ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Issue 3, March 2016

ACTOR BASED ACCESS CONTROL FOR A CENTRALIZED CLOUD SERVER

[1]Priya .M, [2] Magesh kumar .C

Student, Department of IT, SNS College of Technology, Coimbatore, Tamilnadu, India[1]

Assistant Professor, Department of IT, SNS College of Technology, Coimbatore, Tamilnadu, India[2]

ABSTRACT

A personal health record is simply a collection of information about patient's health. If the patients have a shot record or a box of medical papers, they already have a basic personal health record. We proposing secured and scalable third party storage methods using attributes based encryption for personal health records. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. We analyze and suggest suitable parameters for the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server. In order to implement attribute base encryption, data from front end will be stored in the back end as a symbol based format. Implementing attribute based Dual key encryption for 32 bit alpha numeric key. So that even low level working in the hospital or the organization will not able to find out the treatment history for any patients.

Keywords- Access control, attribute-based encryption (ABE), Personal health record, multi-authority, cloud secure data.

1. INTRODUCTION

Personal health record (PHR) 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 paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus 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. Our 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. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our 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. We propose a threshold proxy re-encryption scheme and integrate it 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

All Rights Reserved © 2016 IJARBEST

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Issue 3, March 2016

main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. Our method fully integrates encrypting, encoding, and forwarding. We analyze and suggest suitable parameters for the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server. These parameters allow more flexible adjustment between the number of storage servers and robustness.

In this proposed system Dual system encryption method is an advanced encryption method which will works on both front end and back end. So that data will be much secured. This is because in case of any celebrities, Politician or any public personality may undergo for any crucial treatments, at that time the treatment data should not be getting leaked. This became a prestigious issue for that public personality. So that in this method provides dual system encryption. This is an advanced encryption method which encrypts the data into symbols while storing in the database. So that even low level working in the hospital or the organization will not able to find out the treatment history for any patients.

In added with in case of implementing the data architecture in cloud architecture, all the data will be getting centralized. So that the patients can continues their treatment anywhere at any time. This helps the patient to maintain their PHR and can able to get quality treatment. Here search complexity is increased due to higher data storage. So that patients can be searched with any criteria like their figure print, Iris, Patient name, Father Name, DOB, last treatment place and etc.

Here the third part actor will be the insurance company, so that the centralized data can be accessed by the subscribed insurance company server. This method will not produce any fake data for the insurance claim. By using this method insurance can be properly utilized by the patients after their treatments. The insurance company can look over the treatment location, treatment type, nature of the treatment, bill generated for the treatment and etc in order to provide the proper claim money for the patient.

2. RELATED WORK

Many different application scenarios are envisaged in electronic healthcare (e-health), e.g., electronic health records, accounting and billing, medical research, and trading intellectual property .In particular e-health systems like electronic health records (EHRs) are believed to decrease costs in healthcare (e.g., avoiding expensive double diagnoses, or repetitive drug administration) and to improve personal health management in general. Examples of national activities are the e-health approach in Austria, the German electronic Health Card (eHC) system [1] . under development, or the Taiwan Electronic Medical Record Template (TMT).

Existing works in searchable encryption are unable to meet the above requirements simultaneously. In this paper, we formulate and address the problem of authorized private keyword searches (APKS) [2] on encrypted PHR in cloud computing environments. We first present a scalable and fine-grained authorization framework for searching on encrypted PHR, where users obtain query capabilities from localized trusted authorities according to their attributes, which is highly scalable with the user scale of the system. Then we propose two novel solutions for APKS based on a recent cryptographic primitive, hierarchical predicate encryption (HPE), one with enhanced efficiency and the other with enhanced query privacy. In addition to document privacy and query privacy, other salient features of our schemes include: efficiently support multi-dimensional, multiple keyword searches with simple range query, allow delegation and revocation of search capabilities. We implement our scheme on a modern workstation, and experimental results demonstrate its suitability for practical usage.

