Cryptosystem for Personal Health Records in Cloud

Sathish Kumar V E
PG Scholar
Department of Information Technology
PSG College of Technology
Coimbatore

K Umamaheswari, Ph.D
Professor
Department of Information Technology
PSG College of Technology
Coimbatore

ABSTRACT

Personal Health Record (PHR) sharing in cloud is a major issue in recent trends. The data stored in cloud is not secure because everything depends upon the cloud service provider. An unexpected cloud crash may expose all data in cloud. In order to overcome that a new symmetric key encryption that uses a constant key for encrypting PHR is proposed.The system developed uses a Patient Controlled Encryption (PCE), where the patients control and manage their own health record. The system developed enhances key management by storing the keys by the patient itself. The patients can share their key with whoever they want.The algorithm used here takes less computational time and memory usage for execution than existing cryptographic algorithms.

General Terms

Cryptography, Cloud computing.

Keywords

Personal Health Record, Access control, Data Privacy, Symmetric key encryption, Data Security.

1. INTRODUCTION

A personal health record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient. This stands in contrast to the more widely used electronic medical record, which is operated by institutions (such as hospitals). The intention of a PHR is to provide a complete and accuratesummary of an individual's medical history which is accessible online. The health data on a PHR might includepatient-reported outcome data, lab results, and data from devices such as wireless electronic weighing scales or collected passively from a smart phone. In order to make the PHR to access from anywhere anytime it is necessary to make available it in cloud.Cloud computing is a computing model, for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal managementeffort or service provider interaction. Cloud computing provides anything as a service, where resources such as computing power, storage space, network, and software areabstracted and provided as services on the internet in a remotely accessible fashion. Making a data available in cloud has its own disadvantages. In order to ensure that data is secure (that it cannot be accessed by unauthorized users or simply lost) and that data privacy is maintained, cloud providers attend to data protection, Identity management, Physical and personnel security, Availability Application security and Privacy. One of the possible solution to acquire security is making use of cryptographic techniques. There are two types of encryption techniques symmetric and asymmetric encryption. The asymmetric encryption uses two keys public and private which takes more computational time and main problem with that is key management. Symmetric key encryption is simple and easy to carry out. It is faster than any other cryptographic techniques. Since it uses same key for both encryption and decryption, the keys should be exchanged between sender and receiver. So the key should be made secure. In the proposed system here the key is managed by the users, so the problem of key management is rectified. The security of the single key in symmetric key encryption is more important so the key is transferred using separatesecure protocol.

The paper is organized as follows. Section 2 describes Literature survey and related works. The proposed system is explained in Section 3. The system is developed and performance results are presented in Section 4.

2. LITERATURE SURVEY

In order to secure sharing of health record in cloud and to maintain the confidentiality of health data, different types of cryptographic methods have been proposed. Each proposed method has its own advantage and disadvantages.

In [1],'Cheng Kang Chu, ShemanS.M,Chow, Wen GueyTzdeng' proposed a public-key cryptosystem that produce constant-size secret key. Using that secret key efficient delegation of decryption rights for any set of cipher texts are possible. One can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. A limitation in this work is the predefined bound of the number of maximum cipher text classes. In cloud storage, the number of cipher texts usually grows rapidly. So system has to reserve enough cipher text classes for the future extension.

Ming Li, Shucheng Yu, Yao Zheng, KuiRen and Wenjing Lou proposed the new concept of Attribute-Based Encryption(ABE) in the paper 'Scalable and securingpersonal health records in cloud storage', [2]. ABE is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.Attribute-based encryption can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipient attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used. The complexities per encryption, key generation, and decryption are only linear with the number of attributes involved.However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are nontrivial to solve, and remain largely open up-to-date.

A new Symmetric key algorithm is discussed in the paper ‘A Symmetric Key Cryptographic Algorithm’, [3].The algorithm takes less computational time to encrypt large amount of data and provide more security by the presence of two reverse operations. Architectural support for this symmetric key cryptosystem is discussed which introduces new instructions in the executing environment to gain better performance. The algorithm makes use of binary division. In encryption the binary value of the letter to be encrypted is generated and it is divided by the key which is also converted into binary. The quotient and remainder is appended and stored as a cipher text. During decryption the quotient is multiplied with secret key and added with remainder. The corresponding ASCII value of the letter is generated. The encryption and decryption both performed by converting plaintext and secret key to binary.The Algorithm is very simple in nature and takes less computational time compared to other symmetric key algorithms. There are two reverse operations present in this algorithm which would make it more secured.The biggest problem with symmetric key encryption is that you need to have a way to get the key to the party with whom you are sharing data. When someone gets their hands on a symmetric key, they can decrypt everything encrypted with that key.

