IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134119

HIDDEN CIPHER POLICY ATTRIBUTE BASED ENCRYPTION WITH FAST DECRYPTION ON PERSONAL HEALTH RECORDS

Dr. M. Sravan kumar Reddy[1], K. Snehitha[2], V. Anish[3], G V S Dharani[4], S. Pavan[5]

Associate Professor in Dept. of CSE in RGMCET, Nandyal[1]

Department Of Computer Science Engineering, Student in RGMCET, Nandyal[2-5]

Abstract: Pall computing has surfaced as a revolutionary means of data sharing, enabling a vast number of individualities to pierce information over networks fleetly and efficiently. In surrounds similar as particular health record(PHR) systems, the traditional burden of carrying colorful paper documents for judgments has been soothed. rather, cases can upload their health records to PHR systems, granting them the capability to store, recoup, and widely partake their data with authorized parties, including musketeers, family, and healthcare providers. The necessity for precise access control in PHRs has urged a demand for encryption schemes able of enforcing fine- granulated access control.

Retired ciphertext policy trait- grounded encryption(HCP- ABE) is a promising result to this challenge by cache access control programs within ciphertext, by enhancing sequestration protection. Unlike before mechanisms where access control programs were frequently transferred along with ciphertext, facing a threat to druggies' sequestration, HCP- ABE embeds the access structure directly into the ciphertext. This prevents unequivocal exposure of sensitive attributes similar as" cardiologist" or" central sanitarium" contained within access programs, which could unintentionally reveal a case's medical condition to unauthorized druggies.

While the preface of HCP- ABE addresses sequestration enterprises, being schemes aren't without limitations. numerous of these schemes support only introductory sense gates similar as AND gates or combinations of positive, negative, and wildcard attributes. Accordingly, two significant downsides arise an increase in the size of public parameters commensurable to the number of attributes, and a substantial rise in decryption costs. To alleviate these issues, low- overhead schemes have been proposed. These schemes generally incorporate decryption tests involving the addition of spare factors to ciphertext before decryption. While this approach enhances decryption effectiveness, it also results in a significant increase in ciphertext length, potentially hindering overall performance.

Sweats to optimize encryption schemes for PHRs must strike a balance between security and effectiveness. The exploration and development are necessary to address scalability and performance enterprises while icing strict access control and sequestration preservation. By these challenges, pall computing technologies can continue to transfigure data operation practices, particularly in sensitive disciplines like healthcare, fostering trust and confidence among druggies and easing wide relinquishment**.**

TERMS : Personal Health Records(PHR),Attribute-Based Encryption, Hidden Policy, Fast Decryption

I. INTRODUCTION

In recent years, cloud computing has emerged as a transformative technology, providing a rapid and efficient means for widespread data resource sharing. A substantial number of individuals now access data through networks,exemplified by innovations like Personal Health Record (PHR) systems. Unlike traditional methods where patients had to carry various paper forms for diagnoses, cloud-based PHR systems enable users to store, retrieve, and share health records seamlessly. Patients have complete control over their PHR documents, determining who can access their health data, including friends, family, or healthcare providers. To ensure precise access control in PHR systems, there is a pressing need for encryption schemes capable of fine- grained control. The Hidden Ciphertext Policy Attribute- Based Encryption (HCP-ABE) scheme addresses this need, offering a solution that safeguards privacy by concealing access control policies.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.134119

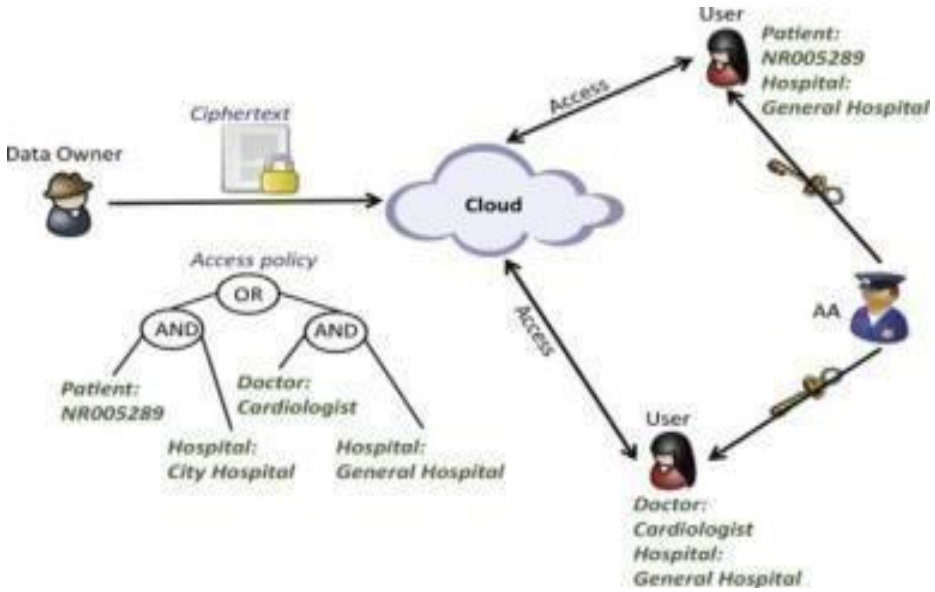
However, shortcomings in prior mechanisms have been identified, particularly the explicit inclusion of access control policies with ciphertext. This practice poses a risk to user privacy since certain attributes within the access structure may divulge critical identity information.