HIPAA [3] regulations, Joint Commission accreditation, and state privacy and other regulations mandate patient data privacy. Databases, for example, need to be secured, while maintaining appropriate and legitimate access, including treatment, payment, and operations (TPO), as well as reporting and auditing. The LMR (Longitudinal Medical Record) [4] Patient Gateway offers secure electronic communication between patients and physicians, as well as request forms, health and disease information, practice information, and other features. The application is entirely Web-based and incorporates services such as prescription renewal,

All Rights Reserved © 2016 IJARBEST

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Issue 3, March 2016

appointment, and referral authorization requests. These are transmitted securely to authorized physicians and practice staff and stored permanently in Partners' clinical information systems. Physicians and staff can communicate directly with patients, can exchange messages with each other, and can place of copies of messages into the electronic chart if desired.

The patient should always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. Therefore, in a "patient-centric" PHR system [5], there are multiple owners who encrypt according to their own ways, using different sets of cryptographic keys. Essentially, realizing fine-grained access control under encryption can be transformed into a key management issue. However, under the multi-owner setting, this problem becomes more challenging. Due to the large scale of users and owners in the PHR system, potentially heavy computational and management burden on the entities in the system can be incurred, which will limit the PHR data accessibility and system usability. On the one hand, for each owner her PHR data should be encrypted so that multiple users can access at the same time. But the authorized users may come from various avenues, including both persons who have connections with her and who do not.

3. PROPOSED WORK

In our 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 dual encryption algorithms which use the same key for both encryption and decryption are known as symmetric key algorithms. These asymmetric 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.

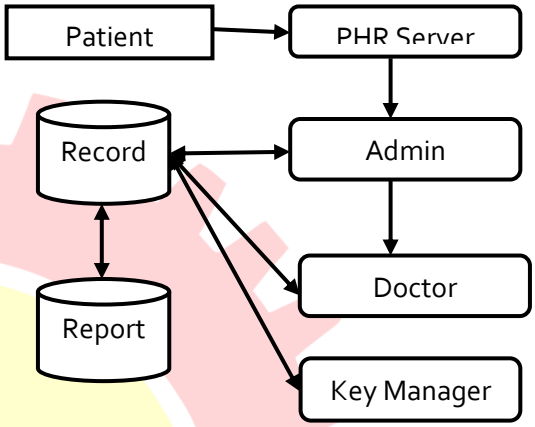

Fig1. Proposed Architecture

3.1 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 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.

3.2 Centralized the mining server

In order to access all the data, we need a centralized server. This server contains all the information about the organization like doctor details, patient details, patient's treatment information, treatment history, Medical reports, insurance details and etc. This de centralized server is for the entire hospitals county wide. Actors will be separated according to their roles and responsibilities. A unique code will be generated for all doctors and patients. So that fake doctors will be identified easily.

3.3 Dual Key Encryption

The 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

All Rights Reserved © 2016 IJARBEST

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Issue 3, March 2016

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.

3.4 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.

3.5 Processing the actor with ABE

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.

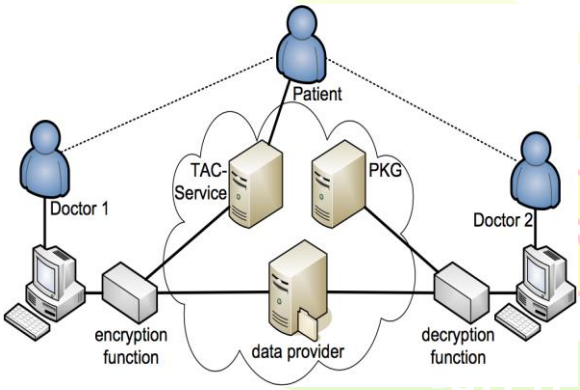

Fig 2. Processing of ABE

4. DUAL ENCRIPTION PROCESS

Advanced Encryption Standard (AES) is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network. AES has a fixed block size of 128 bit and a key size of 128, 192, or 256 bit, whereas Rijndael 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 (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are down in a special finite field.

