MAT JOURNALS

Journal of Analog and Digital Devices
Volume 4 Issue 1

A Methodology for Secure Sharing of Personal Health Records in the Cloud

Akash Tamhane[1], Rishabh Panday[1], Supriya Sunkarwar[1], Ajay Kavhale[1]
Prof. Rina Jugale[2, *]
[1]BE Student, DY Patil College of Engineering, Ambi, Pune, Maharashtra, India
[2]Assistant Professor, BE Student, DY Patil College of Engineering, Ambi, Pune, Maharashtra, India
****Email:** rina.waghmode@dyptc.edu.in*
DOI: http://doi.org/ 10.5281/zenodo.2623033

Abstract

In the health care sector has resulted in value effective and convenient exchange of non-public Health Records (PHRs) among many taking part entities of the e-Health systems. still, storing the confidential health data to cloud servers is prone to revelation or larceny and demand the event of methodologies that make sure the privacy of the PHRs. Therefore, we tend to propose a technique referred to as SeSPHR for secure sharing of the PHRs within the cloud. The SeSPHR 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 by selection grant access to differing types of users on totally different parts of the PHRs. A semi-trusted proxy referred to as Setup and Re-encryption Server (SRS) is introduced to line up the public/private key pairs and to supply the re-encryption keys. Moreover, the methodology is secure against business executive threats and conjointly enforces a forward and backward access management. Moreover, we tend to formally analyze and verify the operating of SeSPHR methodology through the High Level Petri Nets (HLPN). Performance analysis concerning time consumption indicates that the SeSPHR methodology has potential to use for firmly sharing the PHRs within the cloud. conjointly we tend to Implement as a contribution during this paper time Server, Secure Auditing Storage, in Time Server PHR Owner add the start and Ending time attach to uploaded Encrypted files, and conjointly implement the TPA Module for verify the PHR Record its hack or corrupted for the other hacker and wrongdoer if information hack from hacker facet discover all system details of wrongdoer like Macintosh Address and information science Address its our contribution in our project.

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

INTRODUCTION

Cloud computing has emerged as a vital computing paradigm to supply pervasive and on-demand convenience of varied resources within the sort of hardware, software, infrastructure, and storage. Consequently, the cloud computing paradigm facilitates organizations by relieving them from the extended job of infrastructure development and has inspired them to trust on the third-party data Technology (IT) services. to boot, the cloud computing model has incontestable important potential to extend coordination among many aid stakeholders and additionally to make sure continuous convenience of health data, and quantity ability. what is more, the cloud computing additionally integrates numerous vital entities of aid domains, like patients, hospital employees as well as the doctors, nursing employees, pharmacies, and clinical laboratory personnel, insurance suppliers, and therefore the service suppliers. Therefore, the combination of a for mentioned entities ends up in the evolution of a value effective and cooperative health system wherever the patients will simply produce and manage their Personal Health Records (PHRs. Generally, the PHRs contain data, such as:

