RESEARCH ARTICLE OPEN ACCESS

Securing Personalized Medical Data in Cloud Using Homomorphic Encryption

Sweta Agrawal[1], Aakanksha Choubey[2]
Department of Computer Science & Technology
CSVTU, Bhilai
Chhattisgarh – India

ABSTRACT
Cloud computing is an emerging technique growing rapidly day by day due to its low cost, reliability & less hardware usage. However the prospect of outsourcing an increasingly amount of data and computation raises various security and privacy concern. In this paper we deal with the cryptographic technique which is based on Homomorphic Encryption that allows computation on an encrypted data besides providing privacy. We try to implement Homomorphic Encryption in medical domain application and checked its security implications. However inefficiency in its computation and CPU utilization brings limitation for its practical use.
Keywords:- Cloud Computing, Homomorphic Encryption, PHR, AES.

I. INTRODUCTION

Cloud Computing is an emerging computing technology where application and all services are provided through Internet. Cloud Computing can be considered as computing paradigm having greater flexibility and availability at lower cost. According to the National Institute of Standards and Technology (NIST) in the USA, Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

The main issue with Cloud Computing is related to loss of privacy and loss of private data of customer and business by adoption of cloud services. Privacy Preserving is an on-going research area as sensitive information is now frequently stored in computer that are attached to Internet. Still there is lot of issue that need to be addressed especially of data security which should not be intercepted by others. In our approach, Privacy Preservation is adopted using Homomorphic Encryption. Data is secured by the fact that Homomorphic encryption allows computation on encrypted data. It is useful for real time application with crucial time constraints like Bio-medical application, financing and others.

The project development has the following objectives:

- Development of a scheme that can secure data and that allows processing through applications.
- Exploration of Homomorphic Encryption schemes to enable computing on the encrypted data by deeply concentrating on field homomorphism as preserve the structure of two objects operated on using the basic arithmetic operations.
- Integration of the above methods to produce the proposed framework that allows arbitrary computing on encrypted data.
- Implementation and evaluation of the framework in a Cloud Computing environment.

II. EXISTING SYSTEM

On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat prevent these unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to- end data confidentiality assurance in the cloud [2][3]. However, data encryption techniques used now a day prevent cloud from performing any meaningful operation of the underlying plaintext data, making the computation over encrypted data a very hard problem [4]. On the other hand, the operational details inside the cloud are not transparent enough to customers. As a result, these cloud servers behave unfaithfully and return incorrect results. Hence, limitation of existing encryption method demanded methodology that enables computation on data by cloud servers without compromising privacy.

III. PROPOSED SYSTEM

In this paper, we first identified the flaws in existing system that deals with privacy issue in Cloud Computing. Then, we proposed solution for preserving privacy for third party in Cloud [5]. The scheme proposed is Homomorphic Encryption that maintains confidentiality of personal information sent by the cloud users.

The proposed scheme offers three significant features: Enhanced privacy management, competency, Reduced server computation.

A. Enhanced privacy management

With the employment of Homomorphic Encryption functions, the confidentiality of personal information is effectively guaranteed, which makes it difficult for attacker to recover the encoded personal information. B. Competency

As our proposed scheme does not allow third party to decrypt the personal information, third party process the information without knowing it which provides a high competency.

C. Reduced server side computation

The authentication process is carried out at third party. Server only provides information in encrypted manner.

IV. INTRODUCTION TO PERSONAL HEALTH RECORD SYSTEM

Personal Health Record (PHR) is emerged as a patient-centric model of health information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data centre [6]. PHR is an internet based application that allows people to access and co-ordinate their lifelong health information and make if appropriate parts of its available to those who need. PHR security and protection of its data have been of great concern and a subject of research over the years [7] [8]. There are many different forms of cryptographic mechanisms like Asymmetric encryption standard (AES), MD5 proposed to guarantee data security. In this work we propose a unique authentication and encryption technique using Homomorphic Encryption algorithm. In PHR data refers to the information that is collected, analyzed and stored as shown in figure 1.

Example: Medical history, List of medical problems, Medication history.

The medical record, either paper-based or electronic, is a communication tool that supports clinical decision making, coordination of services, evaluation of the quality and efficacy of care, research, legal protection, education, and accreditation and regulatory processes. It is the business record of the health care system, documented in the normal course of its activities [9]. The documentation must be authenticated and, if it is handwritten, the entries must be legible.

The system is designed to manage PHR with different user access environment. The data values are maintained under a third party cloud provider system. The data privacy and security is assured by the system. The privacy attributes are selected by the patients. The data can be accessed by different parties. The key values are maintained and distributed to the authorities.

All data for a patient's medical record is encrypted and stored in the cloud storage system [10]. The patient controls sharing and access to the record by sharing secret keys with specific provider. With Homomorphic Encryption the cloud can compute functions on the encrypted data and send the patient updates, alerts, or recommendations based on the received data.

