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

Pranjali Kamblekar, Karishma Mulik, Payal Varma, Misaba Shaikh, Prof.Ratna Kumar
DEPARTMENT OF COMPUTER ENGINEERING
GENBA SOPANRAO MOZE COLLEGE OF ENGINEERING, PUNE

Abstract:

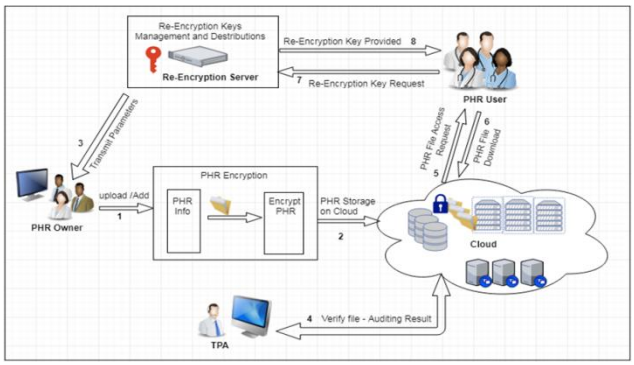
In the health care sector has resulted in price effective and convenient exchange of personal Health Records (PHRs) among several collaborating entities of the e-Health systems. still, storing the confidential health information to cloud servers is susceptible to revelation or stealing and demand the event of methodologies that confirm the privacy of the PHRs. Therefore, we've associate degree inclination to tend to propose the best manner expressed 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 differing kinds of users on altogether completely entirely totally different components of the PHRs. A semi-trusted proxy expressed 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 executive threats and along enforces a forward and backward access management. Moreover, we've associate degree inclination to tend to formally analyze and verify the operational 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. along we've associate degree inclination 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 along implement the TPA Module for verify the PHR Record its hack or corrupted for the choice hacker and soul if data hack from hacker side discover all system details of soul like Macintosh Address and data science Address it's 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 provide pervasive and on-demand convenience of assorted resources at intervals 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 affected 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 to boot to make sure continuous convenience of health information, and amount ability. what's further, the cloud computing to boot integrates various very important entities of aid domains, like patients, hospital employees extra as a results of the doctors, nursing employees, pharmacies, and clinical laboratory personnel, insurance suppliers, then the service suppliers. Therefore, the mixture of a for mentioned entities finishes up among the evolution of a value effective and cooperative health system where the patients can merely prove and manage their Personal Health Records (PHRs. Generally, the PHRs contain information.

Architecture Diagram:



Literature Survey:

Paper 1. Internet of Things: Challenges and Opportunities.

Author Name:S. C. Mukhopadhyay and N. K. Suryadevara.

Description:

The term Internet of things (IoT) is used to describe embedded devices (things) with Internet connectivity, allowing them to interact with each other, services, and people on a global scale. This level of connectivity can increase reliability, sustainability, and efficiency by improved access to information. Environmental monitoring, home and building automation and smart grids could be interconnected, allowing information to be shared between systems that affect each other. Giving these systems better awareness can improve their efficiency, reliability and sustainability. Due to the large number of applications the IoT has the potential to replace people as the largest consumer and producer of information on the Internet. Low powered wireless embedded devices are cost effective and require little infrastructure, however the Internet and its protocols are unsuitable for such devices due to a lack of resources. IPv6 over low-power wireless area networks (6LoWPAN) was created for this purpose by the Internet Engineering Task Force (IETF). The IETF created the standards the Internet operates on. 6LowPAN allows low powered wireless devices to behave like any other Internet connected device with some restrictions.

This chapter will give an introduction of the status of IoT along with the challenges and opportunities of making the IoT.

Paper 2. Research Directions on the Adoption, Usage and Impact of the Internet of Things through the Use of Big Data Analytics.

Author Name:-Frederick J. Riggins**,** Samuel Fosso Wamba**.**

Description: The number of devices connected to the Internet of Things (IoT) by the year 2020 may be as high as 75 billion. Long before that, big data analytics will be needed to make use of the data generated by the Internet of Things. While the technical issues neededto create the Internet of Things are substantial, little attention has been given to the behavioral, organizational and business issues that are necessary for a better understanding of the adoption, usage and impact of the IoT. We propose a framework based on the idea that this technology will evolve from monitored "Things", to "Networks of Things", and ultimately to an "Internet of Things". Each of these instantiations of the technology raises adoption,usage and impact issues that can be scrutinized at four levels of analysis: individual, organization, industry, and society. We apply the framework to propose research questions that need to be addressed by researchers.

Paper 3. Cellular m2m forecasts: unlocking growth cellular m2m connections forecast to reach 1 billion by 2020, GSMA Report.

Author Name: Tom Rebbeck, Michele Mackenzie and Nuno Afonso.

