International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Enable Security and Privacy to PHR with Access Control in Cloud Computing

Mrs .Tambe Puja M and Mr. Shaikh N. S.

Department of Computer Engineering Vishwabharti Academy’ s College Of Engineering Ahmednagar, Maharashtra

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

The researchers have given top priority for data security for well and smooth transmission of data over network by application of encryption strategies along with actual data. In this paper, the need to secure the data for patient monitoring by using AES and MD5 algorithms. In the field of modern healthcare environment, automation has emerged to be more necessary to preserve data for future needs the facts about employers (doctors), employees (staffs) and customer (patients). Hence doctors in need of such a stored voluminous information’ s about a particular person and securely share to patient on need. The clinical and other facts about a person is indeed to be private (trust worthy) and should not be revealed by any other private identity. In order to prevent issues like breaches and malware attacks on cloud, this innovative scheme helps in high level security to safeguard the files or reports that are stored on the cloud. Medical data is a central part of diagnostics in healthcare information systems nowadays. An aim is to not only privacy but also system’ s scheme try to make modification of access policies or file attributes, and break-glass access under emergency situations. The paper proposes Extensive analysis and experimental results on hospital staff management and patient records with help of some cluster technique also security and efficiency of PHR is main concern.

***Keywords**: Encryption; PHR; access policies; medical record ; cloud computing; privacy;*

Introduction

Personal Health Record(PHR), where PHR is meant to securely make storage in cloud environment for uninterrupted anytime, anywhere remote access availability In order to assure the privacy of PHI, the propose work is on efficient and Secure Patient according Access Control scheme which allows data requesters to have different access privileges based on their roles also doctor to manage records. Here the Cloud computing means on demand access and storage of data and programs over the internet instead of using computers hardware and software.

Personal Health Record (PHR) service is an private data from patients perspective. For patients health information need to be stored and exchange in confidential manner. Some standard like Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations have two crucial provisions in protection of healthcare privacy. The Privacy regulations create to assure that patients have more control over their health information and set limits the use and disclosure of health So this paper presents model that also secure storage with analysis and transfer of the information. It allows patients to create, update and manage personal with medical information. Also they can provide health care providers their data’ s control and share their medical information with other users as well . provide the security to Personnel Health Records (PHR) files using semi trusted proxy re-encryption services, and eliminate the insider attacks like collusion attack, bruited force attack as well as SQL injection attack. In this research work to design and implement a security and privacy mechanism health care system such as, data confidentiality, data integrity and finegrained access..

Objective

1. To protect Data confidentiality
2. To protect patient’s Identity
3. User controlled read write access and revocation is the two main security objectives or concerns for any electronic health record model.
4. The main objective of our model is to grant secure patientcentric PHR access and efficient key management simultaneously.

Motivation

1. It is Integration of PHR with cloud service provides the following benefits: (1)Reduced cost, (2)Medical resource sharing and exchange, (3)Dynamic scalability

of resources, (4)Enhanced flexibility, (5)Elimination of device limitation.

2. The proposed scheme for providing confidentiality and secure sharing of PHRs through the public cloud.

3. I made observation that People used PKE for Encrypting data. Due to the slower operations and the larger key sizes it becomes inefficient and then the SKE, PRE uses the same keys for encryption and decryption. But drawback of this scheme is, each file category is encrypted with distinct secret key so every time key needs to be provided whenever doctor tries to update file. Then ABE used for encryption that created bottleneck as computing load is heavy. Therefore there is need for implementation of new cryptosystem.

Problem Statement

A patient self-controllable multi-level privacy-preserving cooperative authentication in computing systems. An approach to resist various privacy attacks such as collusion attack, bruited force attack as well as SQL injection attack that can be performed while sharing PHR file by the patient/doctor to obtain the users security by encrypting file and Decrypting file and granting access permission to various user for PHR in cloud environment.

