INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2018 – 2025
RECEIVED: 15-03-17. PUBLISHED: 06-04-17.

April 06, 2017

ACTOR BASED ACCESS CONTROL FOR A CENTRALIZED CLOUD SERVER FOR E-HEALTH

[1]Aiswarya.M , [2]Amritha.C, [3]Devika K H, [4]Haritha K R, [5]Jebakumari.M,
[1,2,3,4]Students,Department of CSE, Nehru Institute of Technology,Coimbatore, Tamil Nadu,India,
[5]Associate Professor,Department of CSE, Nehru Institute of Technology, Coimbatore, Tamil Nadu,India.

ABSTRACT

The electronic personal health record is a collection of information about patient's health. Here data will be stored in the centralized manner, where the user can access the data from anywhere. To improve the security level of data, Dual-key encryption method is used along with Attribute based encryption(ABE). The data stored in database is in the encrypted form and only during the time of retrieval the data will be decrypted. In this paper, a secured and scalable third party storage method using attribute based encryption is proposed for personal health records. Using third party storage system tremendous number of data can be stored and can be accessed easily using query distribution methods. In order to implement attribute based encryption, data from front end is stored in the back end as a symbol based format. Moreover Dual system encryption method is used which is an advanced encryption method that will work on both front end and back end thus making the data more secured. In addition, implementation of this architecture in cloud makes the data centralized, and the patients can continue their treatment anywhere at any time. This helps the patients to maintain their Personal Health Record (PHR) and get quality treatment.

Keywords*:* Attribute-based encryption,Dual key encryption, PHR

1. INTRODUCTION

1.1 OVERVIEW

Personal health record is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control.

In this work, a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers is proposed. To achieve fine-grained and scalable data access control for PHRs, use of attribute-based encryption (ABE) techniques to encrypt each patient's PHR file is done. Different from previous works in secure data outsourcing, the main focus is on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. This scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Here experimental results are presented which show the security, scalability, and efficiency of the proposed scheme.

A cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. General

encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. In this work a threshold proxy re-encryption scheme integrated with a decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages. This method fully integrates encrypting, encoding, and forwarding, analyzing and suggesting suitable parameters for the number of copies of a message dispatched to storage servers and queried by a key server. These parameters allow more flexible adjustment between the number of storage servers and robustness.

1.2 LITERATURE REVIEW

Several application scenarios are used in electronic healthcare(e-health) , e. g ., electronic health records , accounting and billing , medical research , and trading intellectual property. E-health systems like electronic health records(EHRs) are used to decrease costs in health care and to improve personal health management.

A.-R.Sadeghi et al.(2010) proposed [24] a security architecture for establishing privacy domains in e-health infrastructure,this provided the client platform security and combines this with network security concepts .M.Li et al.(2011) proposed [17] to overcome the problem of authorized private keyword searches on encrypted PHR in cloud computing environments.Akshita et al. (2016) proposed [1] to implement the security in cloud server using attribute based encryption which is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon attributes.Susan Hohenberger and Brent Waters (2013) proposed [25] the design of ABE schemes with faster decryption algorithms.C. Wang et al.(2010) proposed to address the challenge of defining and enforcing access policies based on data attributes, and, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to entrusted cloud servers without disclosing the underlying data contents.

2. METHODOLOGY

2.1 PROPOSED SYSTEM

In the proposed system, all the details that are currently maintained manually are computerized. Due to computerization, the data entered are very much secured, and cannot be accessed or changed by unscrupulous persons. The proposed system is totally user friendly and menu driven thus helping a person to use this with ease and accuracy. The record can be easily updated at any time.