ARCHITECTURE DIAGRAM

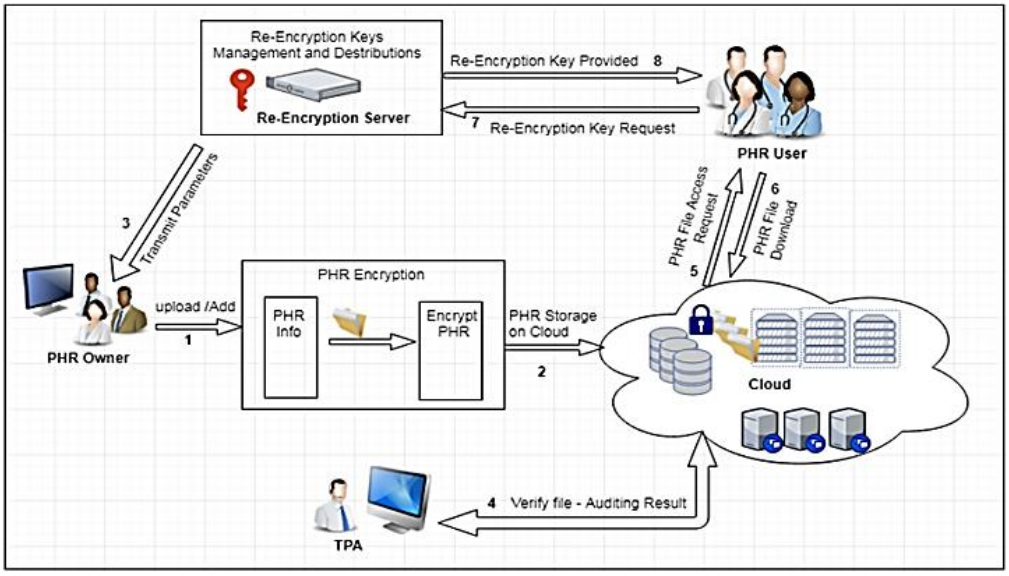

Figure 1: *Proposed model of PHR*

LITERATURE SURVEY

Paper 1. Privacy-Preserving Multi-Channel Communication in Edge-of-Things

Author Name: Keke Gaia, Meikang Qiub, Zenggang Xiongb, Meiqin Liud

Description

Contemporary booming growth of the Internet-based techniques has up a revolution of network-oriented applications. A connected setting any drives the integration of assorted techniques, like edge computing, cloud computing and Internet-of-Things (IoT). Privacy issues have appeared throughout the method of knowledge transmissions, a number of that square measure caused by the low security communication protocols. In follow, high security protection protocols typically need a higher-level computing resource because of a lot of computation workloads and communication manipulations. The implementation of high security communications is restricted once knowledge size becomes massive. This work focuses on the problem of the conflict between privacy protection and potency and proposes a brand new approach for providing higher-level security transmission victimization multi-channel communications. we have a tendency to implement experiment evaluations to look at the performance of the planned approach [1].

Paper 2. A Survey on FinTech

Author Name: Keke Gai, Meikang Qiucor1 b,a Xiaotong Sun a

Description:

As a brand new term within the monetary business, FinTech has become a preferred term that describes novel technologies adopted by the monetary service establishments. This term covers an outsized scope of techniques, from information security to monetary service deliveries. associate degree correct associate degreed up-to-date awareness of FinTech has an imperative demand for each lecturers and professionals. This work aims to provide a survey of FinTech by assembling and reviewing up to date achievements, by that a theoretical information driven FinTech framework is planned. 5 technical aspects square measure summarized and concerned, that embodies security and privacy, information techniques, hardware and infrastructure, applications and management, and repair models. The most findings of this work square measure

fundamentals of forming active FinTech solutions [2].

Paper 3. A cloud based health insurance plan recommendation system: A user centered approach
Author Name: Assad Abbas a, Kashif Bilal a, b, Limin Zhang a, Samee U. Khana,
Description: The recent conception of ''Health Insurance Marketplace'' introduced to facilitate the acquisition of insurance by scrutiny totally different insurance plans in terms of worth, coverage advantages, and quality designates a key role to the insurance suppliers. Currently, the online primarily based tools accessible to look for insurance plans square measure deficient in giving personalized recommendations supported the coverage advantages and value. Therefore, anticipating the users' wants we have a tendency to propose a cloud primarily based framework that provides personalized recommendations regarding the insurance plans. we have a tendency to use the Multi-attribute Utility Theory (MAUT) to assist users compare totally different insurance plans supported coverage and value criteria, such as: (a) premium, (b) co-pay, (c) deductibles, (d) co-insurance, and (e) most profit offered by a thought. To beat the problems arising probably because of the heterogeneous information formats and totally different arrange representations across the suppliers, we have a tendency to gift a regular illustration for the insurance plans. The arrange data of every of the suppliers is retrieved victimization the info as a Service (DaaS). The framework is enforced as software package as a Service (SaaS) to supply tailor-made advocate [3].