3. PROPOSED SYSTEM

The proposed system is a web based application which maintains a centralized repository of all health record information. This allows the users to access the information easily. It provides storage to store personal health records in cloud storage. The records are encrypted before storing in cloud storage with a constant size secret key using a new symmetric key encryption. Symmetric key encryption takes less computational time compared to public key cryptosystems. The secret key is not stored in cloud database because if secret key is known to the attacker he can easily decrypt the data stored in cloud. This makes the key management more efficient. Secret key is sent through secure channel. The objective of this work is to provide a trusted computing environment. The proposed work provides security services like encryption to ensure secure data storage and prevent data access by unauthorized users.

3.1 Description of the system developed

The system developed is a patient controlled encryption system. Patients generate and stores secret keys. The key size is constant. Doctors are responsible for viewing the PHR as requested by patient. The details of interaction between the system and users of the system are discussed below. The users of the system are patient, doctor and admin. Each user have their own role. Admin is responsible for maintaining patient and doctor details. Patient can interact with other patient and doctor based on his need. Based on secret key the parts of the record viewed by other users are controlled by admin. The doctor and patient registration is controlled by the admin. The admin verifies doctor and patient details on enrollment and verifies their identity with the government databases and admin generates ID for every doctor and patient. Initially the system generates random password which can be modified by the patient for their convenience. Forgot password option is built with the option of sending recovery code for mobile number or email ID which is given during the registration.

After registration every user of the system such as patient and doctor have their unique username and password. Patient can upload their health record details as specified by the system. The patient details entered are encrypted and stored by using a symmetric key algorithm with a constant size secret key. The size of secret key is 6 digits which is generated by pseudorandom number generator. The key is generated and stored by the user. User can use any algorithm to generate key. But the size should be 6 digits. The key is kept confidential by the patient. So the health record details are encrypted and stored in the cloud database.

A patient can share his record by using the secret key. If the patient wants to share his record with a doctor he want to fix appointment with the particular doctor based on his problems. Doctors are categorized based on their specialization. If a patient has ear problem means he can fix appointment with a ENT specialist. If the appointment is approved by the doctor, the patient can send his secret key at the time of appointment by using a secure channel. The doctor can view the patient’s record at the time of appointment by decrypting it with the secret key sent by the patient. Here the whole patient record is made available to the doctor. If the patient wants to share his record to other patient who are registered with the system means the personal details only made available to the patient. In order to maintain confidentiality with the health data the personal details only made available to other patient. The health details are kept confidential. The records are stored in a centralized cloud database which can be accessed anywhere.

3.2 Communication between patient and doctor

The communication flow between patient and doctor is shown in the fig 1. Patient uses constant size secret key for encryption. The constant size secret key is generated and stored by the patients. A patient can send request to any doctor available in the healthcare system.

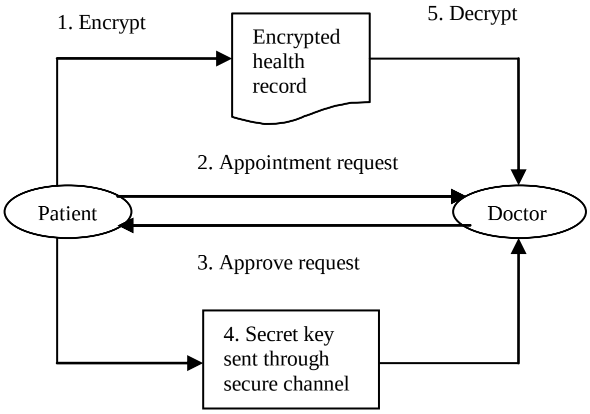

Fig 1: Communication between patient and doctor

- Patient encrypts and stores the PHR in cloud with constant size secret key
- Patient Requests for appointment with doctor
- Doctor approves appointment if he is available
- After doctor approval secret key is sent through secure channel like email from patient to doctor
- Using secret key doctor can view entire PHR

3.3Communication between patient and patient

The communication flow between patient and another patient is shown in fig 2. A patient can send request to any patient available in the healthcare system. After approval by the owner, the secret key is sent to the requester through secure channel. The requester can view the personal details of the owner by decrypting the health record by the secret key.

