

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.643 – 649

RESEARCH ARTICLE

SECURING PUBLIC HEALTH RECORDS IN CLOUD COMPUTING PATIENT CENTRIC AND FINE GRAINED DATA ACCESS CONTROL IN MULTI OWNER SETTINGS

Vaishali Sunagar¹, Chandrakanth Biradar²

Department Of Computer Science, PDA Engineering College, Gulbarga, Karnataka, India
Assistant Professor, Department Of Computer Science, PDA Engineering College, Gulbarga, Karnataka, India

¹ vaishalisunagar2323@gmail.com; ² cbiradar@rediffmail.com

Abstract— *The PHR is defined as the Public Health Record, this PHR enables the patients to manage their own medical records in the centralized way, and (PHR) emerged as a patient-centric model helps in the health information exchange. With the emergence of cloud computing PHR records are stored into the cloud, it reduces the operational cost. By storing the PHRs in the cloud, the patients lose the physical control to their personal health data, so that which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers, in the encryption it is challenging to achieve fine grained access control to the PHR record in a scalable and efficient way, hear each patient, their PHR data should be encrypted so that it is scalable with the numbers of users. also there are multiple owners(patients) in a PHR system And all the owner would encrypt her PHR files using a different cryptographic keys, so it is important to reduce the key distribution, To enable the fine grained and scalable access control for the PHRs hear (AES) .Advanced encryption standard encryption algorithm is used*

Keywords— *PHR (Public Health Record), Cloud Computing, Fine Grained and Scalable Access Control, Encrypt, Cryptography*

I. INTRODUCTION

Public Health Record (PHR) is an emerging patient-centric module for health information exchange, which is often outsourced to be stored at a third party application vendors, such as cloud providers. PHR enables patients to manage their own medical records, prior to storing the records in cloud server they are encrypted using encryption algorithm which ensures the patient's full control over their PHR. Storing PHRs in Cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. A PHR Service allows a patient to create, modify, manage and control personal health records in a centralized place through the web, from anywhere and at any time, can also share the data with wide range of users.

II. LITERATURE SURVEY

An extensive literature survey is conducted to investigate the various approaches for managing the patient records. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to Authorized users. In order to achieve secure scalable and fine grained data access control in Cloud Computing authors used the combination of different types of algorithms viz., Attribute Based Encryption (ABE), proxy re-encryption, and lazy re-encryption [1].

A cipher text policy attribute based encryption scheme with efficient revocation, construction uses linear secret sharing and binary techniques as underlying tools are used, each user is assigned a unique identifier, therefore user can be easily revoked by using his/her unique identifier [2]

Multi-authority ABE scheme specifies that multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors requires that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase M. et al., given a solution which removes the trusted central authority, and protects the users' privacy [3].

The challenges of preserving patients' privacy in electronic health record systems, security in the systems should be enforced via encryption as well as access control. Furthermore we argue for approaches that enable patients to generate and store encryption keys, so that the patients' privacy is protected should the host data center Be compromised [4].

III. EXISTING SYSTEM

In the existing system, PHR model has multiple owners (patients) who may encrypt their records according to their own ways. By using different sets of cryptographic keys each user obtains keys from every owner who's PHR has to be read would limit the accessibility since the patients are not always online.

Another method is central authority to do the key management on behalf of all PHR owners (patients), this requires too much trust on single authority.

DRAWBACKS OF EXISTING SYSTEM

1. There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.
2. Non-availability of authorization for the accessibility of health records which leads to an insecure data manipulation.

IV. PROPOSED SYSTEM

A secured framework for patient-centric information and a suite of mechanisms for data access control to PHRs has been proposed. To achieve fine-grained and scalable data access control for PHRs, we leverage advanced encryption standard (AES) techniques to encrypt each patient's PHR file and use the security policy to allow the access of the data.