Description: In 1952, having purchased the rights to the transistor from AT&T, Masaru Ibuka and Akio Morita of Tokyo Tsushin Kogyo challenged their engineers to build a portable radio that would fit into a pocket. Despite resistance as most people at the time believed that the challenge was impossible, the first battery-powered pocket radios were sold in 1955. The company, under its new name Sony, would go on to sell millions of radios. Today we have an analogous situation.

Telecoms engineers are being challenged to produce a low-power, wide area (LPWA) network1 that can connect to modules that require a single AA battery for 10 years of life and that will cost under USD5 each. This paper looks at the potential market for such a solution. Assuming this challenge can be met, we believe that LPWA services can target a market of over 3 billion machine-to-machine (M2M) connections by 2023 and generating over USD10 billion from connectivity revenues alone.

Paper 4. CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks.

Author Name: Xiaodong Lin.

Description: Node compromise attack is a serious threat to the successful deployment of wireless sensor networks. It is a multiple-stage attack, which usually consists of three stages: physically capturing and compromising sensor nodes; redeploying the compromised nodes back to the sensor network; and compromised sensor nodes rejoining the network and launching attack. Over the last few years, much previous work has tackled the node compromise attack in the late stage, either in the second stage or in the third stage. As a result, the protection measures are often ineffective. In this paper, we will make the first effort on addressing the node compromise problem in the first stage, and present a new couple-based scheme to detect the node compromise attack in early stage. Specifically, after sensor nodes are deployed, they first build couples in ad hoc pattern. Then, the nodes within the same couple can monitor each other to detect any node compromise attempt. Extensive simulation results are given to demonstrate the high detection rate of the proposed scheme.

Paper 5: Trustworthiness Management in the Social Internet of Things.

Author Name: Michele Nitti, Roberto Girau, and Luigi Atzori.

Description: The integration of social networking concepts into the Internet of things has led to the Social Internet of Things (SIoT) paradigm, according to which objects are capable of establishing social relationships in an autonomous way with respect to their owners with the benefits of improving the network scalability in information/service discovery. Within this scenario, we focus on the problem of understanding how the information provided by members of the social IoT has to be processed so as to build a reliable system on the basis of the behavior of the objects. We define two models for trustworthiness management starting from the solutions proposed for P2P and social networks. In the subjective model each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the friends in common with the potential service providers. In the objective model, the information about each node is distributed and stored making use of a distributed hash table structure so that any node can make use of the same information. Simulations show how the proposed models can effectively isolate almost any malicious nodes in the network at the expenses of an increase in the network traffic for feedback exchange.

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

Outcomes:-

Fig:- Welcome page

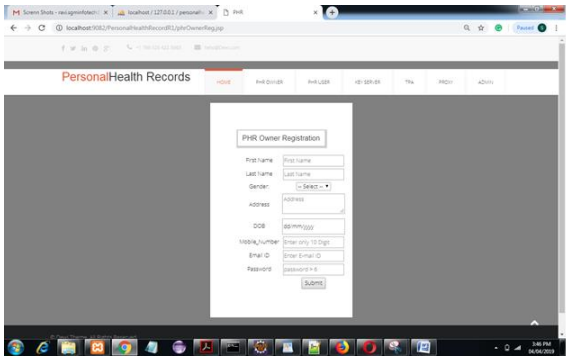


Fig:- PHR owner registration

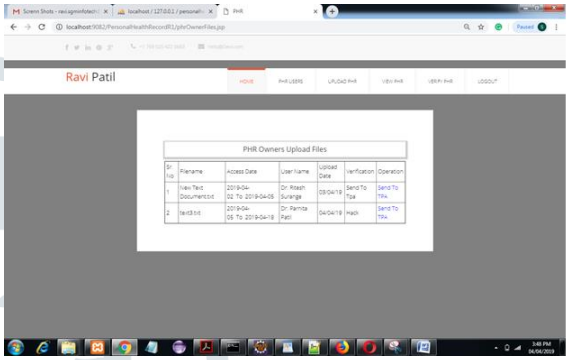


Fig:- PHR owner upload file

Fig:- PHR user request verification

Conclusion: - We projected a way to firmly store and transmission of the PHRs to the licenced entities at intervals the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access management to altogether totally different components of the PHRs supported the access pro-vided by the patients. we have a tendency to tend to enforce a fine-grained access management technique in such how that even the valid system users cannot access those components of the PHR that they are not licenced. The PHR homeowners store the

encrypted data on the cloud and alone the licenced users possessing valid re-encryption keys issued by a semi-trusted proxy square measure able to rewrite the PHRs. The role of the semi-trusted proxy is to urge and store the public/private key pairs for the users at intervals the system. in addition 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 and so the new affiliation users, severally. Moreover, we have a tendency 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 sometime consumed to urge keys, cryptography and decipherment 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.