Literature Survey

Chu et al.[2] proposed system of a new public key cryptosystem which able to aggregate any set of secret keys to generate here one single compact aggregate key by encompassing the power of all keys as being aggregated. But did not focus on how it can help patients to have fine grain access controlled and revocation of access and at the same time how to maintain confidentiality, authentication and integrity of their PHRs.

Kuo et al. [3] proposed in their work patient-centric access control PHR data covered. The proposed scheme ensures the following security properties: (1) confidentiality (2) integrity, (3) authenticity (4) access control, and revocated access control using symmetric key crypto and proxy re -encryption (PRE) scheme. But the main drawback of this scheme is, each file category is encrypted with distinct secret key so whenever they try to update PHR categories, patient have to provide the corresponding secret keys. Besides this, the scheme has proxy reencryption scheme which requires data owners to have too much trust on the proxy that it only converts cipher texts according to his instruction. A PRE scheme allows data owners to the proxy the ability to convert the cipher texts encrypted under his public key into ones for data users. Hence it is desired that proxy doesn't reside in the storage server. This increases communication overhead since every decryption requires separate interaction with the proxy.

Chen et al. [5] have an EHR solution, relying mainly on smart cards and RSA that allow patients to store their medical records on hybrid clouds. In this approach, patients' medical records are stored in two types of clouds the hospitals private cloud also the public cloud. The authors discussed two use cases. The firstly is medical records being accessed by owner of the data i.e., the doctor have records. They can directly access the records from their private cloud or from the public cloud.

The secondly is that of the medical records being viewed by other hospitals, who must seek permission from the data owner before they can access the records. The authors have also provided a solutions for emergency situations. However, the shortcomings of this approach is that data owners, i.e., doctors have access control not patient for the medical records and their computing load is heavy.

Leng et al. [6] proposed a solution that allows patients to specify a policy to support fine -grained access control. They primarily utilized Conditional Proxy Re-Encryption to enforce sticky policies and provided users with write privileges for PHRs. When users finish writing data to their PHRs, they sign the modified PHRs. However, users sign the PHRs using the signature key of the PHR owner and it is therefore difficult to correctly verify who signed the PHRs.

Proposed System

A. Architecture

a) Trusted Authority (TA): It generates the public and secret key parameter The TA is responsible for attributes' keys issuing, revoking, and updating. It grants differential access rights to individual users based on their attributes and roles. TA also maintains an index type records where it stores the location . Authorization of health service providers (e.g., Hospital, urgent care) are denoted as trusted parties.

b) CSP: It provides data outsourcing services and consists of data servers and data service manager. The responsibility of the data storage server is to serve and retrieve data according to authorized users' request..

c) Registered user: Patient and doctors who is registered to the trusted authority is considered as registered user. A registered user is responsible for defining attribute-based access policy and encrypting the sensitive

d) Data-access requester: Cloud users who request to access some specific PHI are called the data-access requester. They need to decrypts the encrypted data if and only if he can successfully completes the access policy.

The encrypted data is stored in a centralized storage, health cloud, for future access. Based on the major perations, the proposed scheme can be classified into four major steps, as shown in Fig 2.

- (PHR collection): In this initial step, using different body sensors, or data stored on public cloud is accessed, PHI may be sensed and ready to be transmitted to the trusted eHealth care service provider.
- (Secure data communication): In this step, public key cryptography is used to securely transfers collected PHI to the eHealth care service provider. Owner securely transfer a secret key to the trusted eHealth care provider, if he authorized the service provider to build-up the access tree.

- Shared PHR to the cloud storage and control accessed : After the data classification, encrypted data securely transfers to the cloud storage, shows as ' Health Cloud' in Fig 1.Here we also find best suitable to particular patient and also updated record PHR is again encrypted and shared to patient and doctor provides key for it.

