Maintenance of Personal Health Record System with Cipher text Policy Attribute-Based Encryption and Quick Decryption

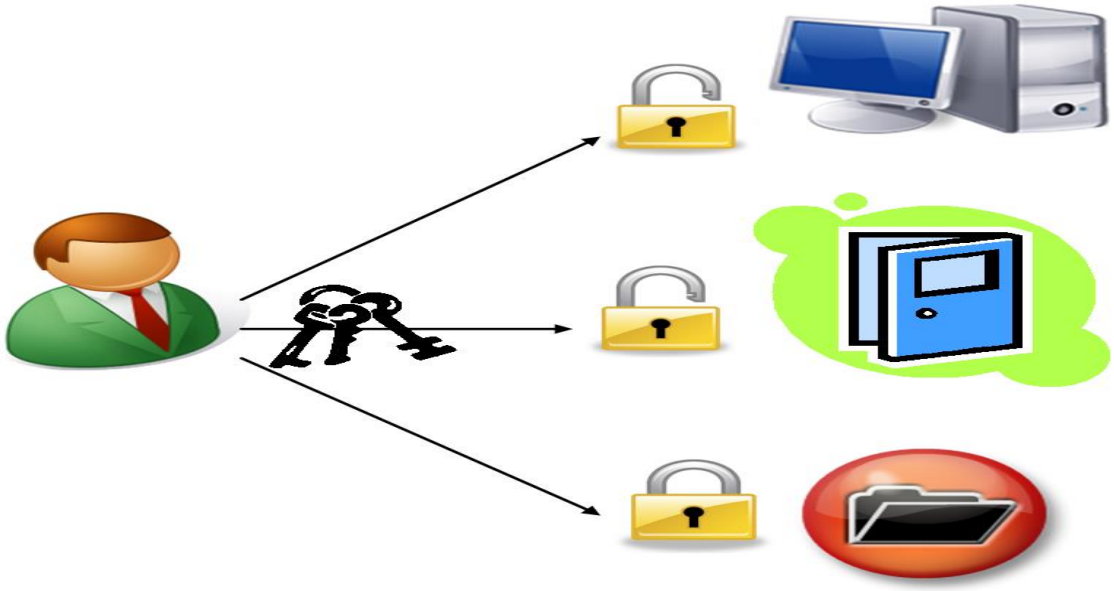
T Jayasri #1, Ambala Mounika #2, Mukka Manasa Manvitha #3, Shaik Shalima #4, Jajula Anil #5
#1Asst. Professor, #2,3,4,5 B.Tech.., Scholars
Department of Computer Science and Engineering,
QIS College of Engineering and Technology

ABSTRACT:
The meteoric rise of information technology coupled with the pervasive use of cloud computing across all industries has prepared the road for the implementation of Personal Health Record (PHR) Systems using cloud computing. The greatest example to utilise is Microsoft Healthvault, which is an online personal health record service offered by the technology giant Microsoft. This service allows users to save, access, and update their personal information, which can then be shared with health care professionals. Some people believe that shifting applications that deal with personal data to cloud computing might result in a loss of control over the data. Therefore, it is essential to have PHR systems that are safe and stored on the cloud. Several frameworks for PHR have been developed, several of which make use of conventional cryptographic methods. However, they are not suitable for the PHR systems since they do not meet the requirements for efficiency, scalability, and appropriateness. Nicely addition, the single owner scenario of standard cryptographic approaches does not fit in with the multi-owner situation of the PHR system. As a result, we propose a PHR framework in which patients have access control and privacy of their personal record using a light weight 64 bit block cypher symmetric encryption algorithm. Additionally, we propose dividing the patient-centric framework into multiple security domains in order to reduce the complexity of key distribution. The plan that has been suggested is adaptable since it enables for break glass judgements to be made in the event of an emergency situation. However, the system does not have integrity, which is something that may be maintained by utilising a digital signature method or an Elliptic Curve Digital Signature Algorithm (ECDSA) scheme to establish integrity of the personal health information.

