International Journal of Computer Networks and Communications Security

VOL.2, NO.1, JANUARY 2014, 15–21
Available online at: www.ijcncs.org
ISSN 2308-9830

Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control

Aderonke Justina. Ikuomola[1] and Oluremi O. Arowolo[2]

[1] Department of Mathematical Sciences, Ondo State University of Science and Technology, Ondo State

[2] Department of Computer Science,Tai Solarin College of Education, Omu Ijebu

E-mail: [1]deronikng@yahoo.com, [2]oluodedeji@yahoom

ABSTRACT

Cloud computing paradigm is one of the popular Health Information Technology infrastructures for facilitating Electronic Health Record (EHR) sharing and EHR integration. Healthcare clouds offer new possibilities, such as easy and ubiquitous access to medical data, and opportunities for new business models. However, they also bear new risks and raise challenges with respect to security and privacy aspects. Ensuring the security and privacy is a major factor in the cloud computing environment. A Secured Cloud based aided medical system is a program designed to aid standard and effective use and access of patient records anytime it is required by medical practitioners. In this paper, a Secured e-Health System called SECHA is proposed. SECHA comprises of five basic component namely; patient, PHR/object, Access Control Module, User/Subject and Cloud. This proposed system ensure the security of electronic health records stored in the cloud using Homomorphic Encryption to secure patients medical records and Bilayer Access Control to gives access right to the records.

Keywords: *Access Control, Cloud Computing, e-Health, Homomorphic Encryption, Security.*

1 INTRODUCTION

Electronic Health Record (EHR) is a digital record shared across different healthcare settings, by network-connected enterprise-wide information systems called EHR systems [8]. Electronic form of personal health records opens new kind of threats to information leakage because electronic data are easy to copy, especially when the records are online. Thus, most Personal Health Records (PHRs) are kept local and specific to one point of care. As such, most existing PHRs only provide the patient with limited insight into parts of the patient's health care information. On the other hand, electronic health records help make health care safer, cheaper, and more convenient by providing complete health history, avoiding repeated tests, and allowing appropriate authorities to have ready access to PHRs anytime anywhere. People usually go to the healthcare centers nearby their residence for health services and their health information is kept secured in the local databases of those healthcare centers. However, patients sometimes may need to get services from different healthcare centers for various reasons, including but not limited to unavailability of service on holidays, need for specialized care at specialized centers, travelling away from usual residential area, and moving residence. The stored health information in a healthcare center is usually accessible only to healthcare personnel of that center. For every healthcare center, there are separate systems to record patients' health information, and information flow between systems is limited. For example a patient having health records in three different hospitals (A, B and C). Doctors of a hospital A cannot access the patient's health records that are stored in two other hospitals B and C. As a consequence, patients often need to retell their medical history and redo tests whenever they encounter a new health care provider [3].

Cloud computing is the use of computing resources which may be hardware or software that are delivered as a service over a network. Cloud computing entitles resource sharing to achieve best utility over a network. Resources are shared on a need basis in the best possible manner under clouds. The Personal Health Record (PHR) sharing among a wide range of personnel has been identified as an important application in the field of cloud computing. The data outsourced to service providers are largely consumed by wide variety of individuals. Hence the need of security and privacy in personal health records is an important issue. This brings the idea of encrypting the data before outsourcing to the servers. To ensure best policy, it is the patient herself who should encrypt the data and determines which users shall have access in what manner [1].

With the widespread use of EHR, building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community.

2 LITERATURE REVIEW

[3] Devised novel privacy management architecture called P3HR, for a patient-controlled personal health record system which uses strong authentication mechanisms with smart IC cards. The IC card stores personal information in an encrypted form and the stored data is made anonymous so that an intruder cannot associate a record with a specific individual. From the prototype implementation, only username/password based authentication was used which is not efficient enough.

