Secure sharing and storage of Personal Health Records in Cloud and reading current health data using Wireless Sensor Networks.

Abstract:

Personal Health Records (PHRs) should remain the lifelong property of patients, who should be able to show them conveniently and securely to selected caregivers and institutions. We present a cloud-based PHR system taking a radically new architectural solution to health record portability. However, there have been wide privacy concerns as personal information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Here, we use novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage the outsourcing decryption technique and a newly proposed key private proxy re-encryption to encrypt each patient's PHR file. This shifts the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design. We will also deploy portable sensors in wireless body sensor networks to collect various physiological data, such as body temperature, heart beat rate .Such physiological data could then be sent to a central server using an online portal, which could then run various web medical applications on these data to return timely advice to the client.

Motivation:

- To provide lifelong medical history of patients
- To provide secure storage of personal health records
- To provide timely health advice to patients

Existing System:

Existing Cloud-assisted health Records(Monitoring Health) monitoring, which applies the prevailing server Client communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of Monitoring Health technology.

Proposed System:

We present a cloud-based PHR system taking a radically new architectural solution to health record portability. Here, we use novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. A semi-trusted authority is responsible for distributing private keys to the individual clients. The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their drive devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through web portal. We will also deploy portable sensors in wireless body sensor networks to collect various physiological data, such as body temperature, heart beat rate .Such physiological data could then be sent to a central server using an online portal, which could then run various web medical applications on these data to return timely advice to the client.

Architecture:

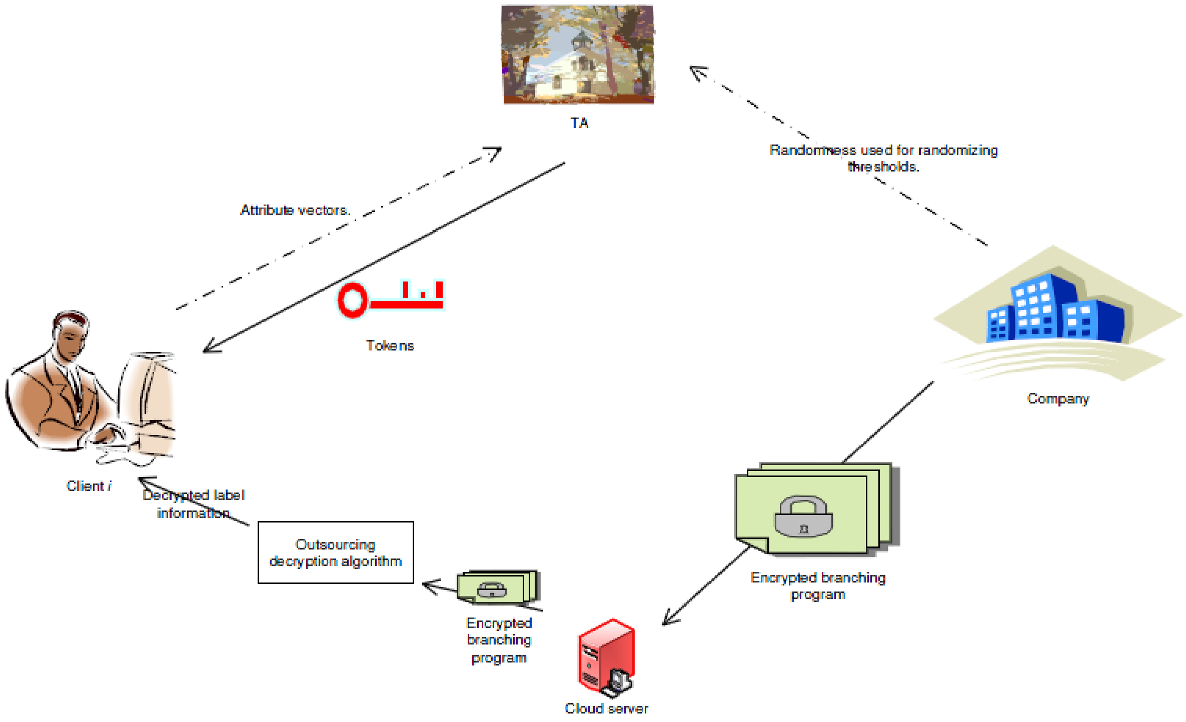
TA
Randomness used for randomizing thresholds.
Attribute vectors.
Tokens
Company
Client *i*
Decrypted label information
Outsourcing decryption algorithm
Encrypted branching program
Encrypted branching program
Cloud server