1. INTRODUCTION

The rapid expansion of cloud computing can be traced back to the fact that it has become an essential component of the day-to-day operations of businesses of all sizes, both the most modest and the most sizable. Recent findings from a poll that was carried out by Forbes [1] indicate that close to 75 percent of corporate customers are now making use of cloud platform in some capacity or another. Cloud storage is the most essential feature that is made accessible to

customers on this platform. Users are able to store a big quantity of data and access it anywhere, anytime, and on demand using cloud storage. Before the advent of modern technology, a patient's medical history was recorded on paper and kept in a filing cabinet. The data were eventually digitised as a result of the expansion of information technology. In a similar manner, information pertaining to medical care was converted into a digital format and stored in electronic health records. These records include specifics regarding a patient's medical history and were previously only accessible to professionals working in the medical field, such as insurance agents, doctors, and physicians. Patients (i.e., people) consequently have a requirement for a Personal Health Record, which enables patients to store, access, and maintain their personal records and efficiently share them with health care professionals when necessary. This is in stark contrast to the electronic health care records that are maintained by hospitals and other health care institutions. The most reliable examples of online personal health record service providers are Microsoft Healthvault and Google Vault. [Citation needed] [Citation needed] However, the proliferation of cloud computing as a platform for the centralised storage and administration of personal health records (PHR) has also brought up concerns about security and privacy. As a result, various standard cryptographic approaches such as symmetric cryptography using algorithms such as AES and public key cryptography using algorithms like as RSA have been suggested for usage as a means of ensuring data privacy and integrity when it is shared across PHR systems. However, the requirement for privacy is the primary worry in a PHR system since patients risk losing control over their own personal health data when it is stored on the cloud. We propose a PHR framework where the patients are the owners, and they are responsible for creating the decryption key using Attribute Based Encryption, and they share the key with authorised users, such as doctors and health care personnel, in order to overcome the difficulties of privacy leakage caused by cloud providers. Additionally, the suggested frameworks guarantee that each data owner has complete control over their information. The system is broken up into several security domains, and each security domain has its own unique users and properties that serve as encryption primitives. This further simplifies the process of key distribution among a large number of owners.



2. RELATED WORKS

Traditional policies for controlling access based on roles RBAC was largely used in PHR systems in order to more precisely control who is allowed access to the electronic health record. Access control was given in RBAC according to the roles that were performed and the privileges that came with those roles, as shown in [2]. Di Vimercati recommended the use of symmetric key cryptography, in which personal health data would be encrypted using symmetric encryption methods and stored on a server that was only partially trustworthy. However, the approach that was offered had a number of limitations, including access control rights sharing and user revocation in [3]. In a later stage of the process, solutions based on public key cryptography were taken into consideration. Benaloh came up with the idea for a PHR framework, which supports the idea that encryption, in conjunction with access control, is required to provide both privacy and security. They have done this by using a hierarchical identity-based encryption system, in which each label is treated as if it were an identity in and of itself. Nevertheless, the procedure that was suggested in [4] still had the possibility of having considerable key management overhead. Dong suggested doing a keyword search on encrypted data while utilising proxy encryption [5]. If every read and write action goes via a proxy server, then access control may be effectively implemented. However, this approach was not without its shortcomings in terms of controlling fine grain. The usage of Multi-Source Order-Preserving Symmetric Encryption (MOPSE), which employs a privacy-preserving symmetric encryption algorithm, was explored by Yao et al. The data owners, who represent the patients (and the physicians), encrypt the files containing their medical information and then upload them to the PHR cloud. This allows the patients' medical records to be shared with cloud data consumers. Cloud data consumers, who represent physicians (and patients), download encrypted PHR files from the PHR cloud in order

to access the shared PHR data files. After downloading the files, cloud data consumers decrypt the files in order to reuse the file for various healthcare requirements.