The classification of the data requester as health worker, physicians, researchers, insurance companies, and agencies, etc. Some of them only need the accumulated number of patients in a specific area, some need disease related syndromes, age and gender specific characteristics, while others may need medication details. Figure 1 shows possible access structures based on different privacy levels, where intermediate nodes work as a logic gates. "

Aim at achieving the following security objectives. Access trees based on different data privacy level

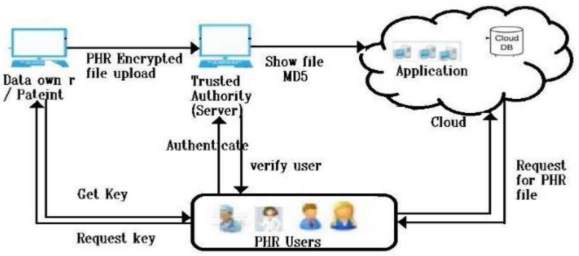

Fig 1: System architecture

1. Patient-centric access control: The system should provide patient-centric access control, where patient can
decide who can get the access to his or her stored PHI.
2. PHR integrity, source authentication and nonrepudiation: All accepted messages need to be delivered
unaltered, and the origin of the messages should be authenticated by the Healthcare service provider. To ensure the non-repudiation, the patient cannot refute the validity of a PHR afterward.
3. Prevention of Cipher text-only attack: The system should be secured enough to prevent recover of the plaintext from a set of stored cipher texts.
4 Provide patient privacy: Privacy is one of the important concerns from a patient perspective. Illegal disclosure andimproper use of patient PHI can cause legal disputes and undesirable damaging in patients personal life.
5 Resistant to collusion attack: If multiple users collude,generally they may be able to make decryption of acipher text by combining their attributes. Users can notget any access to the encrypted data even by sharinginformation in a group.
6 Resistant to Denial-of-Service (DoS) attack: The DoS attack may be caused due to the large groups of legitimate users access the Health records at the same time, or the attacker continuously launch false traffic with a High Data Rate (HDR). The system should ensure acceptable QoS level to resist this DoS attack

B. Software Requirements Specifications

1) Hardware Requirements PHR Owner
   •Pentium IV Processor and above S1= {do, d1, F1, F2, F3, d2, d3, d4, e2}
   •Minimum RAM 512 MB d0: Registration & Login
   •Minimum 40 GB Hard Disk f1: Encryption of PHR
2) Software Requirements f2: Decryption
   •OS Requirements: Windows 7 onwards f3: Secret key generation
   •Net Beans 7.3.1 d1: upload PHR file
   •JAVA JDK 1.7 and above d2: store PHR file and attribute
   •MySQL Server 5.5

Algorithm

- Input : Upload PHR files and Share
- Output: Encrypted data is seen and downloaded with Key
- Algorithm: Make registration using parameters. Login information is authenticated. Choose PHR file to upload
- Encryption: AES for Data Encryption is done by data block of 4 columns of 4 bytes is state key is expanded to array of words. that rounds 9 or 11 or 13 in which state undergoes: byte substitution (1 S-box used on every byte), shift rows (permute bytes between groups/columns), mix columns (subs using matrix multiply of groups), add round key (XOR state with key material), view as alternating XOR key, scramble data bytes, initial XOR key material incomplete last round, with fast XOR and table lookup implementation
- Also access policy set by user Label of each partition, for instance personal information, medical information, insurance information, and prescription information. Role that has access to any particular

partition (any role may be given access to more than one partitions), like doctors may be given access to medical in-formation . Initial members of family/friends to give access. Default access (if any) in case of new member

- AES Decryption: The AES decryption is not same to encryption since steps done in reverse but can define an equivalent inverse cipher with steps as for encryption but using inverses of each step with a different key schedule works since result is unchanged when swap byte substitution shift row swap mix columns, add (tweaked) round key
- MD5 Algorithm Key generation

1. Arrange all input data D into the matrix Format and saved into the Log files.
2. Consider a selected data m act as a new selected data. position m gets changed after allocated Time period. If data get hacked or leaked by some Malicious users Data leakage occurs. To analyze the leakage data and prevent using the data analysis (tamper Analysis).
3. To get original data to call the revert Back function.
4. When the user calls that dishonest file, hash Function gives to the user a previous Data.
5. And log file maintained at the admin side.
6. Return True.
7. Output - The hashed value is changed then the log will generate