[2] Proposes the encryption schemes with strong authentication for users to share partial access rights with others and to perform various searches over their records. They considered the encryption schemes that enable patients to delegate partial decryption rights and that allow patients to search over their health data. They proposed a design framework that is referred to as Patient Controlled Encryption (PCE) as a solution to secure and private storage of patients' medical records which allows the patient to selectively share records among doctors and healthcare providers. The system prevents unauthorized access to patients' medical data by data storage providers, healthcare providers, pharmaceutical companies, insurance companies, or others who have not been given the appropriate decryption keys. The main demerit of the system is that it is not efficient when the patient is absent or unable to authenticate and it doesn’t provide an efficient scenario for emergency access. Others include: potential key management overhead and no support for a key escrow agent in emergencies cases.

A role-based and time-bound access control model (RBTBAC) that provides more flexibility in both roles and time dimensions to control the access of sensitive data was presented by [8]. They combined the role-based access control and time-bound key management to develop a privacy-aware and dynamic key structure for role-based privacy management of EHR data and employed a time tree method for generating time granule values, offering fine granularity of time-bound access authorization and control. This model is more suitable for EHR system since it offers high-efficiency and better security and privacy for patients.

[4] Presented a novel framework of access control to realize patient-centric privacy for personal health records in cloud computing. The framework addresses the unique challenges brought by multiple personal health record (PHR) owners and users, in that they greatly reduce the complexity of key management when the number of owners and users in the system is large. They utilize multi-authority attribute-based encryption to encrypt the PHR data. The problem with this framework is that it does not support more expressive owner-defined access policies and doesn’t enable users to process encrypted data without decrypting it.

A Health Cloud model which is based on Cloud Computing and wireless sensor networks (WSN) concept were proposed by [5] and they also proposed to have the security mechanism inside the cloud to guarantee data confidentiality, integrity, security and fine grained access control using Cipher text-Policy Attribute Based Encryption (CP-ABE) algorithm for the system. The proposed system was able to remove the time consuming burdensome task of collecting patient’s data manually and possibility of typing errors.

[7] Discussed the development in patient centric model and cloud computing in PHR management and proposed a Third Party Auditor (TPA) to verify the cloud server which is used to store and process the PHR. Homomorphic encryption with data auditing was used to verify the trustworthiness of TPA. Although the TPA helps PHR owners to evaluate the risk of their subscribed cloud data services and also help cloud service provider to improve their cloud based service platform but it cannot be fully trusted since the members in it can access the sensitive data.

[6] Addressed the security and privacy concerns of cloud-based PHR system by integrating advanceed cryptographic technique, such as Homomorphic Encryption into PHR system to enable patients protect their valuable healthcare information against partially trustworthy cloud servers and by assigning fine-grained, access privileges to selected data users. The main limitation in this technique is

their key management and policy which are too complex.

[1] Made use of Multi Authority Attribute Based Encryption (MA-ABE) scheme to provide multiple authority based access control mechanism due to its vast access. The proposed system is designed to provide identity based encryption facility using attribute based encryption scheme which handles distributed attribute based encryption process.

3 AN ARCHITECTURE OF THE PROPSED SYSTEM

The architecture of a Secured e-Health in cloud using Homomorphic Encryption and Acces Control (SECHA) is presented in figure 1. SECHA comprises of five basic component namely; patient, PHR/object, Access Control Module, User or Subject and Cloud.

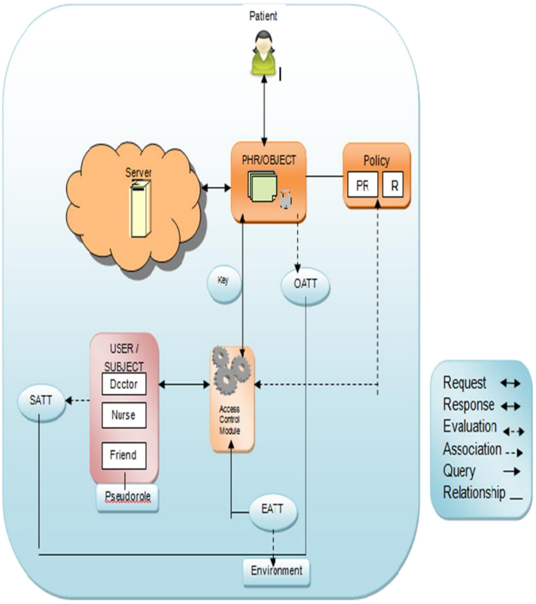


Fig. 1. Architecture of a Secured e-Health in the cloud using Homomorphic Encryption and Access Control (SECHA)

A. Patient

Patient is the person whose medical information is presented in the patient health record (PHR). He is responsible for creating the PHR and has complete right on the data.