2.2 CLIENT/SERVER ARCHITECTURE

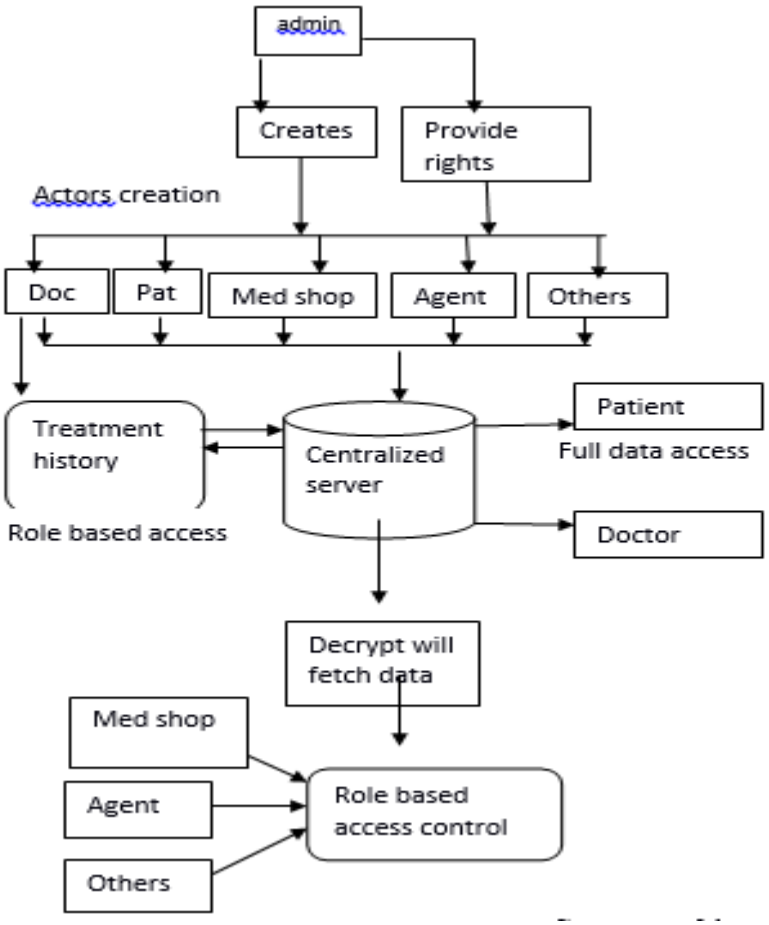
The system consist of an admin. The admin creates the actors and provide the rights to the actors. The actors that are involved in the hospital environment are doctor, patients, medical shop, insurance agent. Doctor uploads the treatment history to the centralized server in the encrypted form which uses the attribute based encryption. The patient and doctor have the right to access the full data according to the role provided to the actors, during the decryption they fetch the data.

Configuring Organization and dataset.

This is the initial module of this project. Here the environment will be the medical domain. So this module contains a hospital environmental based application. An admin is available for controlling the whole application. Admin can

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2018 – 2025
RECEIVED: 15-03-17. PUBLISHED: 06-04-17.
April 06, 2017

create doctor, patient and actors those who can access this application. Admin can customize the whole application and provide rights and customization to the actors.



System architecture

Dual Key Encryption

The de centralized server's data will be encrypted dual times before reaching the server. The entire data will be decrypted twice except the ID. The ID will represent the field for data access. Hybrid cryptography will be implementing for the encryption process. AES has a fixed block size of 128 bit and a key size of 128, 192, or 256 bit, has specified with block and key sizes in multiples of 32 bit, with a minimum of 128 bit. The block size has a maximum of 256 bit but the key size has no theoretical maximum AES operates on a 4×4 column-major order matrix of bytes, termed the state.

Processing the actor with ABE

ABE (Attribute based encryption) the main process in this module is, only actors can access the data with data access control. The encrypted data will be decrypted during the time of retrieval only. Remaining time the data will be remains encrypted in the server's database. While retrieving the data only permitted data of the particular actor will be visible to the actor. Other data and fields will be in encrypted format. To actors can able to access the unwanted or sensitive information of the organization.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2018 – 2025
RECEIVED: 15-03-17. PUBLISHED: 06-04-17.
April 06, 2017

Data log and access history

Data log and access history will be deals with the data patterns like permissions, actors involved, accessed data by the actors, accessed fields, latest updates in the server, last accessed data and time of the server, server restrictions and etc. This module gives the overall data access and security issues in the server. This module can be accessed by both admin and actors

Dual Key Encryption

In designing security systems, it is wise to assume that the details of the cryptographic algorithm are already available to the attacker. The history of cryptography provides evidence that it can be difficult to keep the details of a widely used algorithm secret. A key is often easier to protect (it's typically a small piece of information) than an encryption algorithm, and easier to change if compromised. Thus, the security of an encryption system in most cases relies on some key being kept secret. Trying to keep keys secret is one of the most difficult problems in practical cryptography; see key management. An attacker who obtains the key can recover the original message from the encrypted data. Encryption algorithms which use the same key for both encryption and decryption are known as symmetric key algorithms. These key algorithms allow one key to be made public while retaining the private key in only one location. They are designed so that finding out the private key is extremely difficult, even if the corresponding public key is known. A user of public key technology can publish their public key, while keeping their private key secret, allowing anyone to send them an encrypted message.