Mathematical Model

- PHR Owner

S1= {do, d1, F1, F2, F3, d2, d3, d4, e2}
d0: Registration & Login
f1: Encryption of PHR
f2: Decryption
f3: Secret key generation
d1: upload PHR file
d2: store PHR file and attribute
d3: transmit parameters
d4: set control on file access

- Staff(PHR User):

S2 :{ e1, e2, e3, F2}
e1: PHR file access request
e2: PHR file download
e3: Request key to decrypt
F2: Decryption ()

- Setup or Server:

S3={F1,F3,t1,t2,t3,d3,e3,d3}
T1: Re-Encryption calling F1function
T2: Update & mange keys
T3: Distribute key

- Cloud: Set (C)={d1,d2,d4,e1,e2,e3,c0,c1}

C0-store encrypt file (Storage of encrypting file using El – Gamal Algorithm)
C1-send encrypted file to data user

- Function Encryption ()

Input: Attribute Value (Attr).
Get Byte [] (B1) of that Attr.
Generate Public Key (Pk).
Perform Encryption on B1.
Convert B1 into string (EAttr).

- Function Decryption ()
  Input: Encrypted attribute value (EAttr)

Convert EAttr into byte [] (B2).
Generate Private Key.
Perform Decryption on B2.
Convert B2 into string (DAttr).

- Secret Key ()

Input: Private Key (see Decryption) and No. of Authority (NAuth) =10.
Get Length of private key: Length = PrivateKey.Length.
To become private key multiple of NAuth (i.e. 10) pad it by zero (0).
S1UnoinS2= {do,d1,F1,F2,F3,d2,d3,d4,e1,e2 ,e3}
S2UnoinS3=
{do,d1,F1,F2,F3,d2,d3,d4,e1,e2,e3, t1,t2,t3}
S1UnionS3=
{ do,d1,F1, F2,F3,d2,d3,d4,e2,e3 ,t1,t2,t3}
C1= S1intersectionS2= {d1, e2, F2}
C2= S1intersectionS3= {F1, F3, d0, d3, d4}
C3 = S2intersectionS3={e3}
S1intersection C= {do, d1, d2, d3, d4, e2}
S2 intersection C= {d1, e1, e2, e3}
S3 intersection C= {t1, t2, t3, d0, d3, e3, d4}
C1 intersection C= {d1, e2}
C2 intersection C= {d0, d3, d4}
C3 intersection C= {e3}

- **Success Condition**: Success system when the PHR file
will access with authorized user without any problem.
- **Failure Condition**: Failure system when the server will
fail during the download the file.

Result and Discussions

We propose a sensitive policy; privacy based approach to the PHR files sharing.

- For minimizing the loss of the uploaded files from unauthorized patient/user.
- For minimizing the disclosure risk.
- To maintain the diversity among the uploaded PHR files.
- Minimized security on files on sharing sites The performance of this method based on the access policy set to each PHR file which is shown in Table 1 for different access policy result is successful. The Encryption /Decryptiontime, Key generation and total time of process should beminimum for good performance

Table 1: Shows That Access Policy Set To The Phr File Uploaded

Sr.n o	**Patient Name**	**File name**	**Access Policy**	**Result**
1	Jhon	Neurotherapy_Treatment.doc	Doctor/ Patient	Successfu lly Apply Policy
2	Peter	Heart_Treatment.doc	Doctor/ Patient	Successfu lly Apply Policy
3	Ganesh	Daily_Treatment_Plan.doc	Receptionist	Successfu lly Apply Policy
4	Linda	Tablets_Plan.do c	Receptionist	Successfu lly Apply Policy