B. Patient Health Record (PHR) or Object (O)

PHR/O is the collection of information about an individual's health stored in electronic format. PHR/O is also associated with a predefined finite set of attributes OATT i.e. patient name and medical record number. The PHR/O is encrypted by the patient (the owner of the PHR/O) using homomorphic encryption before it is stored in the cloud and can be accessed by the users/subjects.

i. Homomorphic Encryption

A Homomorphic Encryption is the conversion of data into cipher text that can be analyzed and worked with as if it were still in its original form. Homomorphic encryption plays an important part in cloud computing, allowing patients to store encrypted PHR files in a public cloud and take advantage of the cloud provider's analytic services. The scheme prevents rogue insiders from violating privacy and prevents accidental leakage of private information. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (i.e. without decryption), the client is the only holder of the secret key. When the result of the operation is decrypted, it is the same as if it had carried out the calculation on the raw data.

The homomorpic encryption scheme algorithm consists of four steps:

1. Key Generation - creates two keys i.e. the privacy key sk and the public pk.
2. Encryption - encrypts the plaintext m with the public key pk to yield ciphertext C.
3. Decryption - decrypts the ciphertext C with the privacy key sk to retrieve the plaintext m
4. Evaluation - outputs a ciphertext C of f(m) such that Decrypt (sk,P) = f(m).

Key Generation: KeyGen(p,q)
Input: p,q Є P
Compute n = pq
Choose g Є $Z^*_{n^2}$ such that

$$\gcd(L(g^{\lambda} \bmod n^2),n) = 1 \text{ with } L(u) = \frac{u-1}{n}$$

Output: (pk, sk)
Public key: pk = (n,g)
Secret key: sk = (p,q)

Encryption: Enc(m, pk)
Input: m Є Z_n
Choose r Є Z^*_n
Compute $c = g^m \cdot r^n \bmod n^2$
Output: c Є Z_{n^2}

Decryption: Dec(c, sk)
Input: c Є Z_{n^2}
Compute $m = \frac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$

Output: m Є Z_n

C. Cloud

The cloud is a model for enabling on-demand network access to pool of resources. The cloud server is where all sensitive clinical data about the patient are stored and manipulated. The PHR/O stored in the cloud can also be accessed by the patient and users/subjects from the cloud.

D. User or Subject

These are the subjects (users e.g. doctor, nurse, friend, e.t.c.) that need access to the PHR/O. Subjects (users) are associated with a predefined finite set of attributes SATT. Each attribute is represented by a name, along with its associated value. Examples of subject attributes could be provider, department, and location.

E. Access Control Module

The Access Control Module is a decision engine that uses a Bilayer Access Control model to determine the users that have access right to the PHR/O.

i. The Bilayer Access Control model (BLAC)

In BLAC, subjects are associated with pseudoroles, which are composed of a set of static attributes (i.e. role, department, location, e.t.c.), and objects are associated with policies, which specify how attributes are to be considered for access requests. When an access request is made, the policy associated with the requested object is first checked to see whether the requester has the required pseudorole or not. If the requester holds the right pseudorole, rules (i.e. access mode) within the policies are then checked for additional constraints to approve or deny the access request. This two-step process, which inspired the name BiLayer Access Control, permits fine-grained access decisions. Figure 2 shows the access requests evaluation flow in BLAC model.

