ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Securitising to Personal Health Records in Cloud Computing

[1]Durga Vangapandu, [2]T.Padmaja

[1]Final M Tech Student, [2]Asst.professor

[1]Dept of Computer Science and Engineering

[1,2]Eluru College of Engineering and Technology, Duggirala, Eluru, Andhra Pradesh, India.

Abstract: Personal health record (PHR) service is an emerging model for health information exchange. It allows patients to create, manage, control and share their health information with other users as well as healthcare providers.As more and more healthcare organizations adopt electronic health records (EHRs), the case for cloud data storage becomes compelling for deploying EHR systems: not only is it inexpensive but it also provides the flexible, wide-area mobile access increasingly needed in the modern world. However, before cloud-based EHR systems can become a reality, issues of data security, patient privacy, and overall performance must be addressed. As standard encryption (including symmetric key and public-key) techniques for EHR encryption/decryption cause increased access control and performance overhead, the paper proposes the use of Cipher text-Policy Attribute-Based Encryption (CP-ABE) to encrypt EHRs based on healthcare providers' attributes or credentials; to decrypt EHRs, they must possess the set of attributes needed for proper access. This paper motivates and presents the design and usage of a cloud-based EHR system based on CP-ABE, along with preliminary experiments and analyses to investigate the flexibility and scalability of the proposed approach.

Index terms: Cloud Computing, Attribute Based Encryption, Electronic Health Records, Security, Privacy.

I. INTRODUCTION

The term personal health record (PHR) has undergone substantial changes along with the emergence of cloud computing. In a relatively broad description, put forward by the Markle Foundation, A PHR is a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it. We recognize that the Markle Foundation description has successfully predicted the evolving of PHR in the past ten years. Most healthcare information technology vendors and healthcare providers started their PHR services as a simple storage service, and then turn them into a complicated social-network like service for patients to share personal health information with others.

Currently, interest and investment in PHRs are usually motivated by goals of efficiency, increasing patient empowerment, or improving disease management. However, patients' greatest concern about PHRs, as well as other healthcare system, is security and privacy. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 outlined the legal protections for PHR privacy and security. But, it does not address all the issues involved, especially because HIPAA only applies to covered entities including health plans, healthcare clearinghouses, and healthcare providers. Emerging cloud-based PHR service provider like Dossia, Microsoft, and Google are not covered entities.

Therefore, by introducing cloud computing into PHR service, several important issues regarding PHR privacy and security need better evaluation. Potentially, PHR could protect patient privacy and security in ways that are much more secure than traditional paper-based patient records, since it can provide additional security feature such as password protecting and audit tracking. However, by

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

outsourcing PHR into a cloud server, patients lose physical control to their own healthcare data. PHRs residing on a cloud server are subject to more malicious insider and outsider attacks than paper-based records, which exist in only a small number of physically accessible locations. Hence, we argue extra steps must be taken to provide strong privacy assurance other than directly placing those sensitive data under the control of cloud servers. One straightforward solution is encrypting sensitive data before outsourcing it into cloud server. However, applying traditional cryptography scheme on a PHR system present a major barrier to access and share PHR. PHR system users need to deal with complicated key management problem to achieve fine grained access control when their PHRs are encrypted using symmetric key cryptography or asymmetric key cryptography.

II. RELATED WORKS

Several PHR systems have been proposed or implemented to enable access control on PHR. We classify them into two categories according to their different access control mechanisms.

Authentication-Based PHR system

Some PHR systems choose an attribute-based access control (ABAC) scheme or a role-based access control (RBAC) scheme to manage users' access right. This type of system usually places full trust on the cloud server where the PHRs reside in. A typical example of authentication-based PHR system is an open-source open standard personally controlled health record (PCHR) system that enables patients to own and manage their health records. Indivo provides patients the ability to share their records with different physicians, hospitals and clinics while maintaining access control properties on the patients' health records. Access control decisions are made by the Indivo server according to institutional policies and patient specified policy.

Cryptography Based PHR System

Other PHR systems use cryptographically enforced access control scheme. This type of system usually allows patients to encrypt their PHR data and distribute corresponding decryption key to authorized user. A typical example of cryptography based system is iHealth EMR [ALG+]. It implements a self-protecting electronic medical records (EMRs) using attribute-based encryption. In that system, patient can encrypt each node in the XML-based EMR file with an automatic generated access policy before exporting it to cloud system. PHR users' access rights are defined by the attributes within their private key. However, it does not solve practical problems such as key revocation and key delegation. Nevertheless, the actual implementation is limited since the Encrypted XML file contains malformed metadata and, therefore, cannot be accepted by the third party cloud service such as Google Health.

