Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.585 – 590

RESEARCH ARTICLE

AN ENHANCED ATTRIBUTE BASED ENCRYPTION WITH MULTI PARTIES ACCESS IN CLOUD AREA

Saranya.S[1], Mr. K.N. Vimal Shankar[2]

[1]Department of Computer Science and Engineering,
V.S.B Engineering College, karur,
Anna University, Chennai
Email: saranya.tcesaranya@gmail.com

[2]Department of Computer Science and Engineering,
V.S.B Engineering College, karur,
Anna University, Chennai
Email: mecsevsbec@gmail.com

***Abstract*—Personal health record (PHR) systems are patient-facing portals that contain patient health information and allow patients to interact with the health system. PHR is enabled patient centric model of health information exchange, which is often outsourced to be stored at a third party such as cloud providers. Key distinction is that a PHR typically is under the patient's control, so that an individual patient is the ultimate guardian and editor of information stored or accessible within his or her PHR .In this project, it describes our design and prototype implementation of a social healthcare network over the cloud. Differ from previous work in more secure and strong encryption algorithm for Triple DES. The system is secured with a trust-aware role-based access control.**

Keywords—Personal health records, cloud computing, data privacy, fine-grained access control, attribute-based encryption

© 2014, IJCSMC All Rights Reserved

I. INTRODUCTION

PHRs issued by the American Health Information Management Association (AHIMA) and the American Medical Informatics Association define the PHR as "a tool for collecting, tracking and distribution, up to-date all data about an individual's health or the health of someone in their care. By provide a single, detailed, and complete profile of a person's health position and healthcare activity

The challenges facing health systems, operators are harnessing information technology to tailor care more closely to the needs of patients and make the system easier to navigate. This "patient-centric" model is driven by three factors: The dramatic rise in cost of care, the inability to expand capacity to match the exponential increases in demand for care, and continuing patient demands for higher quality of care. The ultimate goal is an intelligent, patient-centric care model—a system in which all relevant information is available in real time to multiple parties in all care settings, supporting tailored care for each patient Such systems will evolve over many years, requiring operators to continuously integrate new functions and capabilities. Success will also depend on evolution of patient record.

A feasible and promising approach would be encrypting the data based on Attribute Based Encryption (ABE). This technology that supports fine grained access control cryptographically. An ABE user can decrypt information, such as PHRs file, only if he or she possesses a key that corresponds to attributes specified during the encryption process. ABE has been proposed for secure information sharing in applications ranging from storage in clouds to social networks.

To assured patient details very securely stored PHR files. We referred two users personal and professional. The personal details accessing like family members and friends then professional such like doctor, nurses, hospital administrator and health care department. All users are entering data for PHR files. The users entering data to PHR with help of these vendors *Pooled educational resources, specialized search engines and Email and text message alerts etc.*

II. OVERVIEW OF FRAMEWORK

In this section, we describe patient-centric secure data sharing for cloud-based PHR systems.

A.PROBLEM DEFINITION

The proposed system is required to eliminate the risk in unavailability of one branch information in other branch. The proposed system is using an approach such that with the cloud storage space, the hardware and software maintenance risk is reduced. Then how accurately a problem is identified. At present, the multiple branch hospital information is carried out in Office packages locally and is sent through mails for reference. This increase the data redundancy and non-availability of data in time and more secured to transfer the data in PHR files

III. SECURITY PROPERTIES

Many security properties are wanted in a for transaction system. We will not go into details and enumerate all of the security properties wanted but simply mention a couple of them in the following sections.

A.A cryptographic key should not be in clear text in any single point of the System.

This is the basic security property that a PHR must achieve in order for users to have any sort of trust in the system. This is also an important point when different institutions interchange PHR data between themselves, the security of one institution depends on that of others. To achieve this property cryptographic keys must be stored in secure cryptographic processors, if they are ever outside these processors they must be in a form that does not compromise the security of the keys, such as in split knowledge (under the possession of different individuals having certain permissions), or encrypted under another cryptographic key which is protected in a secure cryptographic processor.

B. Security against known key attacks,

If a working key in the system is discovered, this should not enable an attacker to figure out the values of any other keys in the system. Some would say that if a system is secure, no single key will ever be compromised so

© 2014, IJCSMC All Rights Reserved

there is no need to worry about this security property, but as we will see later on this can be a dangerous way of thinking.

C. The security of any 3DES key should be.

It should not be possible for example to break a 3DES key by breaking one or a couple of single DES keys. If a cryptographic key is to be protected by another one, this last key should be of cryptographic strength equal or greater than the key it is protecting. This implies for example, among other things, that if any working key is a 3DES key, the key encryption key should be a 3DES key as well.