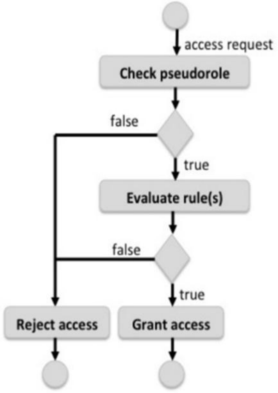


Fig. 2. Access Request Evaluation Flow in the BLAC Model

BLAC is formally described using the following tuple:

M = (S;O;E;A; PR; P; SPR;OP)

Here, S is Subject that access object, O is Object that is accessed by the subject, E is Environment, A is Action, PR is pseudorole, P is Policy, SPR is subject-pseudorole assignment relation, and OP is object-policy assignment relation. More details are provided below:

- E: is the environment, which describes the access context under which access may be provided. Environments are associated with a predefined finite set of attributes EATT. Examples of environment attributes could be access time and system mode.
- A: is a set of actions, which subjects' request, to be performed over objects. Actions are also associated with a predefined finite set of attributes AATT. Examples of action attributes are read and modify.
- PR: is a set of pseudoroles that are composed of n attributes. Each subject is assigned to a pseudorole for initial coarse-grained access control.
- P: is a set of access policies for fine-grained

access control. A policy consists of two elements: a Boolean function called PseudoRole, and a set of zero or more rules. Each rule has four sub-elements also defined as a Boolean function specifying the range of values that must be satisfied for the Subject, Object, Action, and Environment attributes.

Policy Structure

```
<Policy>
    <PseudoRole>…</PsuedoRole>
     <Rule>
       <Subject>…</Subject>
      <Object>…</Object>
      <Action>…</Action>
      <Environment>…</Environment>
    </Rule>
</Policy>
```

- SPR: is the subject-pseudorole assignment relation that is a one-to-many mapping from pseudoroles to subjects.

OP: is the object-policy assignment relation that is a one-to-many mapping from policies to objects.

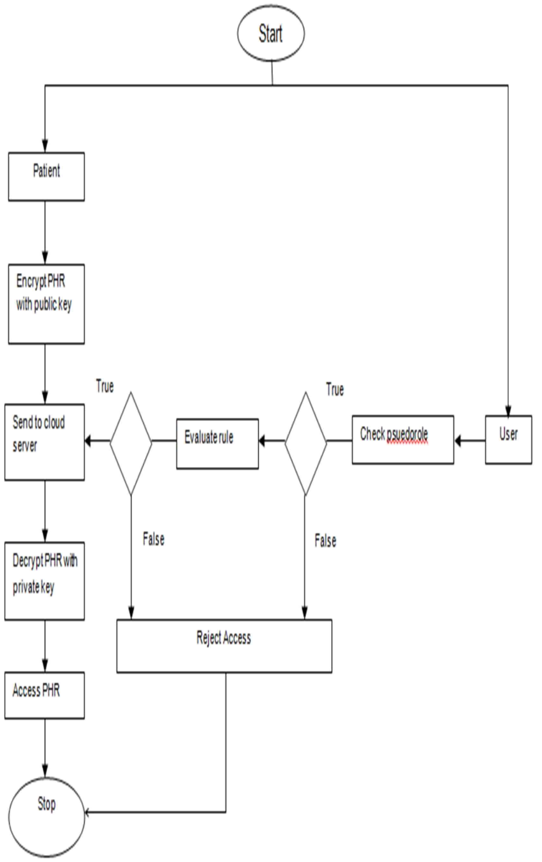
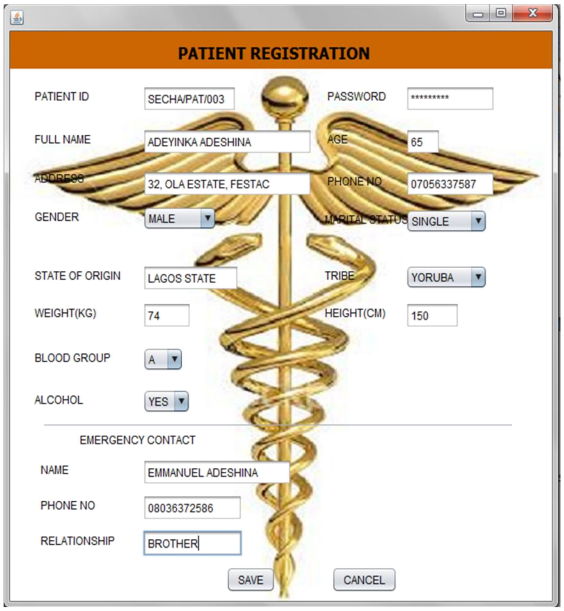


Fig. 3. SECHA Flow Chart

4 IMPLEMENTATION AND SYSTEM PERFORMANCE

The design was implemented with Java Programming Language and MySql database Engine on a Pentium® Dual-Core CPU T4500 with CPU of 2.30Gz and 2.0GB of RAM.