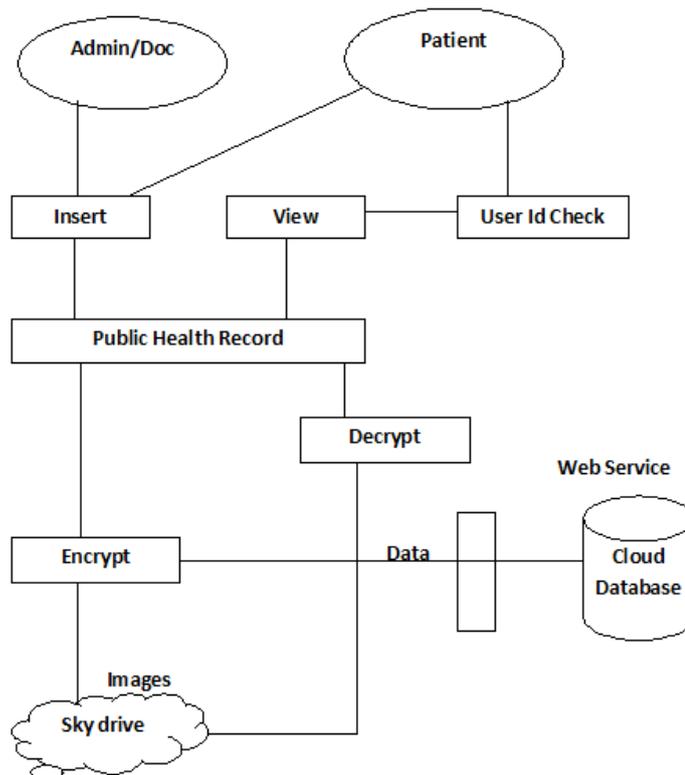


Fig. 1: Block diagram of the proposed system

ALGORITHM USED

Advanced Encryption Standard (AES) is a symmetric block cipher which uses the same key for both encryption and decryption. The algorithm allows a variety of block and key sizes, and not just the 64 and 56 bits of DES block and key sizes, the block and key size can be chosen from 128, 160, 192, 224, 256 bits... The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys 128, 192, 256 bits.

For encryption the number of rounds depends on the chosen key length. The key length 128 bits uses 10 round, the key length 192 bits uses 12 round, the key length 256 bits uses 14 rounds.

For encryption each round consist of following 4 stages

1. Substitution Bytes
2. Shift Rows
3. Mix columns
4. Add Round Key

For decryption: each round consists of the following four stages

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Step1: The substitute bytes stage uses an s-box to perform a byte-by-byte substitution of the block, there is a single 8-bit wide s-box used on every byte, this s-box is permutation of all 256 8-bits values, s-box constructed using defined transformation of values in $GF(2^8)$,

Step 2: The shift rows stage provides a simple permutation of the data, the state is treated as a block of columns, this step provides for diffusion of values between columns. It performs a circular rotate on each row of 0,1.2 and 3 places for respective rows,

Step 3: Operates on each column individually, each byte is replaced by a value dependent on all 4 bytes in the column

Step 4: The add round key stage which is simple bitwise XOR of the current block with a portion of the expanded key,

MODULES USED

The following three modules are

1. *PHR Owner/ patient module*
2. *Data confidentiality module*
3. *Cloud Server module*

PHR Owner/patient module: The main goal of this module is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely public clouds and private clouds according to the different users' data access requirements. PHR service providers encrypt patients' data, PHR services should give patients (PHR owners) full control over the selective sharing of their own PHR data.

Data Confidentiality module: The owners upload encrypted PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the public clouds to access and under a selected set of data attributes that allows access from users in the private clouds. Only authorized users can decrypt the PHR files.

Cloud storage module: The main function of cloud server is to create an interface between the application and users. The authentication of the user name and password is carried out. If user is authentic then he/she gets access to his/her records.

ADVANTAGES OF THE PROPOSED SYSTEM

The proposed system has the following advantages

- Provides higher level Data confidentiality
- On-demand revocation
- Write access control
- Scalability and usability
- To provide faster access information
- Quick and easily find out information of the patient details
- It provides an easy platform for medical data sharing between healthcare and patient.

