A Enhanced Security Model Using an Hybrid Access Control Approach for Preserving the Privacy of Medical Big Data in a Healthcare Cloud

Mahima Rathore[1], Mr Ketan Khandelwal[2]
CSE dept Asst. Professor, CSE dept 12SDBCT, Indore

Abstract- Health care services are essential for the purpose of diagnosing and evaluating patient health check up. All the records of patient health check up is stored in database of cloud. Data theft, modification or editing of data can be possible if there is no security for that data. Electronic medical records need to be stored in a secure manner because it is consisting of patient's medical and personal data. There is a issue of intruders and attackers to attack on patient's medical record. Patient's personal information like his/her name, age, gender, blood group and his/ her medical history are stored on cloud and leakage of these personal information may lead to modification of data or data theft, which is the most significant security issue. This paper aims at preserving text data of medical record by using cryptographic technique like ECC and Blowfish. These techniques will be used for encrypting data randomly and also by random selection of any of the two techniques. After it for decryption of data similar process will work but ECC is used for even chunks of image and text data and Blowfish is used for odd chunks of text data. An implemented and improved approach called hybrid access control approach is used for healthcare cloud using RBAC and ABAC access control methods for privacy of personal health care data.

Keywords- Electronic medical data; ECC; Blowfish; RBAC; ABAC

I. INTRODUCTION

Large data of patient's information are stored on cloud which is in the form of text. Data can be of any form like machine generated data or sensor data for monitoring and supporting laboratory files etc. Electronic medical data is an emerging approach in the field of electronic health research. In health care service, electronic media record consisting of multimedia text data that is transmitted and communicated over insecure connection of internet, because that data is required by doctors for the treatment of patient. Electronic medical record pulls different informations of patient together to know there health details for further treatment and also if patient moves from one hospital to another then his/her health information is required by another doctor to be known for treatment. So, patient's information needs to be managed properly with proper updates for diagnosing health issues in patient.

with Health-care cloud computing server is a health care services which elaborates cloud computing infrastructure on the basis of health service providing with a cloud server so that legitimate user can communicate complete patient's information. Below figure illustrates, Health care cloud computing server which provides benefits for hardware and software both over internet.

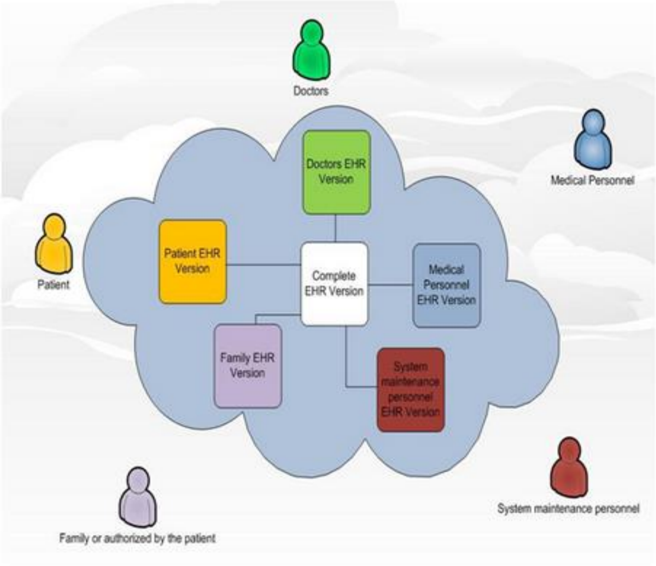
Doctors
Medical Personnel
Doctors EHR Version
Patient EHR Version
Patient
Complete EHR Version
Medical Personnel EHR Version
Family EHR Version
System maintenance personnel EHR Version
System maintenance personnel
Family or authorized by the patient

Fig.1: Health-care Cloud Computing Server

NIST, in the year 2009 defined about cloud computing, as it is a convenient and on-demand model which enables services of configured resources like storage, server, network etc. These are the visual models and require minimal management efforts [6] [7].

Similarly, different types of issues are configured with health care cloud computing in terms of security and privacy and the most significant among them are: lack of transparency, privacy protection, legal issue, and policy regarding issues, license issue and data protection issue [8].

Each issue among them offers with challenges which are abstracted as: challenges relevant to legal policy issues like reliability, compliances, liability and copyright. Another challenge is as data protection, applicable law and data portability. When talking about privacy protection, it is the protection of information which protect content of data by keeping in knowledge of user that where the data should be used and stored.