Figure 4(a & b) shows the registration page of the system where new user or patient can be added by the administrator in order for them to be able to use the system.



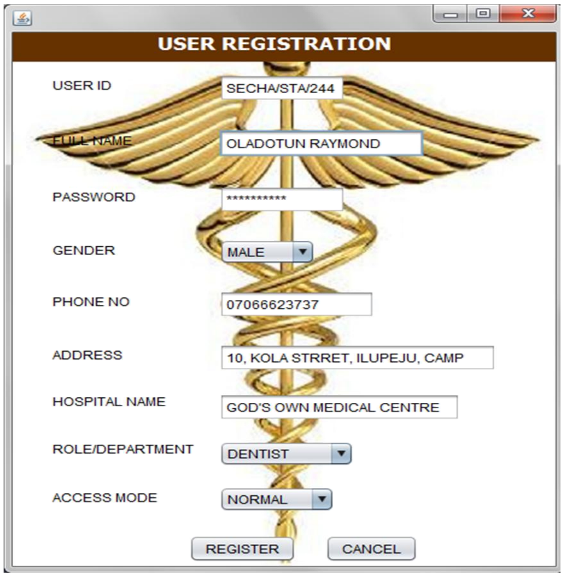
PATIENT REGISTRATION

PATIENT ID	SECHA/PAT/003	PASSWORD	*********
FULL NAME	ADEYINKA ADESHINA	AGE	65
ADDRESS	32, OLA ESTATE, FESTAC	PHONE NO	07056337587
GENDER	MALE	MARITAL STATUS	SINGLE
STATE OF ORIGIN	LAGOS STATE	TRIBE	YORUBA
WEIGHT(KG)	74	HEIGHT(CM)	150
BLOOD GROUP	A		
ALCOHOL	YES		

EMERGENCY CONTACT

NAME	EMMANUEL ADESHINA
PHONE NO	08036372586
RELATIONSHIP	BROTHER

Fig. 4a. Patient Registration Page

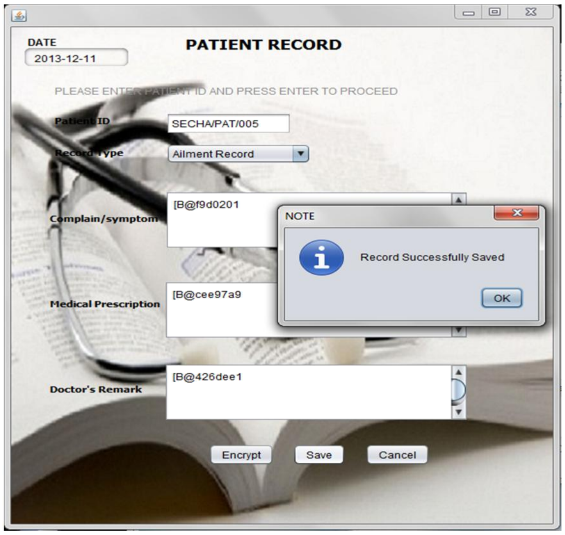


USER REGISTRATION

USER ID	SECHA/STA/244
FULL NAME	OLADOTUN RAYMOND
PASSWORD	**********
GENDER	MALE
PHONE NO	07066623737
ADDRESS	10, KOLA STRRET, ILUPEJU, CAMP
HOSPITAL NAME	GOD'S OWN MEDICAL CENTRE
ROLE/DEPARTMENT	DENTIST
ACCESS MODE	NORMAL

Fig. 4b. User Registration Page

In Figure 5, the patient and doctors/specialist are allowed to gain access to this page based on their psuedorole. The record is encrypted before saving in order to prevent unauthorized user from accessing the record.