The name "Hybrid" is used to show that the algorithm has built-in features that are inherited from data hiding techniques or "Steganography." The distinctive features of this algorithm are as follows:

• Key length is variable: the key length can be varied from 16 up to any larger value depending on the security level required.

• Word length is variable: the block size can be varied between 1 to 16 bit or 1 to 32 and so on. That is, encryption can be performed on 16 or 32 or 64 bit blocks. This, in turn, can be used on different processor architectures employing 16, 32, or 64 bit registers.

• The algorithm, therefore, provides variable degrees of security. However, this increased security level will be at the cost of increased size of the cipher-text.

• The number of rounds is variable: the whole process can be repeated r times using the same key.

The method is quite suitable for hardware implementation employing Field programmable gate arrays (FPGA).

4.1 Encryption Process

The method is reasonably simple. We have a key matrix KLx2 where,

$$k_{ij} \in \{1,2,3,4,5,6,7,8\} \begin{cases} \forall i = 1,...,L\,; \mathrm{L} \geq 16 \\ \forall j = 1,2 \end{cases}$$

This key is known only to the sender and receiver. When the first party wants to send a message M to the second party, he/she determines the key 2 L K×and every character from the message is replaced by a binary value. An eight-bit octet is generated randomly and set in a temporary vector V. the bits in the vector V from position K [1,1] to position K[1,2] are replaced by bits from the secret message. Then the resulting vector V is stored in a file. As long as the message file has not reached its end yet, we move

All Rights Reserved © 2016 IJARBEST

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Issue 3, March 2016

to the next row of the key matrix and another octet is generated randomly and the replacement is performed repeatedly and the resulting vector is stored in the file. The previous procedure is repeated over and over again pending the end the message. The resulting file is sent to the receiver who beforehand has the key matrix. If the key length is not enough to cover the whole message during the encryption process, the key will be reapplied over and over again until the encryption of the whole message is completed. This formal algorithm is shown next.

4.2 Decryption process

For decrypting the received encrypted file the following steps are taken. An octet is read from the encrypted binary plain text message EBPM file, then it is set in a temporary vector V, from this vector, bits are extracted from position K(1,1) to position K(1,2) and set in a BPM file. Since the EBPM file is nonetheless not empty, the next octet is read from the EBPM file and then it is set in a temporary vector V. From this vector, bits are extracted from position K (2, 1) to position K (2, 2) and added to the binary plain text message BPM file. The above steps are repeated over and over again until the EBPM file becomes empty. Every octet form the BPM file is transformed to the corresponding character, and then is put in the plaintext file. When the EPBM is empty the plaintext file becomes the message. In case that the key length is not enough to cover the whole message during the decryption process, the key will be reapplied over and over again till the decryption of the whole message is completed.

4.3 Key Length

Now we will show the number of possible keys, i.e., the key space when the key length is 16. The probability of replacing a string of bits whose length ranges from 1 to 8 bit in an octet is 1/64. Consequently, if the key length is 16 there are 64(16) = 7.9x10(28) possible keys. So we can say that if the attacker has a cipher text and he knows that the key length is 16, there are 7.9x10(28) attempts to find the correct key, i.e. , there are 7.9x10(28)attempts to find the correct plaintext or secret message.

5. EXPERIMENTAL AND RESULTS

The existing system and proposed system is compared with external security using USB, public authorities, PHR security and emergency department. From this we can found that in the existing system there is no external security used. So when the external security introduced, the security of the emergency department is also increased a lot. Also the public authorities are increased in the proposed system due to the security increase. Thus the Dual key encryption security is very high in proposed system and also the security of the emergency department is increased very much.