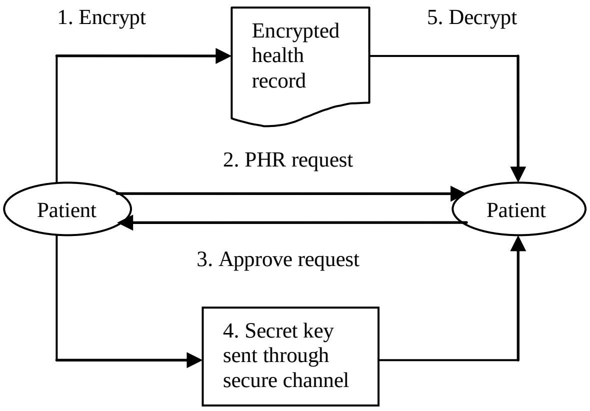

Fig 2: Communication between patient and patient

- Patient encrypts and stores the PHR in cloud with constant size secret key
- Patient Requests other patient secret key for viewing his PHR
- PHR owner can approve or reject the request
- If the request is accepted the secret key is sent to requester email a address
- Using secret key requester can view basic details of PHR owner

3.4 Architecture Diagram

The system is accessible by three users namely admin, doctor and patient. The operations that can be performed by each user is shown in the fig 3.

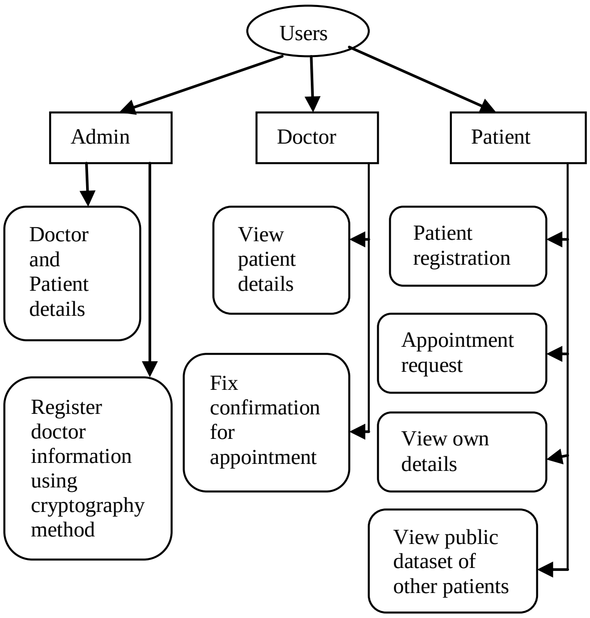
Users
Admin
Doctor
Patient
Doctor and Patient details
Register doctor information using cryptography method
View patient details
Fix confirmation for appointment
Patient registration
Appointment request
View own details
View public dataset of other patients

Fig 3: Architecture Diagram of PHR system

3.5 Data Encryption and Decryption

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. The algorithm used here makes use of binary division in which two reverse operations are possible. The secret key is also converted to binary and operations are performed.

3.7 Algorithm

Encryption Algorithm

Step 1: Generate the ASCII value of the letter
Step 2: Generate the corresponding binary value of it
Step 3: Reverse the 8 digit's binary number
Step 4: Take a 4 digits divisor (>=1000) as the Key
Step 5: Divide the reversed number with the divisor
Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the cipher text.

Decryption Algorithm

Step 1: Multiply last 5 digits of the cipher text by the Key.
Step 2: Add first 3 digits of the cipher text with the result produced in the previous step
Step 3: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number
Step 4: Reverse the number to get the original text i.e. the plain text

Symmetric key encryption is used for encryption of data. This encryption technique is known as binary transformed encryption.

- Converts data to binary value and performs operation
- Works by repeating the same defined steps multiple times
- Secret key encryption algorithm
- Algorithm is reversible

The operations involved in the algorithm are

- Generating ASCII value
- Generating Binary value
- Binary Division

This algorithm is used to encrypt and store health records because health record contain large data, if complex algorithm is used the time consumption for performing encryption and decryption increases.

4. EXPERIMENTAL RESULTS

The system is developed in windows environment using NetBeansIDE 7.4(Java 1.6) with JDBC connectivity. The cloud environment is set by Eucalyptus software. The performance of the algorithm is compared with other available symmetric and asymmetric algorithms. The number of fields in the PHR is taken into account for encryption and decryption and the computational time and memory usage is analysed.

4.1 Comparison Based on Computational Time

The computational time comprises of time taken for encryption and decryption. The values are taken by storing and retrieving PHR with different number of fields. Table 1 shows computational time in seconds for proposed algorithm, Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) using various number of fields in PHR.

Table 1. Comparison based on computational time

Number of fields in PHR	Proposed algorithm	AES	RSA
10	0.4 sec	0.8sec	0.9 sec
20	0.5 sec	0.9 sec	1 sec
30	0.6 sec	1 sec	1.1 sec
40	0.7sec	1.2 sec	1.23 sec

Fig 4 shows the comparison between the algorithm proposed which is a symmetric key encryption, AES algorithm(symmetric key encryption) and RSA algorithm(asymmetric key encryption).