Normally, privacy consists of significant parameters like liability, compliance, trust and uncertainty. Lack in transparency is another important factor for physical storage of data. Another security challenge is related with cyber security which consists of information and command input and output, physical transparency etc.

Finally, relation among third party, consumers and utilities are defined for the proper need of secure computing . In this paper, a Hybrid approach is used for healthcare cloud using RBAC and ABAC access control with using encrypted technique like ECC and Blowfish.

II. RELATED WORK

A. Study of existing work:

Hadeal abdulaziz al hamid et al. In[1] focused on secure personal healthcare data by using fog computing and proposed a protocol called as tri-party one-round authenticated key protocol by creating a session key between participants on the basis of bilinear pairing cryptography by implementing decoy technique for secure storage of image.

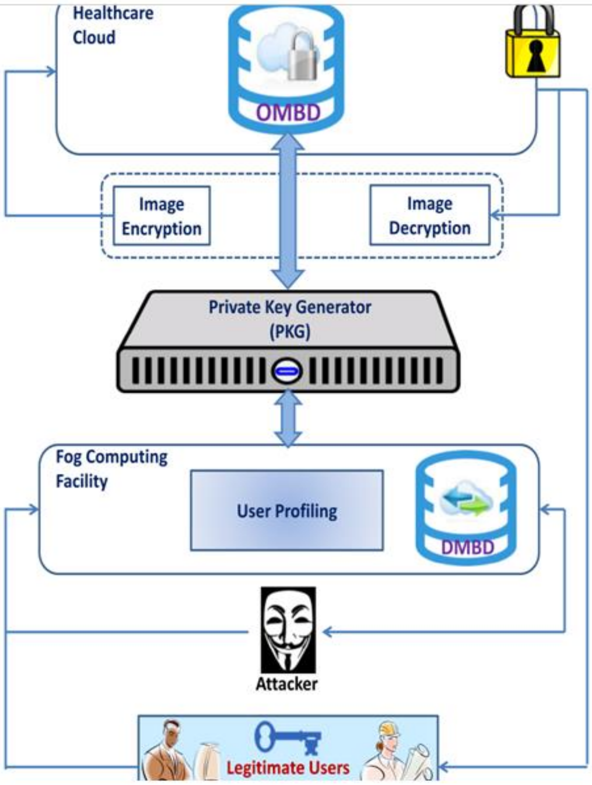

Fig.2: Existing Work

TABLE 2.1: Comparative Table

TITLE	SUMMARY	LIMITATIONS
Security issues in Service Model of Cloud computing environment [2]	Described about the cloud security issues.	Not using cryptographic techniques
Extending the cloud with fog: Security challenges and Opportunities [3]	Proposed fog computing model which extends cloud computing as an opportunity.	Need to improve security measures.
Cloud security and privacy model for providing secure cloud services [4]	Provided layered architecture for securing cloud services	Need to improve access control method.
Security algorithms for cloud computing [5]	Described algorithms for the security of cloud computing	Used AES algorithm for the encryption.

III. PROBLEM STATEMENT

A. Problem Overview

Many of the challenges are faced in healthcare medical record like data protection, privacy from data theft, challenges related to transformation of information, storage related issue.

Each issue among them offers with challenges which are abstracted as: challenges relevant to legal policy issues like reliability, compliances, liability and copyright. Another challenge is as data protection, applicable law and data portability. When talking about privacy protection, it is the protection of information which protect content of data by keeping in knowledge of user that where the data should be used and stored.

B. Limitations of existing work

1. In existing work only image is used as a dataset for encryption and decryption process.

2. They have not chunk the image file. Chunking makes data more secure according to GFS(Google File System).

3. They have not shuffling and directly decoy data. 4. They have not used ECC and Blowfish cryptographic techniques together.

IV. PROPOSED SOLUTION

A. Proposed Work

Proposed work defines and overcome the issue of existing work. In existing work only image is used, and proposed work will be implemented using text dataset for encryption process.

Figure 3 describes about security and privacy of text data and describes security and privacy of image data.

Hybrid technique will be implemented and then permission will grant to user on the basis of some set limit of threshold value. This threshold value is set which will decide whether the user is attacker or genuine on the basis of Hybrid Technique which is the combination of Role Based Access Control (RBAC) and Attribute based Access Control (ABAC).