3. **SYSTEM ANALYSIS**:

In a CP-ABE, the user's attributes used for key generation must satisfy the access policy used for encryption in order to decrypt the ciphertext, whereas in a KP-ABE, the user can only decrypt ciphertexts whose attributes satisfy the policy embedded in the key. This is because in a KP-ABE, the policy is embedded in the key. It is clear that access control is an integral part of ABE, and we can see that in order to do effective fine-grained access control, we need to make use of certain expressive access structures. After then, the realisable (or monotone) access structure that was introduced by the Linear Secret Sharing Scheme (LSSS) was used by a great number of subsequent ABE schemes. Cheung and Newport came up with an additional method to create access structure based on the combination of AND-Gate and wildcard. Cheung and Newport shown that in order to design CP-ABE schemes based on normal complexity assumptions, one just has to make use of this straightforward access structure, which is enough for a wide variety of applications. In the years that followed, a number of other ABE systems were suggested that adhered to this particular access pattern.

DISADVANTAGES:

- The currently implemented ABE schemes that are based on AND-Gate with wildcard are unable to accomplish this attribute.
- Although ABE performs a good job of preventing unauthorised access to the data that has been encrypted, it does not safeguard the privacy of the people who are receiving or decrypting the data by default. In other words, if they have access to the ciphertext, an unauthorised user could still be able to gain some information about the data receivers.
- Despite the fact that a trustworthy ABE is capable of effectively preventing unauthorised access to the data that has been encrypted, it does not, by default, safeguard the privacy of the receivers or decryptors of the data.

PROPOSED SYSTEM:

In this study, we investigate novel methods for the creation of CP-ABE schemes that are based on the AND-gate with wildcard access structure. The currently implemented schemes of this kind are required to make use of three distinct components in order to accurately represent the positive, negative, and wildcard values that may be assigned to an attribute in the access structure. Within the scope of this work, we offer a novel architecture that makes use of a solitary element to symbolise a single feature. Our structure is predicated on the assumption that the "positions" of various symbols may be used to conduct the matching function that is required between the access policy and the user characteristics. To be more specific, we organise the indices of all the positive, negative, and wildcard attributes defined in an access structure into

three sets. Then, with the help of the method of Viète's formulas, we make it possible for the decryptor to get rid of all the wildcard positions and carry out the decryption in a correct manner if and only if the remaining user attributes match those defined in the access structure. This ensures that the decryption is carried out in a secure

ADVANTAGES

- The use of our novel method results in a brand-new CP-ABE scheme that maintains a consistent ciphertext size.
- The technique has been utilised in the initial build to bridge ABE based on AND-Gate with wildcard using Inner Product Encryption (IPE).
- Our first scheme is successful in maintaining a constant ciphertext size.
- Guaranteed to be safe according to both the Decisional Bilinear Diffie-Hellman and the Decision Linear hypotheses.

4. **IMPLEMENTATION**:

Owner:

The Owner Will Sign Up, After Which They Will Await Authorization (The Key) From Admin. Once the key has been obtained, the owner can log in using the key and upload any personal file to the cloud. This file will be encrypted using ABE with wildcard characters. The Owner is responsible for monitoring the upload's progress status and will do so on their own. Ensure that the owner logs out of the session.

User:

The user must register, and then they must wait for the permission (key) from the admin. The user will log in and access the file with the same characteristic in order to decode it. Users are able to both see the file and download the file. The user should logout of the session.

Admin:

Admin will log in on the page designated for admins. Pending requests from any of the aforementioned individuals will be reviewed by him/her. Administrators should check the user's download and session history for potential future referrals Admin logout session

5. **CONCLUSION**

In this article, we provide a unique access management mechanism that acknowledges patient-centric privacy concerns for electronic personal health information stored in the cloud. Taking into consideration the fact that cloud servers are only partially reliable, our argument is that patients should have complete control over their own privacy by encrypting their PHR documents in order to permit fine-grained access. The structure addresses the particular

difficulties posed by the presence of a large number of PHR owners and users in the sense that it significantly reduces the degree of unpredictability associated with key management in situations in which the number of owners and users participating in the framework is very high. We encrypt the protected health information (PHI) using a lightweight form of symmetric encryption so that patients can give access to their PHR not only to personal users but also to users from a variety of public domains who have a wide range of professional backgrounds, capabilities, and affiliations.