Key size

For the one-time padding system the key must be at least as long as the message. In encryption systems that use a cipher algorithm, messages can be much longer than the key. The key must, however, be long enough so that an attacker cannot try all possible combinations. A key length of 80 bits is generally considered the minimum for strong security with symmetric encryption algorithms. 128-bit keys are commonly used and considered very strong.

The keys used in public key cryptography have some mathematical structure. For example, public keys used in the RSA system are the product of two prime numbers. Thus public key systems require longer key lengths than symmetric systems for an equivalent level of security. 3072 bits is the suggested key length for systems based on factoring and integer discrete logarithms which aim to have security equivalent to a 128 bit symmetric cipher. Elliptic curve cryptography may allow smaller-size keys for equivalent security, but these algorithms have only been known for a relatively short time and current estimates of the difficulty of searching for their keys may not survive. A message encrypted using a 109-bit key elliptic curve algorithm had been broken by brute force. The current rule of thumb is to use an ECC key twice as long as the symmetric key security level desired. Except for the random one-time pad, the security of these systems has not been proven mathematically, so a theoretical breakthrough could make everything one has encrypted an open book. This is another reason to error on the side of choosing longer keys.

Reduced manual efforts

The number of persons involved in maintaining the transactions is reduced, so that the processes can be carried out quickly, as the reports are not transferred to any persons for testing, etc.Faster Transactions The transactions can be carried out quickly, than the manual efforts. The time taken for transactions would be the time taken for feeding the data into the computer only; there would be no time needed for calculations or generation of reports.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2018 – 2025
RECEIVED: 15-03-17. PUBLISHED: 06-04-17.
April 06, 2017

Increased Reliability

The computational complexity is reduced, so that the error-rates are also reduced. Unlike manual efforts, any changes can be reprogrammed in the software, quickly.

The reports can be generated quickly anytime when they are needed. The reports generated would be neat and attractive and can be changed to any required form.

Secured Data and Backup

Unscrupulous persons cannot access the data stored through the software, as there are passwords for every entry. The large amount of data can be taken backup, so that loss of data is greatlyreduced.

2.3 FEATURES OF THE PROPOSED SYSTEM

- There should be entry screen and reports for all modules.
- The information's flow should be developed. Help messenger, alert, list of values
- Should be provided making the project user friendly.
- Database should be structured with minimum redundancy.
- System security should be provided
- The system has been developed to generate timely reports.
- Saving information at various stages in faster manner.
- Faster addition, deletion, modification capabilities and data entry.

2.4 ATTRIBUTE BASED ENCRYPTION

Step 1: Gen(λ , U) $\rightarrow$ (PK,MK).

The algorithm takes the security parameter(λ) and a universal description (U).

Step 2: Encrypt(PK,M,S) $\rightarrow$ CT.

Theencryption takes the input as public parameters PK, a message M and a set of attributes S and outputs a ciphertext CT .

Step 3 :KeyGen(MK,A) $\rightarrow$ SK.

In key generation ,it takes input as master secret key MK and an attribute structure A and outputs a private key SK associated with the attributes.

Step 4 : Decrypt(SK,CT) $\rightarrow$ M.

In decryption , it takes input as private key SK and a ciphertext CT and outputs a message M if S satisfies A or the error message .

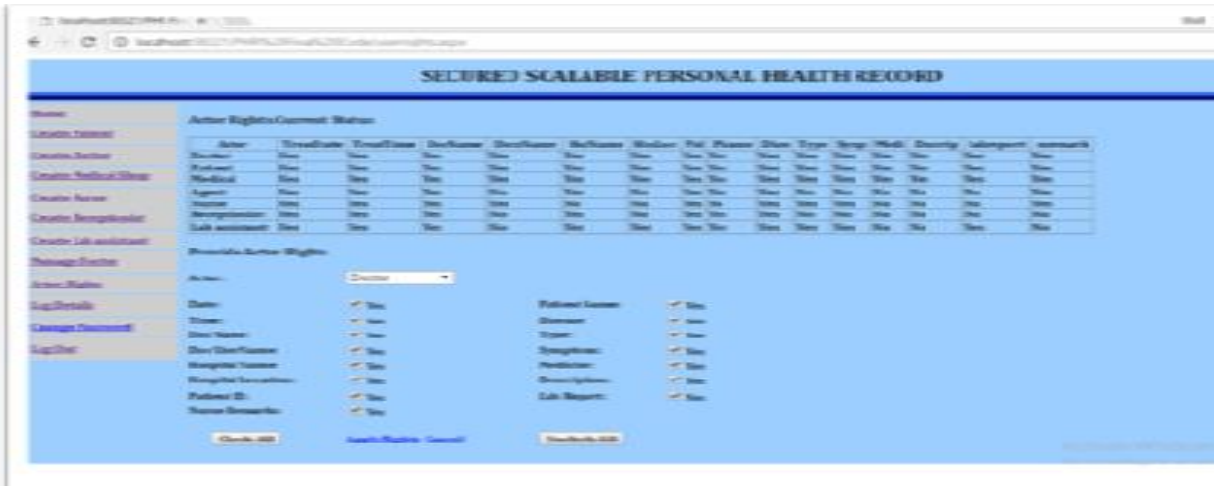
For all(PK,MK) $\in$ Setup(λ , U), all S $\subseteq$ U,

