

MedRec

Sunu Sukesan¹, Prof. Neelima P² and Dr. Mahalekshmi T³

Student, Final Year Master of Computer Application¹

Assistant Professor, Master of Computer Application²

Principal, Sree Narayana Institute of Technology³

Sree Narayana Institute of Technology, Kollam, Kerala

Abstract: *The objective of this project is to develop a web application which can perform high level of security feature with double encryption in it. We are aiming to develop a web application which shows the complete details of a doctor which the patient like to consult. It also helps the user to share their health reports with their consultants and can receive comments for that. The widespread acceptance of cloud-based services in healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs[2][3][8]*

Keywords: Access control, cloud computing, Personal Health Records, privacy, encryption

I. INTRODUCTION

The widespread acceptance of cloud-based services in healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs. The Secure Sharing of PHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re- encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyse and verify the working of Secure Sharing of PHR methodology through High Level Petri Nets (HLPN). Performance evaluation with regard to time consumption indicates that the Secure Sharing PHR methodology has potential to be employed for securely sharing the PHRs in the cloud[3][4] [5]

II. Background

A) Technologies used in this project

- **Eclipse** is an integrated development environment (IDE) used in computer programming[7]. It contains a base workspace and an extensible plug-in system for customizing the environment. Eclipse is written mostly in Java and its primary use is for developing Java applications, but it may also be used to develop applications in other programming languages via plugins including Ada, ABAP, C, C++, COBOL, Fortran etc.
- **XAMPP** is a free and open-source cross- platform web server solution stack package developed by Apache Friends[2], consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages[3][4] Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server possible.

II. EXISTING SYSTEM

E healthcare systems are increasingly popular a large amount of personal data for medical purpose are involved, and people start to realise that they would completely lose control over their personal information once it enters the cyber space. According to the government website, around 8 million patient's health information was leaked in the past 2

years. There are good reasons for keeping medical data private and limiting the access. An employer may decide not to hire someone with certain diseases. An insurance companies may refuse to provide life insurance knowing the disease history of a patient. The existing cloud system doesn't use the double encryption, proxy server security mechanisms. As times change, a change in the existing system of data security in the field of medical science has not been on the spotlight until now.

Data security and patient confidentiality should go hand in hand, and improvements in security measures are the need for the hour in a sector where patient data could be accessed by unauthorized person [7]. Currently, the healthcare industry is adopting new technologies rapidly. Predominantly, the Information Technology, which is used to assist both doctors and patients alike, and to improve the delivery of healthcare services. The most important section of a hospital information system today is the Electronic Health Record (EHR), where patient information is stored

A) Drawbacks of the Existing System

- Weak protection of patients' data in medical institutions.
- Cannot provide a better security in the applications.

IV. PROPOSED SYSTEM

The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data or computation outsourcing paradigm. We introduce the private cloud which can be considered as a service offered to mobile users. A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers. In the proposed system we introduce the MedRec theme ensures patient-centric management on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to differing kinds of users on whole completely different elements of the PHRs. A semi-trusted proxy noted as Setup and Re-encryption Server (SRS) is introduced to line up the public/private key pairs and to provide the re-encryption keys. Moreover, the methodology is secure against corporate executive threats and collectively enforces a forward and backward access management[1]

A) Advantages

- Authentication: authentication is the process of identifying the person who is trying to log in the system using his credentials and also provide him the best security features[2][5].
- Encryption: Encryption here means the security that we offer in our system for the patients. We provide double encryption for the medical records of patients
- Widely usable: can be widely used by doctor and patients and also along with the encryption feature we provide the basic features of a medical application[4]

B) System Description:

PHR = Personal Health Record
 Process 1= PHR converted in encrypted format
 Process 2 = PHR store on cloud in Re-Encryption format
 Process 3 = PHR users access Re-Encryption format
 Process 4= PHR user request for re encryption key
 Process 5 = PHR user download in Decryption format[4]

C) Algorithms

a) RSA Algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private [5]

b) Message Digest Algorithm

MESSAGE DIGEST ALGORITHM: The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input[5].

D) Requirements

- Hardware System: core i3
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech.
- Ram: 512 Mb

Software Requirements

- Operating system: Windows XP/07/08/10
- Coding Language: JAVA
- IDE: Eclipse Neon
- Database: MYSQL

V. RESULTS AND DISCUSSIONS

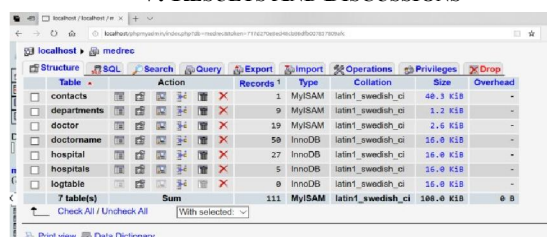


Table	Action	Records	Type	Collation	Size	Overhead
contacts		1	MyISAM	latin1_swedish_ci	48.3 K B	-
departments		9	MyISAM	latin1_swedish_ci	1.2 K B	-
doctor		19	MyISAM	latin1_swedish_ci	2.6 K B	-
doctorname		50	InnoDB	latin1_swedish_ci	16.8 K B	-
hospital		27	InnoDB	latin1_swedish_ci	18.4 K B	-
hospitalis		5	InnoDB	latin1_swedish_ci	26.8 K B	-
logtable		8	InnoDB	latin1_swedish_ci	16.8 K B	-
7 table(s)	Sum	111	MyISAM	latin1_swedish_ci	188.8 K B	0 B