REFERENCES

[1] M. Abdalla, A. De Caro, and D. H. Phan, "Generalized key delegation for wild carded identity-based and inner-product encryption," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1695–1706, Dec. 2012.

[2] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Berlin, Germany: Springer-Verlag, 2011, pp. 90–108.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321–334.

[4] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in Proc. 21st Annu. Int. CRYPTO, 2001, pp. 213–229.

[5] C. Chen et al., "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in Topics in Cryptology (Lecture Notes in Computer Science), vol. 7779, E. Dawson, Ed. Berlin, Germany: Springer-Verlag, 2013, pp. 50–67.

[6] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," in Proc. 5th Int. Conf. Provable Secur. (ProvSec), 2011, pp. 84–101.

[7] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 456–465.

[8] N. Doshi and D. Jinwala, "Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext," in Proc. Int. Conf. Adv. Comput., Netw. Secur., 2012, pp. 515–523.

[9] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in Proc. 5th Int. Conf. ISPEC, 2009, pp. 13–23.

[10] A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang, "Threshold ciphertext policy attribute-based encryption with constant size ciphertexts," in Proc. 17th Austral. Conf. Inf. Secur. Privacy, 2012, pp. 336–349.

[11] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proc. 35th Int. Colloq. Auto., Lang. Program. (ICALP), 2008, pp. 579–591.

[12] 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), 2006, pp. 89–98.

[13] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in 13th PKC, 2010, pp. 19–34.

[14] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. Theory Appl. Cryptogr. Techn. 27th Annu. Int. Conf. Adv. Cryptol. (EUROCRYPT), 2008, pp. 146–162.

[15] J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding CP-ABE," in Proc. 7th Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), 2011, pp. 24–39.

[16] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. 24th Annu. Int. EUROCRYPT, 2010, pp. 62–91.

[17] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in Proc. 32nd Annu. Conf. CRYPTO, 2012, pp. 180–198.

[18] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in Proc. 12th Int. Conf. Inf. Secur. (ISC), 2009, pp. 347–362.

[19] X. Li, D. Gu, Y. Ren, N. Ding, and K. Yuan, "Efficient ciphertextpolicy attribute based encryption with hidden policy," in Internet and Distributed Computing Systems, vol. 7646. Berlin, Germany: Springer-Verlag, 2012, pp. 146–159.

[20] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Proc. 6th Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS), 2008, pp. 111–129.

[21] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT), 2005, pp. 457–473.

[22] S. Sedghi, P. van Liesdonk, S. Nikova, P. Hartel, and W. Jonker, "Searching keywords with wildcards on encrypted data," in Security and Cryptography for Networks (Lecture Notes in Computer Science), vol. 6280. Berlin, Germany: Springer-Verlag, 2010, pp. 138–153.

[23] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO, 1984, pp. 47–53.

[24] E. Shi and B. Waters, "Delegating capabilities in predicate encryption systems," in Proc. 35th Int. Colloq. Auto., Lang. Program. (ICALP), 2008, pp. 560–578.

[25] T. V. X. Phuong, G. Yang, and W. Susilo, "Poster: Efficient ciphertext policy attribute based encryption under decisional linear assumption," in Proc. 21st ACM Conf. Comput. Commun. Secur. (CCS), Arizona City, AZ, USA, 2014.

[26] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf. Public Key Cryptogr., 2011, pp. 53–70.

[27] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Computationally efficient ciphertext-policy attribute-based encryption with constantsize ciphertexts," in Provable Security. New York, NY, USA: Springer-Verlag, 2014, pp. 259–273.

[28] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption: Extended abstract," in Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2010, pp. 753–755.