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

Keshav Kumar, Megha Sakshi, Mehul Dabhade, Akshay Yerulkar, Prof. D.A. Yerate
DEPARTMENT OF COMPUTER ENGINEERING
Sinhgad Institute of Technology Lonavala Pune

Abstract:

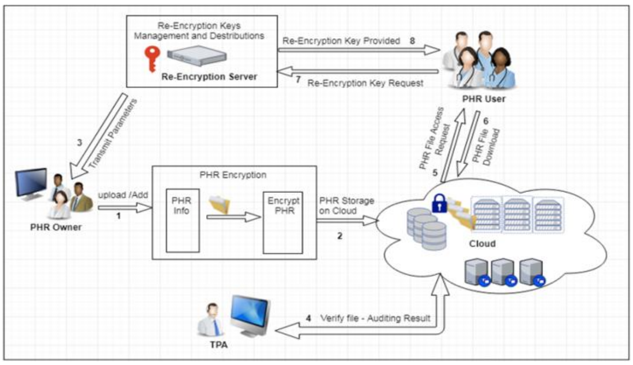
In the health care sector has resulted in worth effective and convenient exchange of personal Health Records (PHRs) among several collaborating entities of the e-Health systems. still, storing the confidential health information to cloud servers is susceptible to revelation or theft and demand the event of methodologies that ensure the privacy of the PHRs. Therefore, we have a tendency to tend to propose a way stated as SeSPHR for secure sharing of the PHRs at intervals 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 selectively grant access to different types of users on wholly totally different components of the PHRs. A semi-trusted proxy stated as Setup and Re-encryption Server (SRS) is introduced to line up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against corporate executive threats and collectively enforces a forward and backward access management. Moreover, we have a tendency to tend to formally analyze and verify the in operation of SeSPHR methodology through the High Level Petri Nets (HLPN). Performance analysis regarding time consumption indicates that the SeSPHR methodology has potential to use for firmly sharing the PHRs at intervals the cloud. collectively we have a tendency to tend to Implement as a contribution throughout this paper time Server, Secure Auditing Storage, in Time Server PHR Owner add the beginning and Ending time attach to uploaded Encrypted files, and collectively implement the TPA Module for verify the PHR Record its hack or corrupted for the opposite hacker and offender if data hack from hacker side discover all system details of offender like Macintosh Address and data science Address its our contribution in our project.

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

Introduction:

Cloud computing has emerged as an important computing paradigm to produce pervasive and on-demand convenience of assorted resources at intervals the type 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 impressed them to trust on the third-party information Technology (IT) services. to boot, the cloud computing model has incontestable vital potential to increase coordination among several aid stakeholders and in addition to create certain continuous convenience of health information, and amount ability. what's additional, the cloud computing in addition integrates various important entities of aid domains, like patients, hospital staff further because the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance suppliers, and thus the service suppliers. Therefore, the mixture of a for mentioned entities finishes up within the evolution of a price effective and cooperative health system where the patients can merely turn out and manage their Personal Health Records (PHRs. Generally, the PHRs contain information, such as:

Architecture Diagram:


Re-Encryption Keys Management and Destributions
Re-Encryption Server
Re-Encryption Key Provided 8
7 Re-Encryption Key Request
PHR User
3 Transmit Parameters
PHR File Access Request 5
6 PHR File Download
PHR Owner
upload /Add 1
PHR Encryption
PHR Info
Encrypt PHR
PHR Storage on Cloud 2
Cloud
TPA
4 Verify file - Auditing Result

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.

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 embody 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.

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

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 Shamshirband

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

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

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:

AES Algorithm:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (ciphertext).

Message Digest Algorithm

- Append Padding Bits
- Append Length
- Initialize MD Buffer
- Process Message in 16-Word Blocks

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 way to firmly store and transmission of the PHRs to the commissioned entities at intervals the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access management to altogether completely different elements of the PHRs supported the access provided by the patients. we tend to tend to enforce a fine-grained access management technique in such how that even the valid system users cannot access those elements of the PHR that they are not commissioned. The PHR householders store the encrypted info on the cloud and alone the commissioned users possessing valid re-encryption keys issued by a semi-trusted proxy unit able to rewrite the PHRs. The role of the semi-trusted proxy is to induce and store the public/private key pairs for the users at intervals the system. to boot to protective the confidentiality and guaranteeing patient-centric access management over the PHRs, the methodology put together administers the forward and backward access management for outward-bound and so the new affiliation users, severally. Moreover, we tend to tend to formally analyzed and verified the in operation of SeSPHR methodology through the HLPN, SMT-Lib, and so the Z3 convergent thinker. The performance analysis was done on the on the concept of some time consumed to induce keys, secret writing and secret writing operations, and turnaround. The experimental results exhibit the viability of the SeSPHR methodology to firmly share the PHRs at intervals the cloud setting.

Reference: 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 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.