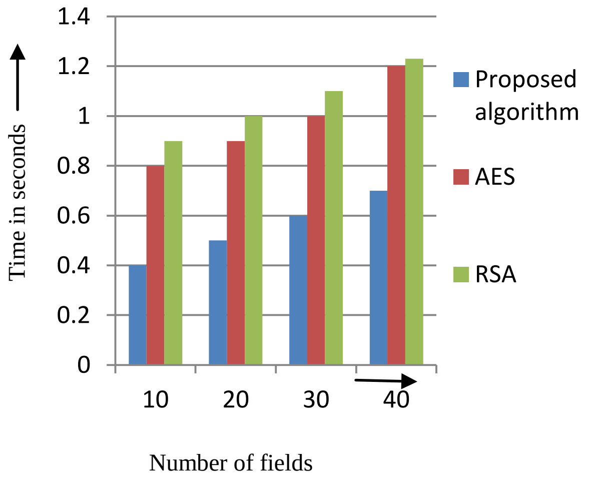

Fig 4: Comparison based on computational time

In that, the proposed system takes less computational time when compared to other algorithms.The computational time of the system increases by 57% compared to symmetric key encryption(AES algorithm) and 62% compared to asymmetric key encryption(RSA algorithm).

4.2 Comparison Based on Memory Usage

For an algorithm to execute, the system requires certain amount of memory space.The memory space used for performing encryption and decryption operations for different fields in PHR using different algorithms is given in Table 2. The memory usage is calculated in terms of kilobytes(KB).

Table 2. Comparison based on memory usage

Number of fields in PHR	Proposed algorithm	AES	RSA
10	1 kb	1.4 kb	1.5 kb
20	1 kb	2.2 kb	2.3 kb
30	1.5 kb	2.5 kb	3 kb
40	2 kb	2.8kb	3.2kb

Fig 5.shows the comparison between the algorithm proposed, AES algorithm(symmetric key encryption) and RSA algorithm(asymmetric key encryption). Comparison is done by storing and retrieving PHR with different number of fields. In that proposed system takes less memory usage when compared to other algorithms. The overall memory usage is less than 40% compared to other existing algorithms.

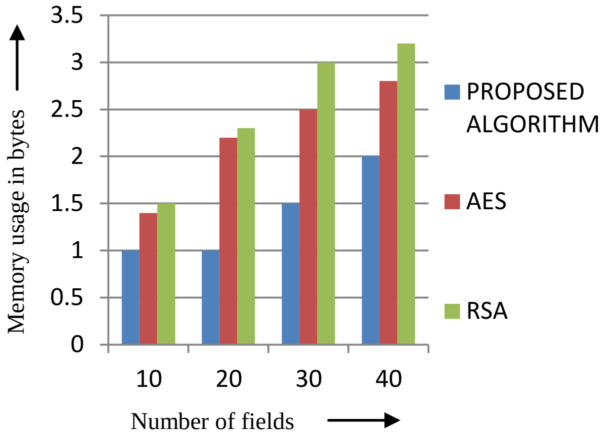

Fig 5:Comparison based on memory usage

The memory usage of the system is less than 36% compared to symmetric key encryption(AES algorithm) and 42% compared to asymmetric key encryption(RSA algorithm).

The system proposed takes less computation time and less memory for performing encryption and decryption. The computational time increases by 59% and the memory usage decreases by 39% compared to other symmetric and asymmetric key encryption methods.

5. CONCLUSION AND FUTURE ENHANCEMENT

The proposed system provides the technique of encrypting the health record data before uploading into the cloud to ensure data security. Doctor retrieves the whole health record data and patient retrieves personal data in the record by performing decryption using the secret key sent to them over the secure channel. It also provides trusted computing environment with an authentication service which prevents data access by unauthorized users. The proposed system uses symmetric key cryptographic algorithm and it is compared with available symmetric key and asymmetric key cryptographic algorithms. The results show that symmetric encryption algorithm used in the system takes less computation time and memory usage. The future enhancement of the project is to enable updating health record and building separate protocol for key transfer.

6. REFERENCES

[1] Cheng Kang Chu, ShemanS.M,Chow, Wen GueyTzdeng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 468-477, Feb. 2014.

[2] Ming Li, Shucheng Yu, Yao Zheng, KuiRen and Wenjing Lou, “ Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan 2013.

[3] Ayushi,"A Symmetric Key Cryptographic Algorithm",International Journal of Computer Applications, vol 1, no. 15, pp. 0975-8887, 2010.

[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] Hans Lohr, Marcel Winandy, Ahmed Regha, "Securing the E HealthCloud", International Conference on Trusted Systems 2009 (INTRUST'09), 2009.

[6] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," master's thesis, Worcester Polytechnic Inst., 2011.

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

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