D. It should not be possible to combine different key parts in order to trick a secure cryptographic processor into revealing information that can lead to breaking any cryptographic key secured by the processor.

This is important to consider for example when deciding how keys protected outside a security processor should be stored. Of course, when analyzing the security of a system, the above security properties must be specified more formally, and others should be enumerated, but the above list is enough for us to be able to discuss about security problems related to migrating from DES to 3DES.

IV. KEY BLOCKS

The key block for the keys encrypted in the payment application key databases, and the key blocks for the key exchange keys, are not adequate to support 3DES. Attacks have been presented against key blocks currently used by the financial institutions, in which keys can be used for functionalities that they were not intended for, and knowledge of certain working keys can leak knowledge of other keys, violating security property. The attacks work even if the key blocks use encryption with a provably secure mode of operation such as CBC, even when used in combination with variants or control vectors.

The techniques of the attacks are based on substituting parts of the keys and brute forcing single DES keys twice. This can be done on average in 2×255 =256 steps, which is much smaller than 2112 (the number of steps needed to try each and every double length 3DES key). This clearly violates security properties. It is crucial to *cryptographically* tie the functionality of a key to the key itself, this can be achieved by securely using a MAC or a digital signature scheme for example, or an encryption mode of operation that also provides integrity. A proposal to ANSI X.9F for a new key block format is described in [5]. What is important to remember is that encryption alone does not provide integrity.

V. OVERVIEW OF OUR FRAMEWORK

The goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key is divided into multiple security domains (namely, public domains and personal domains) according to the different users' data access necessities. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, and medical researchers. For each PSD, is personally related with a data owner such as family members or close friends, and they make accesses to PHRs based by the owner. In both domains can utilize Triple DES to realize cryptographically enforced, patient-centric PHR files. Especially, in a PUD multi authority ABE is used to specify role-based fine-grained access policies for her PHR files, while during time we need to specify the list of authorized users when doing Triple DES encryption. Since the PUDs contain it reduces the key management overhead for both the owners and users. Each data owner (e.g., patient) is a trusted authority of her own PSD, who uses a ABE system to manage the secret keys and access rights of users in her PSD. For PSD, data attributes are defined by the PHR data, such as the category of a PHR file. For the purpose of PSD access, since the number of users in a PSD is often small, it reduces the trouble for the owner. When encrypting the data for PSD, all the owner needs to know the data properties. The multi domain approach best for different user and access requirements in a PHR system. The use of ABE makes the encrypted PHRs self-protective.

© 2014, IJCSMC All Rights Reserved

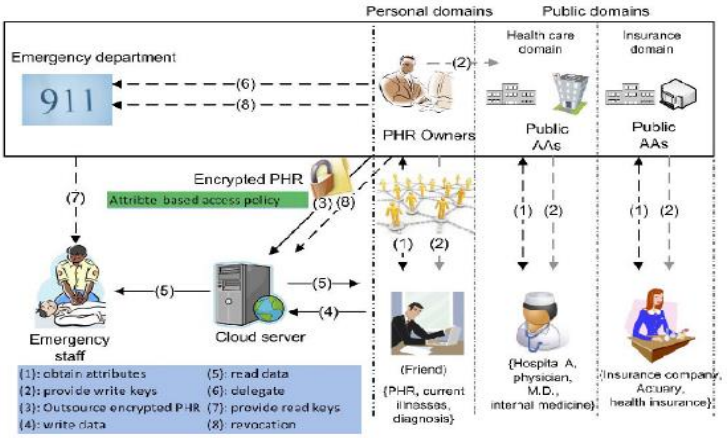


Fig. 1. The proposed framework for patient-centric, secure and scalabl PHR sharing on semitrusted storage under multiowner settings.

VI. DETAILS OF THE PROPOSED FRAMEWORK

A. Database (With visit data only) management in hospital Server

The hospital server is updated with the day to day visit results of the transactions made by them. Since the server requirement is to minimum (since the cloud manage every data (here the hardware resources are kept to be minimum)), only un-encrypted information is to be stored in data owner's (hospital) space. This is to verify the data integrity between the data replicated redundantly in more cloud spaces. The data to be stored in strongly encrypted in both the places.

B. Database (With all regular visits, prescription and receipt data) Management in Cloud Space

The cloud server is updated with the day to day visit details, prescription and receipt made by them. The cloud provider manages all data (here the hardware resources are kept to be maximum). The kind of users accessing the data is more and so different privileges are to be assigned to them so that unauthorized data modification or theft is prevented. The data is encrypted and stored so that the all users (except content owner) are unable to view the actual data.