V. FRAMEWORK FOR SECURE SHARING OF PERSONAL RECORDS

The system designed manages privacy management in cloud, which can prevent scrutiny of personal health information. The system is divided into six major modules [11]. These are:

A. Data Owner

Data owner in the system manages patient details and assigns access mechanism to various authorities. The data owner verify that his data is being correctly stored and properly maintained in the cloud since the data owner no longer possesses physical control of the data.

B. Cloud Server

Cloud server is the storage where the sensitive PHR is stored and manipulated. It requires greater concern to maintain the data privacy and correctness. The owner in the system uses the cloud server for data storage and maintenance of their PHR record.

C. Key Management

The key management module is used to manage key values used by several authorities. Key management includes key creation and distribution. Key values are uploaded by owner.

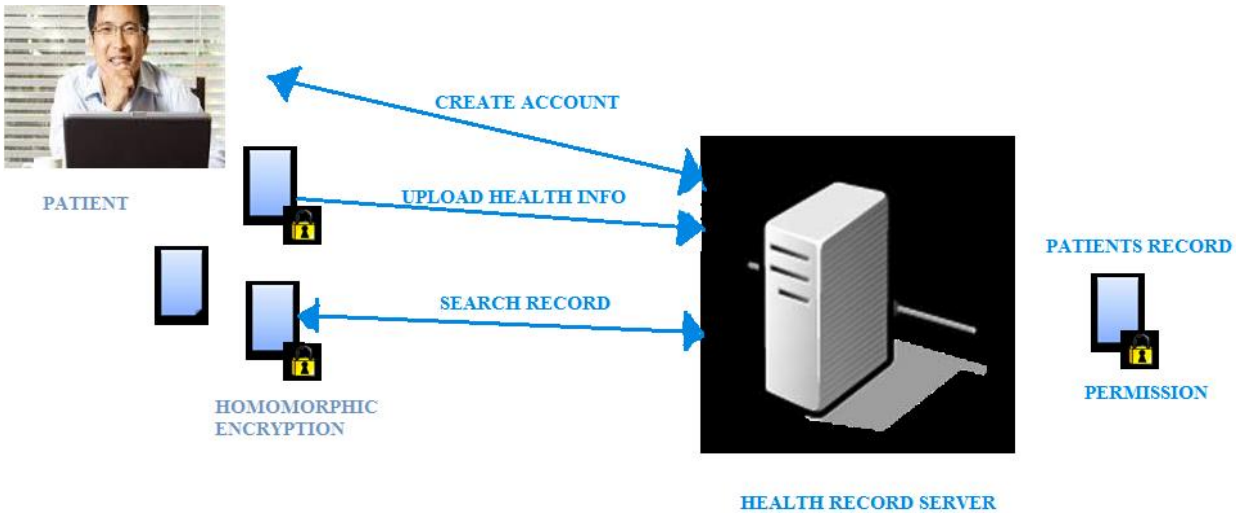

Fig. 1 Overview of PHR System

D. Security Process

It uses Homomorphic based operations. Each authority has different access mechanism based on their role. Data decryption is performed under user environment.

E. Authority Analysis

Authority Analysis module is designed to verify the user with their roles. Authority based key values are issued by key management server.

F. Client

Client is the person who creates his medical record and he has the complete rights on that data. Client can share his information with his friends or to the doctors.

VI. ALGORITHM

The process on cloud server can be represented by algorithm ProofGen [12] and the process on customer can be organized into three algorithms (KeyGen, ProbEnc, ResultDec). These four algorithms are summarized below and will be instantiated later:

A. KeyGen

The key generation algorithm Gen takes as an input the security parameter 1^{λ} and outputs a pair of keys (pk, sk), i.e. public key (pk) and private key (sk).

B. ProbEnc

The encryption algorithm Enc takes as an input the public key pk and message μ and outputs the ciphertext C.

C. ProofGen

It outputs a ciphertext c such that the ciphertext generated by Evaluate does not reveal anything about the data that it evaluates beyond the output value, even for someone who knows the secret key.

D. ResultDec

The decryption algorithm Dec takes as an input the private key sk and ciphertext c and outputs a message μ.

VII. IMPLEMENTATION

This project is implemented in Java and security is implemented using Homomorphic Encryption. Connect Apache Tomcat server 7.0 to the Net beans where the security code is implemented. From SQL database we import the data and on that data the security are implemented. Private and public keys are used to encrypt the data.

A prototype for PHR systems are developed in this section. The username and password is used to login. The patient or user can login only after completing the registration procedure. Figure 2 shows the screenshots of registration.