Figure: Database Design



Figure 1: Database design

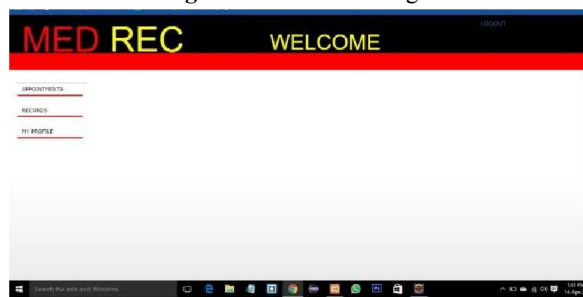


Figure 2: Homepage

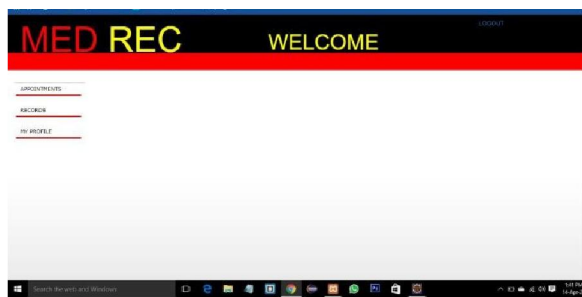


Figure 3: Admin homepage

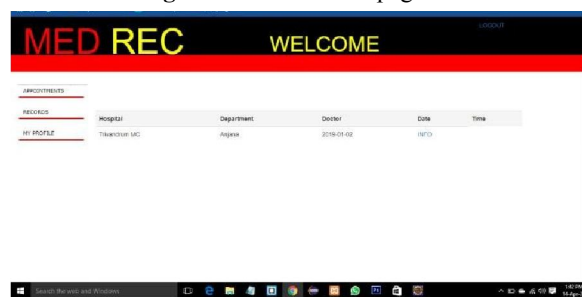


Figure 4: View patient

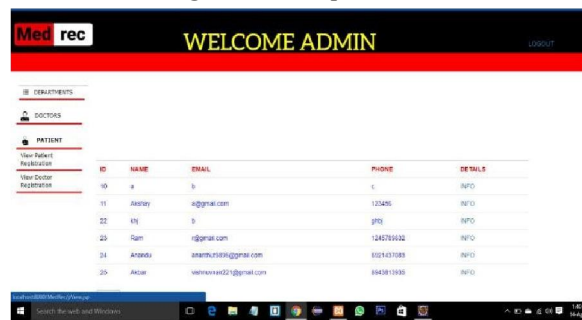


Figure 5: View Doctor

V. CONCLUSION

Substantially addressing cyber security in health care situations isn't going to be easy, and will take cooperation from everyone from doctors to nurses, to IT professionals and manufacturers. The significance of security and privacy in e-Healthcare information raised the issues of individual consent, confidentiality and privacy, which are the main determinants in adopting and successful utilizing the e-Healthcare information. Current trends in the domain of e-Healthcare information management point to the need for comprehensive incorporation of security, privacy and confidentiality safeguards within the review of e-Healthcare information management frameworks and approaches. This raises major challenges that demands holistic approaches spanning a wide variety of legal, ethical, psychological, information and security engineering. The need for such security measures to go mainstream is of high importance in a digital age like the present. The vast and improving technologies have enabled humankind to flourish and achieve feats of great significance. The analysis of articles showed the healthcare industry lags behind in security. Like other industries, healthcare should clearly define cyber security duties, establish clear procedures for upgrading software and handling a data breach, use VLANs and de-authentication and cloud-based computing, and to train their users not to open suspicious code. The healthcare industry is a prime target for medical information theft as it lags behind other leading industries in securing vital data. It is imperative that time and funding is invested in maintaining and ensuring the protection of healthcare technology and the confidentiality of patient information from unauthorized access. To

improve cyber security in health care, organizations need to hire informatics professionals who can not only collect, manage and leverage data, but protect it as well. The proposed system will bring a limelight on the importance and significance of data security, as well as improve the overall reliability of storing medical records[7]

REFERENCES

IEEE/ CSI/ Conference Paper/Journal Paper/Others

- [1]. K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy - preserving multi-channel communication in Edge-of-Things," *Future Generation Computer Systems*, 85, 2018, pp. 190-200.
- [2]. K. Gai, M. Qiu, and X. Sun, "A survey on FinTech," *Journal of Network and Computer Applications*, 2017, pp. 1-12.
- [3]. A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach," *Future Generation Computer Systems*, vols. 43-44, pp. 99-109, 2015.
- [4]. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Sham-shir band, "Incremental proxy re- encryption scheme for mobile cloud computing environment," *The Journal of Supercomputing*, Vol. 68, No. 2, 2014, pp. 624-651.
- [5]. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431-1441, 2014.
- [6]. David, "Design and Implementation of House Automation System" stopper natural philosophy, Vol. 500, No. 334, pp. 108710642, James calendar month 2004.
- [7]. BajiKok American ginger, Amir janduBinnRamlii, C. Prakaash, Syeed Abdul ReehmanBinn Syed Mohammed, "SMS entrance way Interface - Remote watching and dominant via WiFi SMS" fourth National Conference on Telecommunication Proceedings, Shah of Iran and Alam, Malaysia, pp. 84- 87, 2002.
- [8]. Theodoros Giannakopoulos, Nicolas - Alexander Tatlas, Todor Ganchev and Ilyas Potamitis, "A sensible, time period Speech-Driven Home Automation Front-end" *IEEE Transactions on shopper natural philosophy*, Vol. 51, No. 2, pp. 514-523, May 2005
- [9]. Boggula Lakshmi, B. Madhuravani, B. Veda Vidya, C. Sowjanya "SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud" Volume-8 Issue-4, November 2019