PATIENT RECORD

DATE: 2013-12-11

PLEASE ENTER PATIENT ID AND PRESS ENTER TO PROCEED

Patient ID: SECHA/PAT/005

Record Type: Ailment Record

Complain/symptom: [B@f9d0201

Medical Prescription: [B@cee97a9

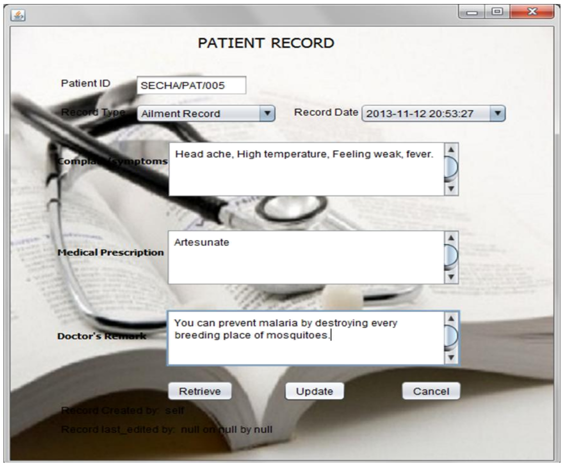
Doctor's Remark: [B@426dee1

NOTE

Record Successfully Saved

Fig. 5. New Record Page

In Figure 6, the patient and doctors/specialist are allowed to gain access to this page but can only edit the record he/she created. The record is retrieved from the server as an encrypted text and then decrypted with the private key before editing can take place.


PATIENT RECORD

Patient ID: SECHA/PAT/005

Record Type: Ailment Record

Record Date: 2013-11-12 20:53:27

Complain/symptoms: Head ache, High temperature, Feeling weak, fever.

Medical Prescription: Artesunate

Doctor's Remark: You can prevent malaria by destroying every breeding place of mosquitoes.

Record Created by: self

Record last_edited by: null on null by null

Fig. 6. Decrypting the record for editing

5 CONCLUSION

In this work, a cloud based patient privacy system has been presented. PHR is stored in the cloud, and can be accessed through a web portal by multiple owners and users. The patient which is the owner of the PHR encrypts it and stores the ciphertext in the cloud server. When an access request is made, the policy associated with the requested object is first checked to see whether the requester (user) has the required pseudorole or not. If the requester holds the right pseudorole, rules within the policies are then checked for additional constraints to approve or deny the access request.

The program thus produce assistance to the physicians or a medical practitioners, since it facilitate their work when compared with the manual system presently in use. With the use of this proposed system large number of patient will be attended to at a limited time and the patient records can be accessed anywhere in the world with security of the patient data ensured.

In future, it will be of interest to improve on this system by integrating an emergency rule access to the system.

6 REFERENCES

[1] Abraham S. E. and Gokulavanan R. (2013). “Ensuring Privacy and Security in Data Sharing under Cloud Environment,” International Journal of Computer Applications Technology and Research, 2(2), 188-194.

[2] Benaloh J, Chase M., Horvitz E. and Lauter K. (2009). “Patient controlled encryption: ensuring privacy of electronic medical records,” in CCSW ’09, 103–114.

[3] Huda M.D.N, Sonehara N. and Yamada S. (2009). ”A Privacy Managemaent Architecture for Patient-Controlled Personal Health Record System,” Journal of Engineering Science and Technology, 4(2), 154 – 170.

[4] Li M., Yu S., Ren K. and Lou W. (2009). “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in SecureComm’10, 89–106 (2009).

[5] Onik F. A., Salman-Al-Musawi S. S, Anam K. and Rashid N. (2012). “A Secured Cloud based Health Care Data Management System,” International Journal of Computer Applications, 49(12), 0975 – 8887.

[6] Soubhagya B, Venifa M. G, Jeya A. and Celin J, (2013). “A Homomorphic Encryption Technique for Scalable and Secure Sharing of Personal Health Record in Cloud Computing,” International Journal of Computer Applications 67(11), 0975 – 8887.

[7] Vidya S., Vani K. and Priya D. K. (2012). “ Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing,” International Journal of

Engineering Research & Technology (IJERT), 1(10).

[8] Zhang R., Liu L. and Xue R. (2010). “Role-Based and Time-Bound Access and Management of EHR Data,” Security Comm. Networks, 1–21.