Paper 4. Incremental proxy re-encryption scheme for mobile cloud computing environment
Author Name: Abdul Nasir Khan, M. L. Mat Kiah, Sajjad A. Madani, Mazhar Ali, Atta ur Rehman Khan, Shahaboddin Shamshir band

Description: Due to the restricted machine capability of mobile devices, the analysis organization and academe square measure engaged on machinely secure schemes that have capability for offloading the computational intensive knowledge access operations on the cloud/trusted entity for execution. Most of the prevailing security schemes, like proxy re-encryption, manager-based re-encryption, and cloud-based re-encryption, square measure supported El-Gamal cryptosystem for offloading the machine intensive knowledge access operation on the cloud/trusted entity. However, the resource hungry pairing based mostly cryptographical operations, like secret writing and secret writing, square measure dead exploitation the restricted machine power of mobile device. Similarly, if the info owner needs to switch the encrypted file uploaded on the cloud storage, once modification the info owner should code and transfer the whole file on the cloud storage while not take into account [4].

Paper 5: A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds
Author Name: Assad Abbas, Samee U. Khan, Senior Member, IEEE
Description: Cloud computing is rising as a replacement computing paradigm within the care sector besides different business domains. Massive numbers of health organizations have started shifting the electronic health data to the cloud surroundings. Introducing the cloud services within the health sector not solely facilitates the exchange of electronic medical records among the hospitals and clinics, however conjointly allows the cloud to act as a case history storage center. Moreover, shifting to the cloud surroundings relieves the care organizations of the tedious tasks of infrastructure management and conjointly

minimizes development and maintenance prices. all the same, storing the patient health knowledge within the third-party servers conjointly entails serious threats to knowledge privacy. As a result of probable revealing of medical records keep and changed within the cloud, the patients' privacy considerations ought to basically be thought of once coming up with the protection and privacy mechanisms. Varied approaches are wont to preserve the privacy of the health data within the cloud surroundings. This survey aims to cover the progressive privacy protective approaches utilized within the e-Health clouds. Moreover, the privacy protective approaches area unit classified into cryptanalytic and non-cryptographic approaches and taxonomy of the approaches is additionally conferred. Moreover, the strengths and weaknesses of the conferred approaches area unit reported and a few open problems area unit highlighted [5].

Mathematical Model

- System Description:
- Let S be the system
- Object it consist of following
- U=no of User
- U= u1,u2,u3.....Un
- F=no of PHR in les
- F=f1,f2,f3....fn
- 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

ALGORITHM

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

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.

REQUIREMENT

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/J2EE
IDE: Eclipse Kepler
Database: MYSQL

CONCLUSION

We projected a technique to firmly store and transmission of the PHRs to the licensed entities within the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access management to totally different parts of the PHRs supported the access pro-vided by the patients. We tend to enforce a fine-grained access management technique in such some way that even the valid system users cannot access those parts of the PHR that they're not licensed. The PHR house owners store the encrypted information on the cloud and solely the licensed users possessing valid re-encryption keys issued by a semi-trusted proxy area unit ready to rewrite the PHRs. The role of the semi-trusted proxy is to get and store the public/private key pairs for the users within the system. Additionally to conserving the

confidentiality and guaranteeing patient-centric access management over the PHRs, the methodology conjointly administers the forward and backward access management for outbound and therefore the new connection users, severally. Moreover, we tend to formally analyzed and verified the operating of SeSPHR methodology through the HLPN, SMT-Lib, and therefore the Z3 problem solver. The performance analysis was done on the on the idea of your time consumed to get keys, coding and decoding operations, and turnaround. The experimental results exhibit the viability of the SeSPHR methodology to firmly share the PHRs within the cloud setting.

REFERENCE

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 cen-tered approach, "*Future Generation Computer Systems*, vols. 43-44, pp. 99-109, 2015.
4. A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Sham-shirband, "Incremental proxy re- encryption scheme for mo-bile cloud computing environment,"*The Journal of Supercom- puting*,Vol. 68, No. 2, 2014, pp. 624-651.
5. A. Abbas andS. 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.

Cite this Article as:
Akash Tamhane, Rishabh Panday, Supriya Sunkarwar, & Prof. Rina Jugale. (2019). A Methodology for Secure Sharing of Personal Health Records in the Cloud. Journal of Analog and Digital Devices, 4(1), 14–18. http://doi.org/10.5281/zenodo.2623033