Table 1. compare Existing with proposed system

Algorithm	No of Attribute				
	5	10	15	20	25
External USB	0.13	0.18	1.43	1.65	1.86
Public Authorities	0.09	0.13	0.21	1.32	1.47
Proposed	0.02	0.06	0.14	1.12	1.27

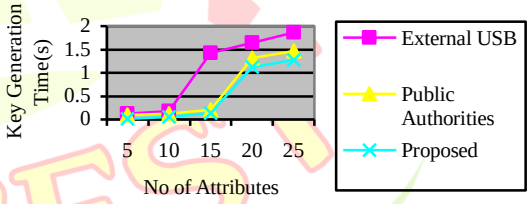

Fig 3. ABE Key Generation Time

Table 2. Time To Encrypt Time

Algorithm	No of Attribute				
	5	10	15	20	25
External USB	0.43	0.65	1.45	1.98	2.43
Public Authorities	0.35	0.54	1.34	1.78	2.34
Proposed	0.23	0.36	1.03	1.34	1.67

All Rights Reserved © 2016 IJARBEST

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Issue 3, March 2016

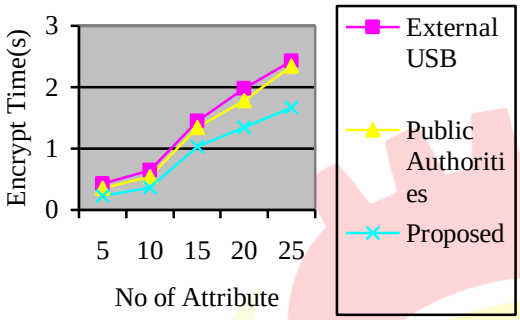

Fig 3. ABE Encrypt Time

Table 3. Time to Encrypt Time

Algorithm	No of Attribute				
	5	10	15	20	25
External USB	0.54	0.68	1.32	1.76	2.43
Public Authorities	0.43	0.58	1.26	1.64	2.14
Proposed	0.32	0.40	1.13	1.48	1.04

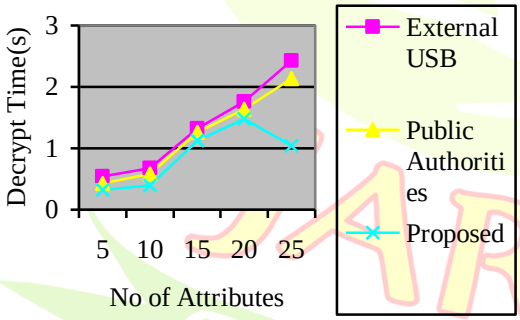

Fig 3. ABE Decrypt Time

6. CONCLUSION AND FUTURE WORK

The current system has been developed according to the given commitment as well as the system is working in an efficient manner. Most of the details are computerized and stored in the centralized server. So in this application data can be accessed anywhere and anytime. All the actors have been created in this application and unique code has been generated. For initial security purpose all the information has been encrypted while centralizing in the main server. So that all available data in the server will be in encrypted format. This information helps in making decisions regarding the security issues occurring in the future system. The current system required by the client based on their input in a faster manner. Since the Input given by the client is analyzed using the data mining techniques, an unknown or hidden information is retrieved from the data base. Fields can be customized by the admin using access customization method. In this method admin can decide the security and data accessing level for the actors. This method will be combines with ABE as the future enhancement.

REFERENCES

[1] 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.

[2] 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.

[3] 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/ he-privacy26, 2006.

[4]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.

[5] 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.

[6] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and

All Rights Reserved © 2016 IJARBEST

Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in IEEEINFOCOM'10, 2010.
[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010
[9] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records,"in CCSW '09, 2009, pp. 103–114.
[10] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,"Ciphertext-policy attribute-based threshold decryption with delegation and revocation of user attributes," 2009.
[11] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp.121–130.
[12] Wang,W., Li, Z., Owens, R., Bhargava, B.: Secure and efficient access to outsourced data. In: CCSW 2009, pp. 55–66 (2009)
[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98

All Rights Reserved © 2016 IJARBEST