In the context of PHRs, access policies established by patients may contain sensitive attributes such as the involvement of a cardiologist or association with a central hospital. Even if an unauthorized user fails to decrypt the information, they may still infer details about the encryptor's health condition from the access policy in cleartext form.

The inception of HCP-ABE in , embedding the access structure in the ciphertext instead of transmitting it directly, marked a significant advancement. Subsequent schemes extended this approach, but limitations persisted. These schemes typically supported only AND gates or AND gates with positive, negative, and wildcard attributes in their access structures, resulting in two major drawbacks. Firstly, the size of public parameters escalated linearly with the number of attributes. Secondly, the decryption cost saw a substantial increase.

In response to these challenges, low-overhead schemes were introduced ([13]– [14]). These schemes commonly adopted a strategy of introducing a decryption test by appending redundant components to ciphertext before the decryption stage. While these innovations improved decryption efficiency, they simultaneously increased the length of ciphertext, becoming a bottleneck for achieving higher performance. Moreover, these schemes were found to be highly susceptible to decisional Diffie-Hellman test (DDH-test) attacks.

In summary, the evolving landscape of cloud computing, particularly in PHR systems, has prompted the development of encryption schemes with fine-grained access control. While HCP-ABE addresses privacy concerns, subsequent schemes have grappled with limitations in access structure support, parameter size, and vulnerability to attacks, prompting the exploration of alternative solutions.



A. 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.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134119

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.

B. OUR CONTRIBUTION

In recent years, with the rapid development of the internet and cloud computing, many smart medical systems have emerged. However, existing methods for character-based encryption often increase privacy risks by sending access control codes along with the ciphertext. This practice raises concerns that special benefits in access rights, especially when it comes to personal health records (PHRs), could reveal important information such as a patient's heart rate, family history of genetic diseases, or laboratory tests.

To solve these problems, our contribution can be divided into three main parts:

Access structure: A feature in our scheme consists of two parts - a custom feature name index and many competitor prices. It is worth noting that the value of each property in the access code defined by the encryptor remains secret and is not sent along with the ciphertext. Just enter the matrix and the specified Ï function in ciphertext. More importantly, our scheme can be adapted to any access control policy, expressed as a shared privacy scheme.

Fast Decryption: Given the complete secrecy of the access code associated with the ciphertext, it becomes difficult for the decryptor to determine the truth of its behaviour. To solve this problem, we propose a well- designed encryption-based ciphertext policy that supports fast decryption. Our strategy reduces the number of bilinear tests to be continuously performed during decryption.

Proof: Unlike previous solutions, our solution solves two problems. First, the size of the difference remains constant, avoiding linear growth with the size of the world. Second, authorized users can verify the validity of the decrypted message and increase the reliability of decryption. Additionally, in the model based on static theory, we ensure the full security of our scheme by using two encryption methods.

Security Analysis: Perform a comprehensive security analysis of the HCP-ABE scheme based on cryptographic techniques. This includes evaluating its resistance to various cryptographic attacks and ensuring that it meets security requirements such as confidentiality, integrity and accuracy.

In summary, we aim to improve privacy in smart healthcare, especially PHRs, by hiding useful features, enabling them, and ensuring that evidence from large populations is immutable. . The scheme contributes to the overall trust of encrypted data processing by providing security in the standard model.

C. Organization

We comprehensively examine data on electronic personal health information sharing and identity-based encryption methods. Section III details the notation, Boneh-Franklin Identity-Based Encryption (BF-IBE) scheme, mathematical assumptions, and basic structure. Section 4 introduces our decentralized decryption method based on BF-IBE, and Section 5 introduces the security analysis. Section VI presents the results of our analysis. We also continue our planning for the initial (t, n) secret expression, which will be discussed in Section VII. The article concludes with a final section that summarizes the main insights and conclusions presented.

II. 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.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.134119

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 (CP-ABE) is capable of ensuring data security in case of health. However, there are two disadvantages to directing CP-ABE in healthcare. On the other hand, the right of access is cleartext 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

III. 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).

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134119

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.

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.

The privacy sweats are demanded to integrate HCP- ABE with being healthcare systems, while usability studies can guide the development of stoner-friendly interfaces. also, rigorous security analysis and compliance with nonsupervisory fabrics like HIPAA and GDPR are essential for icing the adaptability and legitimacy of HCP- ABE results in healthcare settings.

V. ACKNOWLEDGEMENT

We would like to extend our sincere gratefulness 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,andB.Waters,“Attribute- based encryption for fine grained access control of encrypted data,”inProc.13thACMConf.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,” inProc. 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,May2005,pp.457–473.

[7]. J.Bethencourt, A.Sahai,and B.Waters,“Ciphertext- policy attribute based encryption,”inProc. IEEE Symp. Secur. Privacy(SP), May2007, 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.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134119

[12]. J. Li, K. Ren, B. Zhou, and Z. Wan, "Privacy- Aware Attribute Based Encryption with UserAccountability," 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 AttributeBased 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* (LectureNotes 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.