Elliptic Curve Cryptography (ECC) is a type of public-key cryptography (PKC) that is based on the algebraic structure of elliptic curves overnite fields. The security of ECC is based on the hardness of the elliptic curve discrete logarithm problem, and achieves RSA-equivalent security with a much smaller elliptic curve group; for example, a 163-bit key in ECC is considered to be as secure as 1024-bit key in RSA [6]. ECC implementations use less memory and processing power, which allows them to be used on compact platforms such as smart phones and smart cards.

Bilinear Maps construct a relationship between two cryptographic groups leading to new schemes.

Attribute-Based Encryption (ABE) extends Identity Based Encryption (IBE), originally proposed by AdiShamir [4], by using a public key as an arbitrary string to identify a user. Boneh and Franklin's pairing- based encryption scheme [3] was the first to use fully functional IBE that is based on a novel solution of a pairing on groups of elliptic curves over finite fields.

Sahai and Waters subsequently introduced a new type of IDE called Fuzzy Identity-Based Encryption (FIBE). In FIBE, a private key is associated with a set of attributes, w, and able to decrypt ciphertexts encrypted with a set of attributes, w' , if and only if at least k attributes overlap between w'and w. FIBE's motivation was to design an error-tolerant IBE that uses biometric identities as public keys. IBE and FIBE have limited applications, as they not allow for a scalable and fine-grained access control to ciphertexts.

III. PROPOSED SYSTEM

The CPE-ABE Scheme Following Bethencourt, Sahai, and Waters [2], in our CP- ABE scheme, healthcare providers share one public key for encryption, thus avoiding PKI; however, each healthcare provider has a distinct secret key for decryption. CP-ABE supports

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

complex policies to specify which secret keys can decrypt which ciphertexts: each healthcare provider's secret key is labeled with a set of attributes, and ciphertexts are associated with access policies. The secret key of a health-care provider can decrypt a particular ciphertext only if the attribute set of the healthcare provider's key satisfies the access policy associated with that ciphertext, as illustrated in Figure 1. Here, the nurse practitioner with the ABCD Medical Group can access EHRs that are only allowed to physician assistants or nurse practitioners, and who work in the ABCD Medical Group; and the physician assistant with the WXYZ Medical Group is not allowed access.

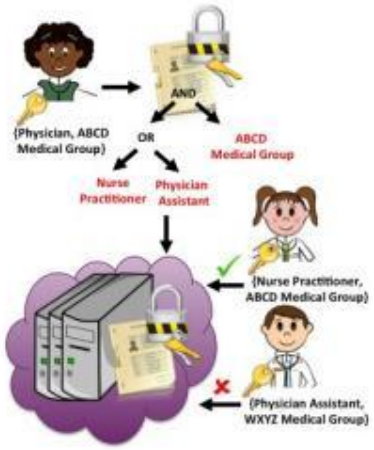

Figure 1: Using CP-ABE in a cloud-based EHR System

A CP-ABE scheme consists of four fundamental algorithms:

Setup, Encrypt, Key Generation, and Decrypt, and one op-

tional algorithm, Delegate.

- Setup: the setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.
- Key Generation(MK, S): The key generation algorithm uses the master key MK and a set of attributes S that describe the key, and outputs a private key SK
- Encrypt(PK, M, A): The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over a set of attributes. It will encrypt M and produce a ciphertext CT such that only a user who possesses the set of attributes satisfying the access structure will be able to decrypt CT.
- Decrypt(PK, CT, SK): The decryption algorithm takes as input PK, a ciphertext CT, which was obtained for an access policy A, and a private key SK for a set S of attributes. If the set S of attributes satisfies the access structure A, then the algorithm will decrypt the ciphertext and return a message M.
- Delegate(SK, S'):The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S' C S. It outputs a secret key SK' for the set of attributes S'

CP-ABE thus supports flexible and fine-grained access control with healthcare providers being able to access only relevant EHRs encrypted with access policies that satisfy their keys' attributes. Also, if a secret key is compromised, only EHRs that can be decrypted with that key will be compromised; other EHRs are still protected.

System Architecture

In our scheme, EHRs are stored in the cloud, and can be accessed through a web portal by multiple owners and users. Owners, who create EHRs, are responsible for generating access policies based on the attributes of authorized healthcare providers, encrypting EHRs based on the generated policies and uploading encrypted EHRs into the cloud. EHRs are organized into a labeled hierarchical data structure [1], which makes it possible to share different parts of the EHR, thus making the scheme more flexible.

Figure 2 shows the architecture for the proposed cloud-based EHR system, which consists of three main components: the cloud-based EHR system, Healthcare Providers(owners and users), and the Attribute Authority (AA). The system uses two fundamental cloud services: data storage and computing resources. The first service is for storing encrypted EHRs that are accessible only to healthcare providers through authentication mechanisms, and access policies based on complete attributes of healthcare providers. The second service is for hosting the web portal, generating access policies, and performing other needed computing tasks.

