1343–1356, May. 2013.
12. J. Li, K. Ren, B. Zhou, and Z. Wan, "Privacy-Aware Attribute-Based Encryption with User Accountability," in Information Security—PROCEEDINGS (Lecture Notes in Computer Science), vol. 5735, P. Samarati, Eds. Berlin, Germany: Springer, Sep. 2009, pp.347–362.
13. J. Li, H. Wang, Y. Zhang, and J. Shen, "Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing," KSII Transactions Internet J., vol. 10, no. 7, pp. 3339–3352, Jul. 2016.
14. Y. Zhang, X. Chen, J. Li, and D. Wong, "Anonymous attribute-based encryption supporting efficient decryption test," in Proc. 8th

ACM Sym. Infor, Comput. Commun. Secur. (SIGSAC), May. 2013, pp. 511–516.

15. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A Ciphertext Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length," in Infor. Secur.Prac., Experience—ISPEC (Lecture Notes in Computer Science), vol. 5451, F. Bao, H. Li, Eds. Berlin, Germany: Springer, Sep. 2009, pp.13–23.
16. T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures," in Applied Cryptography and Network Security—ACNS (Lecture Notes in Computer Science), vol. 5037, S.M. Bellovin, R. Gennaro, Eds. Berlin, Germany: Springer, Sep. 2009, pp.13–23.
17. T.V. Phoung, G. Yang, and W. Susilo, "Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions," IEEE Trans. Information Foren. Security, vol. 11, no. 1, pp. 35–45, Sep. 2015.
18. C. Jin, X. Feng, and Q. Shen, "Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size," in Proc. Inter. Conf., Commun. Netw. Secur. (ICCNS), Nov. 2016, pp. 91–98.
19. Q. Wang, L. Peng, H. Xiong, and J. Sun, "Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing," IEEE Access J., vol. 6, pp. 760–771, Nov. 2017.
20. P. Chaudhari, M.L. Das, and A. Mathuria, "On Anonymous Attribute-Based Encryption," in Information Systems Security—ICISS (Lecture Notes in Computer Science), vol. 9478, S. Jajoda, C. Mazumdar, Eds. Cham: Springer, Dec. 2015, pp.378–392.
21. Hou, Jie, and Terry Gao. "A method of shear line detection in vector fields based on descriptive statistics of circular data." Multimedia Tools and Applications 81.15 (2022): 20853-20870.
22. Hou, J., & Gao, T. (2022). A method of shear line detection in vector fields based on descriptive statistics of circular data. Multimedia Tools and Applications, 81(15), 20853-20870.
23. Mahto, Dashrath, and Subhash Chandra Yadav. "Hierarchical Bi-LSTM based emotion analysis of textual data." Bulletin of the Polish Academy of Sciences Technical Sciences (2022): e141001-e141001.
24. Mahto, D., & Yadav, S. C. (2022). Hierarchical Bi-LSTM-based emotion analysis of textual data. Bulletin of the Polish Academy of Sciences Technical Sciences, e141001- e141001. [25]. Kumar, Vinit, et al. "Secure Deep Learning Framework for Cloud to Protect the Virtual Machine from Malicious Events." Wireless Personal Communications 131.3 (2023): 1859-1879.