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2018 – 2025
RECEIVED: 15-03-17. PUBLISHED: 06-04-17.
April 06, 2017

2.5 ABOUT THE METHOD

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

3. RESULT



This screenshot shows the admin giving rights to each actor.

This screenshot shows the login details.

CONCLUSION

In this paper, an Attribute Based Encryption along with Dual key encryption is proposed to increase the security of personal health record system stored in the cloud. This solution ensures confidentiality of the health records and protection from unauthorized users. It also keeps the login details of the actors and provides faster accessablity to the actors as a unique key is used.

REFERENCES

[1] Akshitasaxena,NitinChaudhary,"Decimal attribute based encryption in cloud server",vol 5,issue 12,dec 2016.

[2]Allison Lewko, YannisRouselakis, Brent Waters," Achieving Leakage Resilience Through Dual System Encryption".

[3]Allison Lewko,Brent Waters ,"Decentralizing Attribute-Based Encryption".

[4]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.

[5]D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, vol. 3027. Interlaken, Switzerland, May 2004, pp. 506–522.

[6]D. Boneh and X. Boyen." Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles. In Advances in Cryptology" – Eurocrypt, volume 3027 of LNCS, pages 223–238. Springer, 2004.

[7]DananThilakanathana ,ShipingChenb , Surya Nepal b , Rafael Calvoa , Leila Alemb," A platform for secure monitoring and sharing of generic health data in the Cloud".

[8]DimitriosZissis,DimitriosLekkas," Addressing cloud computing security issues".

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

[10]Fuchun Guo1, Yi Mu 2, Zhide Chen1, and Li Xu 1" Multi-Identity Single-Key Decryption without Random Oracles"2000.

[11]V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[12]HaixunWang,Jianyin,Chang-ShingPerng and Philip S.Yu"Dual Encryption for Query Integrrity Assurance"RC24300(W0707-044) July 5,2007.

[13] Javier Herranz, Fabien Laguillaumie, and Carla Rafols." Constant size ciphertexts in threshold attribute-based encryption. In Public Key Cryptography", pages 19–34, 2010.

[14] Jiguo Li, Yuerong Shi and Yichen Zhang," Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage" Int. J. Commun. Syst. 2017; 30: e2942 Published online 19 February 2015 in Wiley Online.

[15]Lakshminath R. Dondeti, Sarit Mukherjee ,AshokSamal," Scalable Secure One-to-many Group Communication using Dual Encryption".

[16] Lakshminath R. Dondeti ,SaritMukherjee and Ashok Samal "A Dual Encryption Protocol for Scalable Secure Multicasting"

[17]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'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[18]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.

[19] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

[20]H.Y. Lin and W.-G Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage",IEEE Trans. Parallel and Distributed Systems, vol.21, no.11, pp. 1586-1594,Nov.2010.

[21]Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258, pp. 355–370, Feb. 2014. H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[22]Ostrovsky, R., Sahai, A., Waters, B.: "Attribute Based Encryption with NonMonotonic Access Structures. In": ACM conference on Computer and Communications Security (ACM CCS). (2007)

[23]Rongmao Chen, Yi Mu, Senior Member, IEEE, Guomin Yang, Member, IEEE, FuchunGuo, and Xiaofen Wang," Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 4, APRIL 2016.

[24]H.Lo hr,A.-R.Sadeghi,andM.Winandy," Securing the e-health cloud,"Proc.First ACM Int'1 Health Informatics Symp.(IHI '10),pp.220-229,2010.

[25]Susan Hohenberger,BrentWaters,"Attribute based encryption with faster decryption",May 8 2013.

[26]VipulGoyal, Abishek Jain, Omkant Pandey, and Amit Sahai. "Bounded ciphertext policy attribute-based encryption". In ICALP, 2008.

[27]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.