APPLICATIONS

The applications of the AES system spans the following areas

- Multi level Hospital Management
- Health Care Website
- National health data center
- Any time access of medical data
- Privacy protections of patients

V. RESULTS AND ANALYSIS

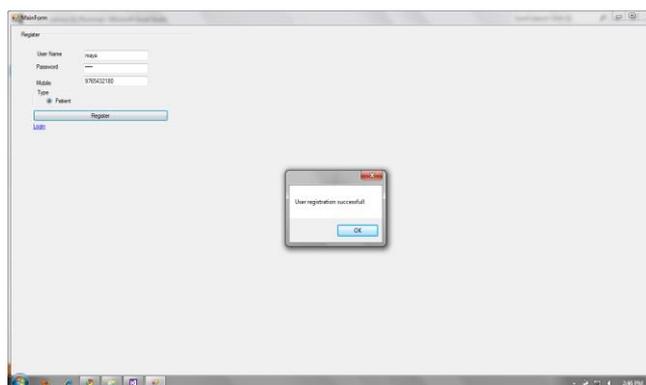


Fig1.Patient registration

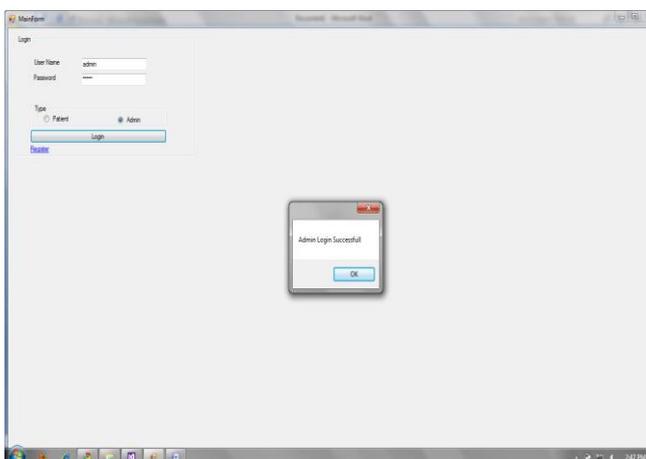


Fig2.Admin login

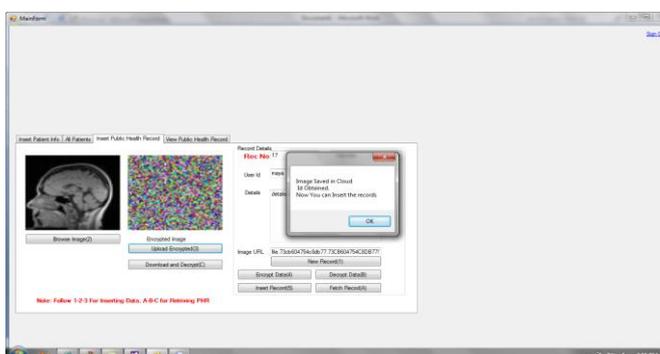


Fig3. Encryption

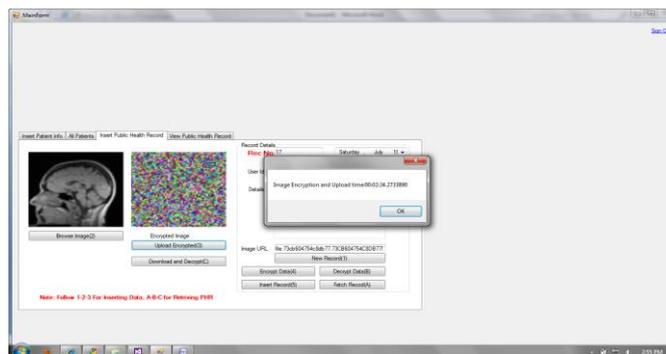


Fig4. Encryption Time

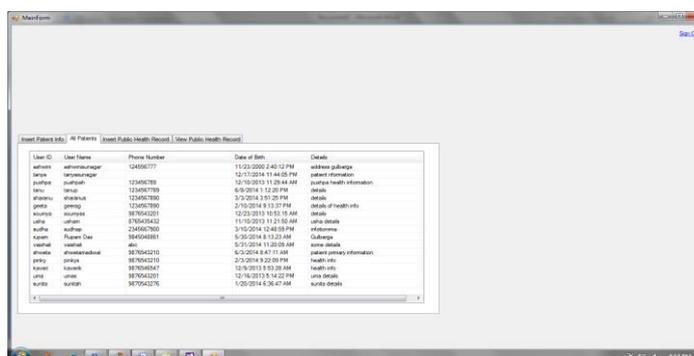


Fig5.view all patients

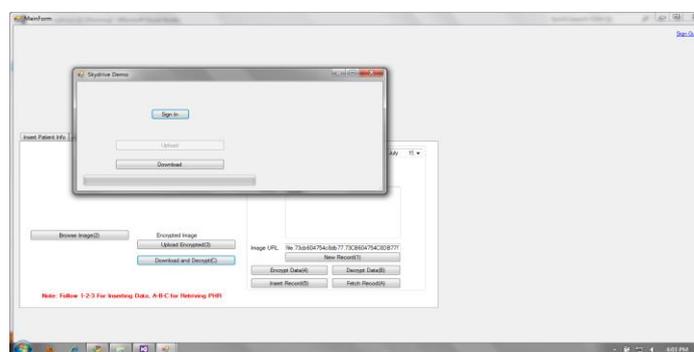


Fig6. decryption

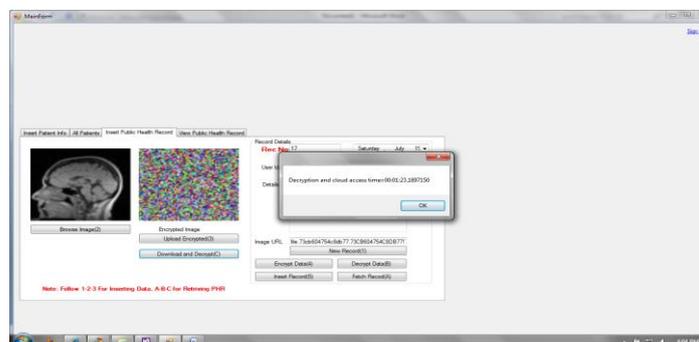


Fig7. Decryption time

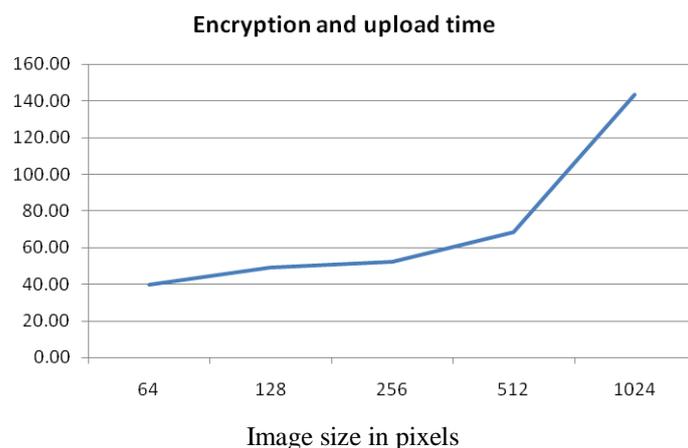


Fig8. A line graph of encryption and upload time(sec) versus image size in pixels

VI. CONCLUSION

The proposed method overcomes the drawbacks of the existing system and provides higher security level by using Advanced Encryption Standard (AES) encryption algorithm. This approach allows the users to maintain the data in a secured cloud environment by meeting the goals like data confidentiality, write access control, on-demand revocation, etc.

It also makes sure that the secret data of the patient is accessed and used by only authorized persons, providing highest level of security.

REFERENCES

1. Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable, and fine-grained data access control in cloud computing. In: IEEE INFOCOM 2010 (2010)
2. Liang, X., Lure. Lin, X., Sheen, X.S.: Cipher text Policy attribute based encryption with efficient revocation. Technical Report, University of Waterloo (2010)
3. Chase. Chow, S.S.: improving privacy and security in multi-authority attribute Based encryption nicks 2009, pp.121-130(2009)
4. Benaloh, J., Chase, M., Horvitz, E., Lauter, K.: Patient controlled encryption: ensuring privacy of electronic medical records. In: CCSW 2009: Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 103–114 (2009)
5. Identify –based encryption with Efficient Revocation Alexandra Boldyreva VipulGoyal.
6. Secure Management of Personal Health Records by Applying Attribute-based encryption Luan Ibraimi, Muhammad Asim, Milan Petkovic
7. Dynamic and Efficient Key Management for access Hierarchies Mikhail J. Atallah, Keith B. Frikken, and Marina Blanton
8. Authorized Private Keyword Search Over Encrypted Data in Cloud Computing Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou
9. Authorized Private Keyword Search Over Encrypted Personal Health Records in Cloud Computing, Ming Li, Shucheng Yuy, Ning Cao