The result is to meet expected output on given experimental data file. The system Privacy Based Securely shared Of Personal Health Records a Method in the Cloud that needs to upload patients information in encrypted form on cloud with policy set on cloud and that file is decrypted with key based on authentication also policy based access. The expected result is to generate key, encryption of file with secure storage on cloud to avoid misuse of information some accessibility rights are set and key is provided based on that to guarantee confidentiality. Also valid system user cannot obtain the re-encryption parameters for a PHR partition for which access is not granted to the user. The server gives user access permission and keys to user. The Actual output works with patient registration and login also patient upload PHR file and set policy send on doctor desk for checking. The PHR file is encrypted before uploading. Decryption done with key asked from user firstly policy is checked the key provided for decryption of data.

Table 2: Encryption Process Time In Existing System And Proposed System Different File Size

File name	File Size	Existing System (encryption in sec)	Proposed System (encryption in sec)
Abc.txt	80kb	4sec	2sec
Xyz.txt	100kb	6sec	4sec
Pqr.txt	150kb	8sec	6sec
Report.txt	300kb	15sec	12sec

The Table 2 shows better performance of proposed system as compared to exiting with minimum time in encryption for different file size. And so the turnaround time will also be less. Sample file is tested with 80kb, 100kb, 150kb, 300kb thatrequired 2sec, 4sec, 6sec, 12sec in proposed system instead of 4sec, 6sec, 8sec, and 15sec in existing system

Conclusions

The increase of storage on cloud and work on distributed system that need to ensure healthcare systems based on cloud storage should be privacy based, how to protect PHRs stored in the cloud is a central question. Also it enforces a patient-centric access control to different portions of the PHRs based that to be easily accessible. In this proposed method, also discuss how the confidentiality, and authentication of PHRs can be achieved with hospital that manages and analysis doctor specialization and diseases with which patients are mostly affected with help of data mining techniques. This system also enables a owner of data to exercise complete control over their PHRs and perform revocation of access rights. Furthermore we can do project work on real time application using the hospital record based on global server that is to be easily accessible and potential to patient and Doctors.

Acknowledgment

I express my profound thanks to all those who helped me directly or indirectly in making paper. Finally I would thank to all our friends and well-wishers who supported me in completing work successfully I am especially grateful to our guide for him as he had given time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

References

[1] M. Ali, A. Abbas, M. U. S. Khan and S.U. Khan ” SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud” , IEEE Transactions on Cloud Computing, 2018

[2] C. Chu, S. Chow, and W. Tzeng, “ Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage” , IEEE Transactions on Parallel and Distributed Systems, 2014, 25 (2): 468- 477.

[3] Kuo-Hsuan Huang, En-Chi Chang, and Shao-Jui Wang, “ A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud” , Fourth International Conference on Networking and Distributed Computing, 2014.

[4] Dixit, G. N. “ Patient Centric Frame Work For Data Access Control Using Key Management In Cloud Server” , International Journal of Engineering, 2 (4), 2013.

[5] Chen, Y. Y., Lu, J. C., & Jan, J. K. “ A secure EHR system based on hybrid clouds,” Journal of medical systems, 36 (5), 3375 -3384, 2012.

[6] Leng, C., Yu, H., Wang, J., & Huang, J. “ Securing Personal Health Records in the Cloud by Enforcing Sticky Policies,” TELKOMNIKA Indonesian Journal of Electrical Engineering, 11 (4), 2200-2208, 2013.

[7] 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.

[8] Chen Danwei, Chen Linling, Fan Xiaowei, He Liwen, Pan Su, and Hu Ruoxiang “ Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing” , China Communications, Supplement No.1, 2014.

[9] Ming Li, Shucheng Yu, and Yao Zheng, “ Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption” , IEEE Transactions on Parallel and Distributed Systems, 24(1), pp. 131-143, 2013.

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

[11] M. Chase, and S.S.M. Chow, “ Improving Privacy and Security in Multi-Authority Attribute-Based Encryption” , Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009.

[12] M. Chow, M. Chase “ Improving Privacy and Security in MultiAuthority Encryption” , Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009.