Fig: PHR with full privacy preservation

[IEEE TRANASCTIONS ON IMAGE PROCESSING VOL:8 NO:6 YEAR 2013 CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring Huang Lin_, Jun Shaoy, Chi Zhangz, Yuguang Fang_, Fellow, IEEE]

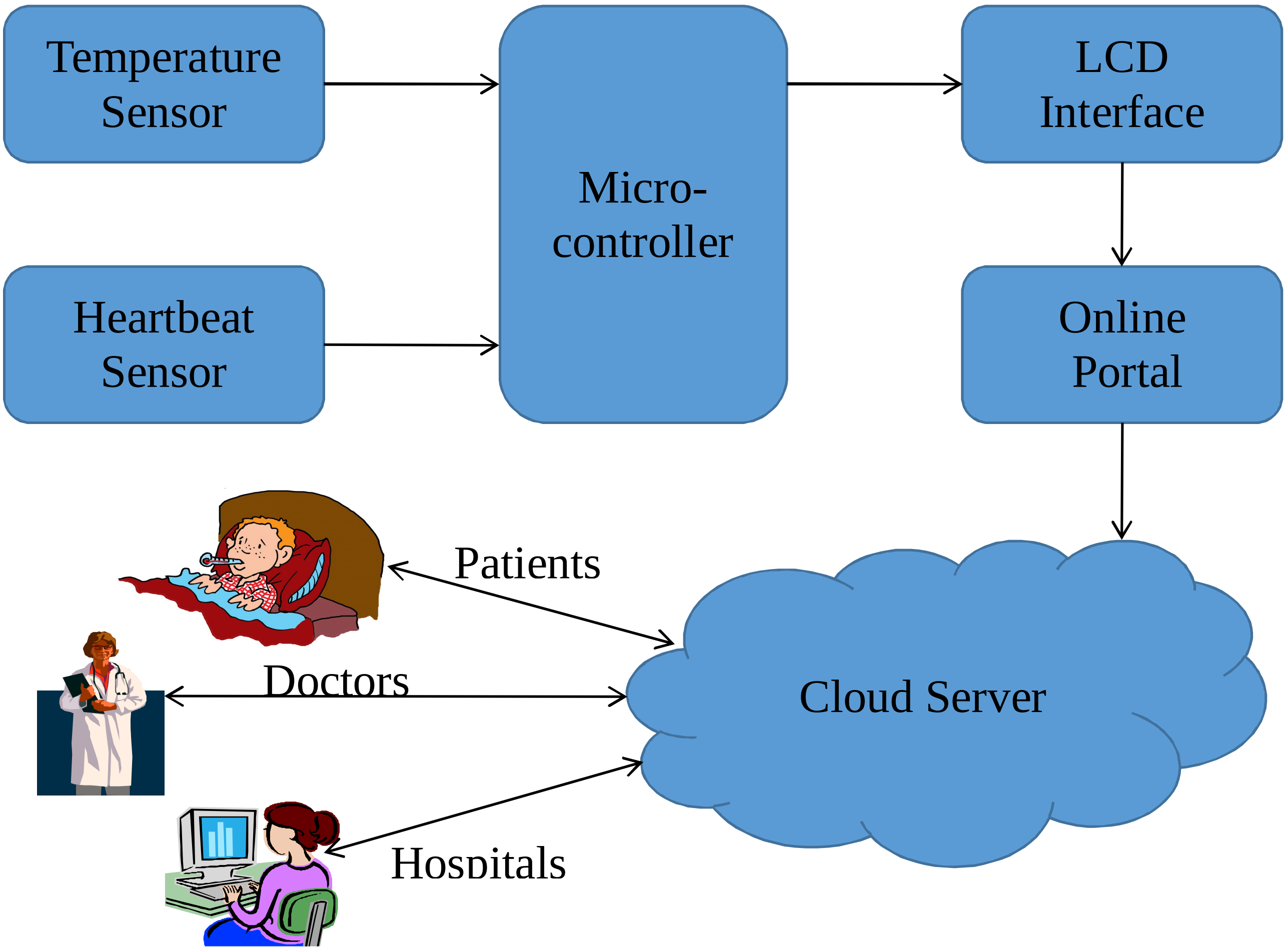

Fig:Model for Cloud based PHR

Description:

The primary function of this system is to store patient health data in cloud securely. Individual clients collect their medical data and store them in their drive devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through web portal. To achieve fine-grained and scalable data access control for PHRs, we leverage the outsourcing decryption technique and a newly proposed key private proxy re-encryption to encrypt each patient's PHR file. This shifts the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. We monitor the temperature and Heart Beat of the patient. Temperature sensors & heart beat sensors are attached to the patients. These are in turn connected to the microcontroller. The data collected by the sensors are sent to the Microcontroller. The Microcontroller displays the data on the screen. Sensors attached to the patient give the pulses. These analog pulses are fed to the ADC which is connected to the microcontroller. We feed the data received on screen to the centralized server using web portal.

Modules:

1. Registration: A user should get registered by giving the appropriate information and details, through which the administrator can communicate with them. Once when the user has been registered,only then he can post queries where he would be able to obtain information from the system.

2. Upload files: As the administrator is the whole and sole of the application so only he has the right to upload records, to view the users, to allocate the tokens and modify rest of the things.Attribute Based Encrytion is based on attributes to encrypt data for security.

3. Semi Trusted Authority: A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors.

4. Query: A client delivers the private key sets obtained from the TokenGen algorithm to the cloud, which runs the Anon Decryption algorithm on the cipher text generated in the Store algorithm. Starting from p1, the decryption result determines which cipher text should be decrypted next. For instance, if v1 ∈ [0, t1], then the decryption result indicates the next node index L(i). The cloud will then use skv(L(i)) to decrypt the subsequent cipher text CL(i). Continue this process iteratively until it reaches a leaf node and decrypt the respective attached information.

5. Token Generation: To generate the private key for the attribute vector v=(v1, · · · , vn), a client first computes the identity representation set of each element in v and delivers all the n identity representation sets to TA. Then TA runs the AnonExtract(id, msk) on each identity id ∈ Svi in the identity set and delivers all the respective private keys skvi to the client

System Specification:

Hardware Requirements:

- 5 V DC Power Supply
- ATMEL AT89S52 Microcontroller
- LCD 16*2 Alpha Numeric
- Memory – External EEPROM
- Buzzer – Frequency 1 to 18 KHz (5V – 12V DC)
- Temperature & Heartbeat sensors
- RS 232 for Serial Communication – MAX 232

System	: Pentium IV 2.4 GHz
Hard Disk	: 40 GB
Floppy Drive	: 1.44 Mb
Monitor	: 15 VGA Colour
Mouse	: Logitech
Ram	: 512 Mb

Software Requirements:

Operating system	: Windows XP
Coding Language	: Jsp Javascript
IDE	: Netbeans
Data Base	: My SQL Server

Application:

- Provide medical consultation
- Improve the quality of healthcare services and potentially reduce healthcare costs
- Secure storage of personal health records
- Retrieval of health reports anytime from any remote location

Conclusion:

Portable sensors could be deployed in wireless body sensor networks to collect various physiological data, such as blood pressure (BP), breathing rate (BR), Electrocardiogram (ECG/EKG), peripheral oxygen saturation (SpO2) and blood Glucose to provide various functionalities ranging from sleep pattern analyzers, exercises, physical activity assistants, to cardiac analysis systems.

References:

1. *IEEE TRANASCTIONS ON IMAGE PROCESSING VOL:8 NO:6 YEAR 2013 CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring Huang Lin_, Jun Shaoy, Chi Zhangz, Yuguang Fang_, Fellow, IEEE*
2. *MyPHRMachines: Lifelong Personal Health Records in the cloud Van Gorp, P. ; Sch. of Ind. Eng., Eindhoven Univ. of Technol., Eindhoven, Netherlands ; Comuzzi, M.*
3. *Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud Van Gorp, P. ; Sch. of Ind. Eng., Eindhoven Univ. of Technol., Eindhoven, Netherlands ; Comuzzi, M.*