B. System Architecture

System Architecture consist of some essential steps

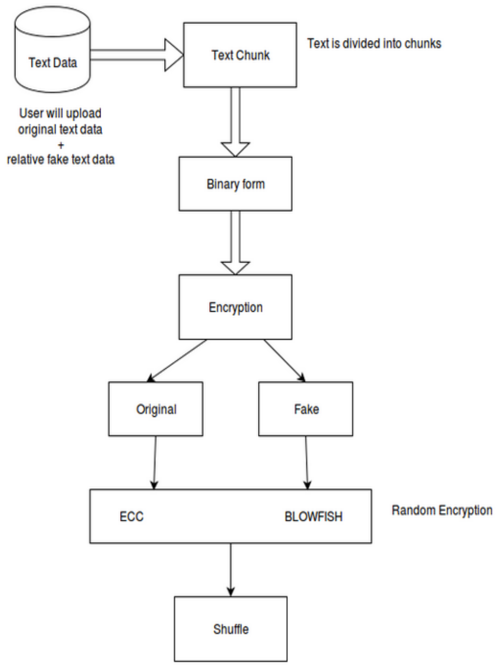
Text Data
Text Chunk
Text is divided into chunks
User will upload original text data + relative fake text data
Binary form
Encryption
Original
Fake
ECC
BLOWFISH
Random Encryption
Shuffle

Fig.3: System Architecture using text data

1. User will upload original text data and also relative fake data cloud over insecure internet connection.
2. After it data is divided into chunks in binary form.
3. Then encryption technique will be followed on original and fake data using ECC and Blowfish technique.
4. And, these cryptographic techniques will be applied randomly on any random data.
5. With it data will be shuffle for further process.

Steps for decryption of data:

a) At last for decryption process, authenticate user have the authority to decrypt data.

b) Information regarding decryption is provided to authenticate user.

c) Where user will be given information that:

- Even chunks will be decrypted using ECC algorithm.
- Odd chunks will be decrypted using Blowfish algorithm.

d) Process will be followed similar to the encryption process.

V. CONCLUSION

There is an issue of intruders and attackers to attack on patient’s medical record are a big challenge. Patient's personal information like his/her name, age, gender, Blood group etc are stored on cloud and leakage of these personal information may lead to modification of data or data theft, which is the most significant security issue.

Hybrid technique will be implemented in this paper which will grant permission to user on the basis of some set threshold value. This paper aims at preserving text data of medical record by using cryptographic technique like ECC and Blowfish.

In Future scope, we will store the Patient’s complicated information like X-ray, MRI, CT-Scan and all image kind of data into the healthcare cloud.

VI. REFERENCES

[1]. Hadeal abdulaziz al hamid 1 , sk md mizanur rahman, “a security model for preserving the privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography”. IEEE, September 28, 2017.

[2]. B.Hari Krishna, Dr. S. Kiran, G. Murali, R. Pradeep kumar Raddy, “Security issues in Service Model of Cloud computing environment”. International conference on computational science, 2016.

[3]. J Shropshire, ‘‘Extending the cloud with fog: Security challenges and opportunities,’’ in Proc. 20Th Amer. Conf. Inf. Syst., Savannah, Georgia, 2014, pp. 1–10.

[4]. Khalid EI Makkaoui*, Abdellah Ezzati, Abderrahim Beni-Hssane, ”Cloud security and privacy model for providing secure cloud services” IEEE, 2016

[5]. Akshdeep Bhardwaj, GVW Subrahmanyam, Vinay Avasthi, Hanumat sastry, “Security algorithms for cloud computing”, International conference on computational modeling and security, 2016

[6]. I. Foster, Y. Zhao, I. Raicu, and S. Lu, ‘‘Cloud computing and grid computing 360-degree compared,’’ in Proc. Grid Comput. Environ. Workshop, Austin, TX, USA, Nov. 2008, pp. 1–10.

[7]. P. T. Grance. (Oct. 2009). The NIST Definition of Cloud Computing. [Online]. Available: http://csrc.nist.gov/groups/SNS/cloud-computing

[8]. B. A. Akyol, ‘‘Cyber security challenges in using cloud computing in the electric utility industry,’’ Pacific Nortwest Nat. Lab., Washington, DC, USA, Tech. Rep. PNNL-21724, Sep. 2012.