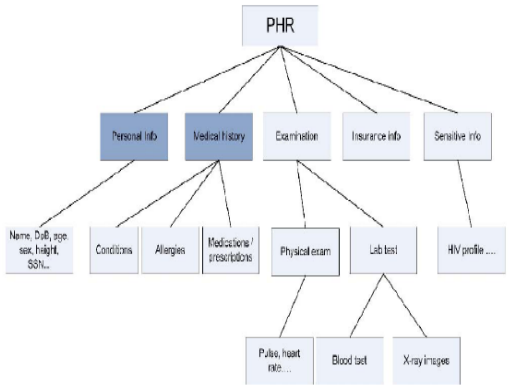


Fig. 2. The attribute hierarchy of files—leaf nodes are atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader have access to.

C. Hospital and Patient Login Provision

In different kind of privileges is assigned to different users so that they can view and access the data according to their requirements. The key arrangements are made such that content owner can modify all the data, the users only view the data.

D. Attribute Based Encryption

© 2014, IJCSMC All Rights Reserved

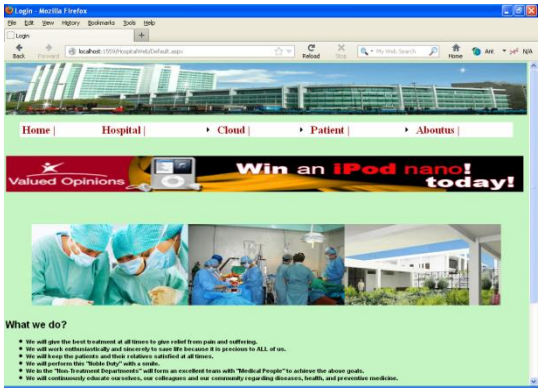
The attribute based encryption is the process of partitioning the attribute to specified field of group user. ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation, and decryption are only linear with the number of attributes involved. Each owner only needs to manage the keys of a small number of users in her personal domain.

E. Triple Data Encryption Standard Algorithm

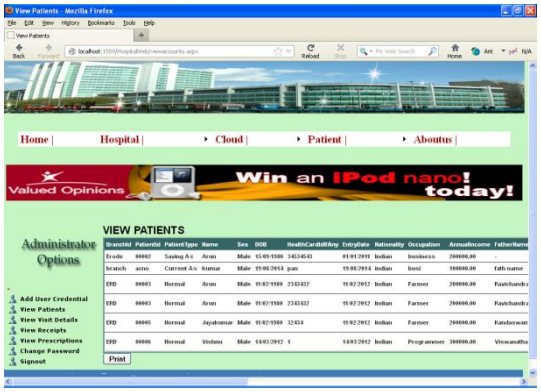
Triple DES is the common name for the Triple Data Encryption Algorithm block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. The triple DES algorithm is used to encrypt the date for the user accessed data.

Project Screenshots

Home Page



Visit Details



VII. CONCLUSION

This paper has secured information sharing, Attribute Based Encryption (ABE) and Triple Data Encryption Standard (Triple DES) as basis of the solution to use PHR files to support strategic objectives. Examples, not discussed in this paper, include Predicate Encryption where the attributes are encrypted and Functional Encryption allowing greater generality in attributes/policies .In the longer term Functional Encryption could lead to the prospect of cryptographically controlled reduction. This paper has outlined how ABE may be used by secure information sharing with both ABE adopters and legacy . The benefits of this approach are improved security within domains, mainly by reducing the attack surface for insiders and malware, and also by minimising dependency upon critical cryptographic servers. Triple DES reduces the impact of risks associated with errors and compromise of egress data guards, and scenarios have been identified these benefits could lead to improved security.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, ―Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,‖ Proc. Sixth Int'lICST Conf. Security and Privacy in Comm. Networks(SecureComm '10), pp. 89-106, Sept. 2010.

© 2014, IJCSMC All Rights Reserved

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, ―Securing the EHealth Cloud,‖ Proc. First ACM Int'l Health Informatics Symp.(IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, ―Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing,‖ Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] The Health Insurance Portability and Accountability Act,http://www.cms.hhs.gov/HIPAAGenInfo/01_Overvi w.asp,2012.

[5] Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them,‖ http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded, ‖ http://articles.latimes.com/2006/jun/26/health/ heprivacy26,2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, ―Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private,‖ BMJ, vol. 322, no. 7281, pp. 283-287,Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, ―Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ Proc. ACM Workshop Cloud Computing Security(CCSW '09), pp. 103-114, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, ―Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing,‖ Proc. IEEE INFOCOM '10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, ―Shared and Searchable Encrypted Data for Untrusted Servers,‖ J. Computer Security,vol. 19, pp. 367-397, 2010

© 2014, IJCSMC All Rights Reserved