Once healthcare providers obtain their private keys from the AA, they log in to the system using their username and password; on first login, they will need to download and install light weight software for encrypting

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

and decrypting EHRs locally. When a healthcare provider requests access to an encrypted record, she will first locate and download it, and then use her key and the lightweight software to decrypt it. To upload a new record, she will first request the desired attributes and generate the access policy using the Access Policy Engine; encrypt the record using the lightweight software and finally upload the encrypted record.

Key Management

Key management must be cost-effective and its components carefully implemented in a cloud-based EHR system.

- Generation and Distribution: The AA generates the public key and the master private key using the Setup algorithm. When a new healthcare provider joins the system, the AA derives a distinct secret key associated with her attributes by running the Key Generation algorithm offline. Healthcare providers must store their secret keys securely, and regenerate keys after a predefined expiration date. Secret key regeneration is performed without the need to refresh the system parameters, public key, and master private key. Healthcare providers can only seek their secret keys through their healthcare organizations. Our design does not require backward secrecy: when a new health-care provider joins the system, she should be able to access all previously encrypted EHRs if and only if the attributes associated with her key satisfy the access policies associated with the encrypted EHRs.

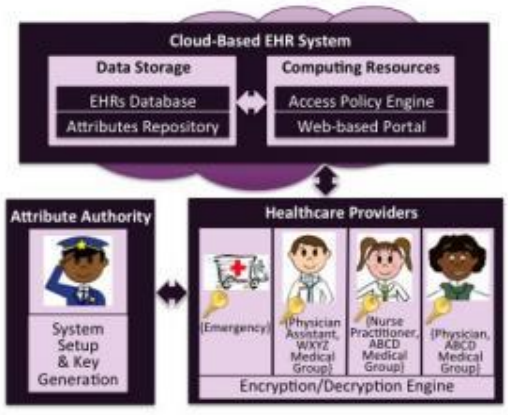

Figure 2: The Cloud-Based EHR System Architecture

Key Management

Key management must be cost-effective and its components carefully implemented in a cloud-based EHR system.

- Generation and Distribution: The AA generates the public key and the master private key using the Setup algorithm. When a new healthcare provider joins the system, the AA derives a distinct secret key associated with her attributes by running the Key Generation algorithm offline. Healthcare providers must store their secret keys securely, and regenerate keys after a predefined expiration date. Secret key regeneration is performed without the need to refresh the system parameters, public key, and master private key. Healthcare providers can only seek their secret keys through their healthcare organizations. Our design does not require backward secrecy: when a new health-care provider joins the system, she should be able to access all previously encrypted EHRs if and only if the attributes associated with her key satisfy the access policies associated with the encrypted EHRs.
- Revocation: The cloud-based EHR requires forward secrecy such that when a healthcare provider's access is revoked, she should not be allowed to access EHRs that she was able to access before being revoked. Owners of encrypted EHRs have the option to add an expiration date to access policies used for encryption, or to re-encrypt them with updated access policies to prevent access by revoked healthcare providers. The problem of re-distributing secret keys is thus avoided.
-
- Escrow: In the cloud-based EHR system, the AA can regenerate secret keys for healthcare providers to access EHRs during emergencies.

IV. CONCLUSION

In this paper, we address the security and privacy concerns of cloud-based PHR system by integrating advanced cryptographic techniques, such as CP-ABE, into PHR system. CP-ABE that provides effective solutions to some of the issues related to standard encryption mechanisms. It also investigated the feasibility of adopting CP-ABE in terms of performance and storage overhead.

References

[1] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter. Patient controlled encryption: ensuring privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Proceedings of the 2007 IEEE Symposium on Security and Privacy, 2007.

[3] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '01. Springer, 2001.

[4] CareCloud. Carecloud, web-based medical practice management software, 2011. http://www.carecloud.com/.

[5] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, CCSW '09, 2009.

[6] K. D. Edoh. Elliptic curve cryptography: Java implementation. In Proceedings of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD '04. ACM, 2004.

[7] Google. Google Health, 2011. https://www.google.com/health.

[8] B. W. John Bethencourt, Amit Sahai. Advanced crypto software collection, Feb 2011. http://acsc.cs.utexas.edu/cpabe/.

[9] P. Junod and A. Karlov. An e_cient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. In Proceedings of the 10th Annual ACM Workshop on Digital Rights Management, DRM '10, 2010.

[10] D. R. Levinson. Audit of information technology security included in health information technology standards, May 2011. http

Durga Vangapandu received her MCA Degree in Computer Science of Engineering Department from Acharya Nagarjuna University Campus Guntur (DT) in 2007.The M.tech Degree in CSE from Eluru College Of Engineering & Technology Duggirala Eluru. in 2013.

T.Padmaja received the M.tech Degree from Sri Vasavi Enginering College Tadepalligudem with distention. Currently she is working as an Asst .Professor in Eulur College of Engineering and Technology Duggirala Eulur, Andhra Pradesh, India. She have 7year of experience as a faculty from sir C.R.R College for women's EULUR