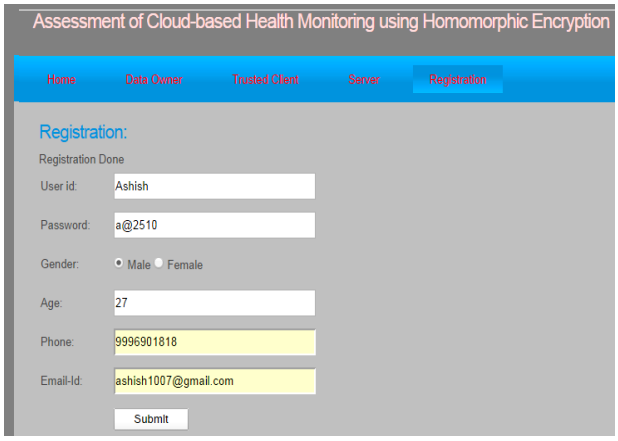

Fig. 2 Registration Page

Figure 3 shows the uploading of the health record that are being encrypted and stored. Here the client updates its health records that are stored with the specific period of time.

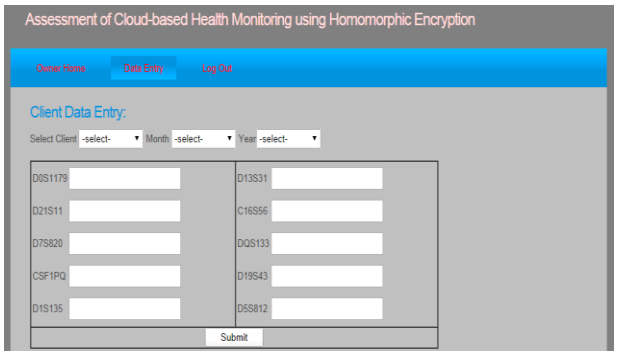

Fig. 3 Client Data Module Page

Figure 4 shows how the owner accessing the data of various clients and verify the data. The owner can access data of clients only if he have data key with him.

Fig. 4 Owner Verifying Data Page

The Homomorphic Encryption has the best encryption method to ensure security and privacy of shared data.

Figure 5 shows how data is encrypted and stored in cloud. Here we implement the Homomorphic scheme by encrypting database on cloud.

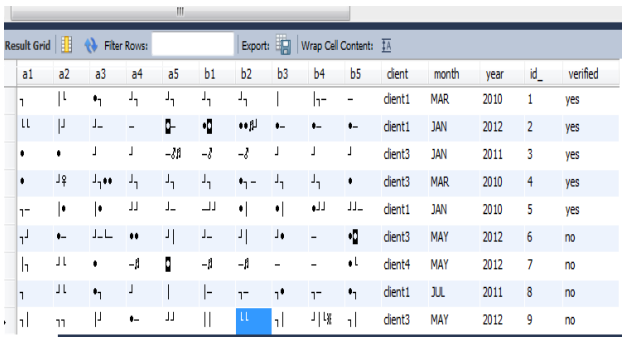

Fig. 5 Database on Cloud

VIII. CONCLUSION

In this paper we proposed a framework of secure sharing of personal health records by first addressing the security and privacy concerns of cloud-based PHR system. This is done by integrating advanced cryptographic technique, such as Homomorphic Encryption, into PHR system which not only provides privacy but also allows computation on encrypted data. By using appropriate cryptographic techniques, patients can protect their valuable healthcare information against partially trustworthy cloud servers. In the future work cryptographic techniques may enhance more efficient way to address the security and privacy issue of PHR systems by increasing efficiency of Homomorphic Encryption.

REFERENCES

[1] "Securing Personal Health Records in Cloud using Attribute Based Encryption". (April-2013). *International Journal of Engineering and Advanced Technology (IJEAT)* .

[2] "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium. (2010). *ser. IHI"10* , 220-229.

[3] Aderemi A. Atayero, O. F. (October 2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. *Journal of Emerging Trends in Computing and Information Sciences* .

[4] Gentry. (2010). Computing Arbitrary Functions of Encrypted Data. In n. 3. vol 53, *Communications of the ACM* (pp. 97-105).

[5] Grance, P. M. (2011). "The NIST Definition of Cloud Computing". *National Institute of Standards and Technology, U. S. Department of Commerce* .

[6] H. L¨ohr, A.-R. S. (2010). "Securing the e-health cloud". *Proceedings of the 1st ACM International Health Informatics Symposium* , pp. 220-229.

[7] H.-A. Park, J. H. (2011). "PKIS: practical keyword index search on cloud datacenter,". *EURASIP Journal on Wireless Communications and Networking* , 1-16.

[8] M. Karthika, J. V. (JUN-2014). Retrieving Secure Data from Cloud Using OTP. *International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163* .

[9] M. Li, S. Y. (sept.2010). "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in

multi-owner settings,". *SecureComm"10* , 89-106.

[10] Noh, J. H. (2010). "Attribute-based access control with efficient revocation in data outsourcing systems,". *IEEE Transactions on Parallel and Distributed Systems, .*

[11] Q. Liu, G. a. (2012). Secure and privacy preserving keyword searching for cloud storage services. *Journal of Network and Computer Applications* , 927-933.

[12] S. Sobitha Ahila, D. (2014). "State Of Art in Homomorphic Encryption Schemes." . *Int. Journal of Engineering Research and Applications* .