Sharing and Storage of Personal Health Records in Cloud Securely and Reading and Storing Current Health Data using Sensor Networks

Saurav Mawandia[1] Padmashree T[2] Dr.N.K Cauvery[3]

Abstract— Health record of a patient form his birth should be consolidated at one place and should remain his lifelong property which can be shown to any hospital or doctor whenever required. We propose a Personal Health Records (PHR) system which will store patient's health records securely. To ensure the patient's data is not misused we have encrypted their PHR's before outsourcing it. To achieve this security we propose Attribute based encryption (ABE) which allows only part of PHR's to be hidden from any institution or caregiver. We also propose an AES encryption to ensure security of PHR. This will help for storage of PHR in the cloud without compromising privacy of patient. We will also deploy portable sensors to collect various physiological data, such as body temperature, heart beat rate and transfer it wirelessly to the PHR of the patient. Such physiological data could help as a monitoring purpose as advised by doctor and help doctors to give correct advise to their clients. A patient can also take advice for small diseases from the doctor using an online portal. Preliminary analysis of security and performance reveals the effectiveness of the proposed design.

Key words: PHR, ABE, FRAMEWORK

I. INTRODUCTION

In recent years, Personal health record (PHR) has helped patient to store their health data in a single place. The PHR system helps patients to store and control their health data in a single place and helps them in sharing and retrieving it conveniently. The patient is given full control on their records and allows them to share their records with anyone they want to. As there is a high cost involved in maintaining the data center many PHR system outsource it for example, Microsoft HealthVault1.Diffrent hospitals also have their own PHR which leads to have multiple copies of a PHR of a single patient. In the recent time institutions have started storing PHR in cloud. Though it is very convenient and exciting to store PHR in cloud but it has various security implications. The issue with cloud storage is how patients can control their health information when they are stored remotely which people don't trust. The Federal Health Insurance Portability and Accountability) HIPAA act 1996 which demands the security of PHR was also recently amended to include business associate cloud provider. On the other hand, the health information is at constant risk and is subjected to malicious behavior due to high value of the sensitive information. To ensure security of patient's data a patient-centric encryption model is required to store data on semi trusted server. The most feasible approach is to encrypt data before storing. The patient should be owner of its record and should be responsible for it by deciding on which part of PHR to be encrypted and selecting the audience. PHR can be shared with a decryption key. Furthermore, the patient should have right to give access and revoke access to any institution or person whenever he feels it necessary. However, the goal of patient- centric security is always in conflict with scalability of PHR system. The audience of the PHR can view it for personal and professional reasons. Examples of personal users are friends and family member and the professional users can be doctors, pharmacists, researchers and caregivers etc. The professional users has potentially large scale; the patient will be overwhelmed by the key management overhead if they manage their PHR on own. On the other hand since this list of professional users are unpredictable which cannot be decided upfront there is a need for to give option to patient to configure PHR whenever required and also there are multiple owners who may encrypt according to their own cryptographic keys. Allowing each user to obtain keys from patient may be difficult as patient may not always be available to give the key. An alternate solution is to employ a central authority (CA) which will manage the key's on behalf of the patient but this will cause another problem as we will be trusting a single authority therefore we propose a semi trusted authority which will help to manage security of the PHR. The personal health record of day to day life such as temperature and heartbeat data can also be attached directly to personal health record on day to day basis if required. It can be used for monitoring purpose and also help to provide online consultation. A patient can also take online consultation for a disease by posting his symptoms anonymously (if he wants to hide his identity) directly to doctor and get consultation from the doctor.

II. RELATED WORK

In this paper we have taken inputs from various papers. The major source is attribute based encryption which employs cryptographically ensured access control. The traditional public key encryption (PKE) based schemes employed to realize fined grained access control, has high key management overhead and requires encryption of multiple file copies using different user's keys. To deal with this problem the ABE can be employed. The fundamental property of ABE is preventing against user collusion. In Goyalet. al's paper on ABE ,data of a certain set of attribute is encrypted which allows multiple users having a proper key to decrypt the data. This helps in making key management and encryption more efficient. We have also referred the Advanced Encryption Standard (AES) which is used to encrypt data using symmetric block cipher.

A. ABE:

ABE is widely used to provide fine-grained access control for any outsource data. It ensures that cipher text and users secret key are dependent on attributes. For Instance if a any retail customer's sensitive data such as his mobile number is to be hidden then attribute based encryption can be used to encrypt his mobile number. Only users who are authorized can view sensitive data which are encrypted using ABE. However, with the increase in unrevoked users the cipher text length grows linearly. Ibraimi and others applied cipher text policy ABE (CP-ABE) to manage sharing of PHR. In Akinyele and others used it for protecting Electronic Health Record which can be stored on mobile or cloud server and can be accessed when service provider is offline. However, there are several drawbacks in the mentioned work. First, they propose a single Trusted Authority (TA) which will allow TA to access all the encrypted files and also create a huge load which may become a bottleneck as it may cause privacy issues. Different patients or organizations may have different subdomains and may need different attribute to be hidden which may become a problem. Second, there is a need for an efficient user revocation mechanism which can be demand based for ABE with the support to dynamically change/update policy. Our idea to have a semi trusted authority will help to deal either the above mentioned problem.

III. Framework for the System

In this section, we discuss about our patient centric cloud based PHR and reading of health data using sensor networks.

A. *Overview of framework:*

PHR System primarily helps to store patient health data in cloud securely. Patients collect their medical data and store them locally in any drive devices, and then the data is transformed to attribute vectors. This attribute vectors serves as an input to monitoring program in cloud server using a web portal. To obtain fine-grained and scalable data access control for PHRs, we propose a combination of ABE and AES. This will help to shift the computational complexity of the parties involves to the cloud without compromising clients privacy. A semi trusted authority will facilitate any encryption and the user will be allowed to encrypt his data. The patients can also consult doctor for ant disease anonymously and get the response online using the portal. We also propose to monitor the temperature and Heart Beat of the patient with the help of temperature & heart beat sensors which are attached to the patients. These are in turn connected to the microcontroller which receives the data from sensor network. 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 use Zigbee to wirelessly transfer data from the display to the system which is saved in log files of the system and then it is fed to the online portal. Fig 1 explains the proposed framework

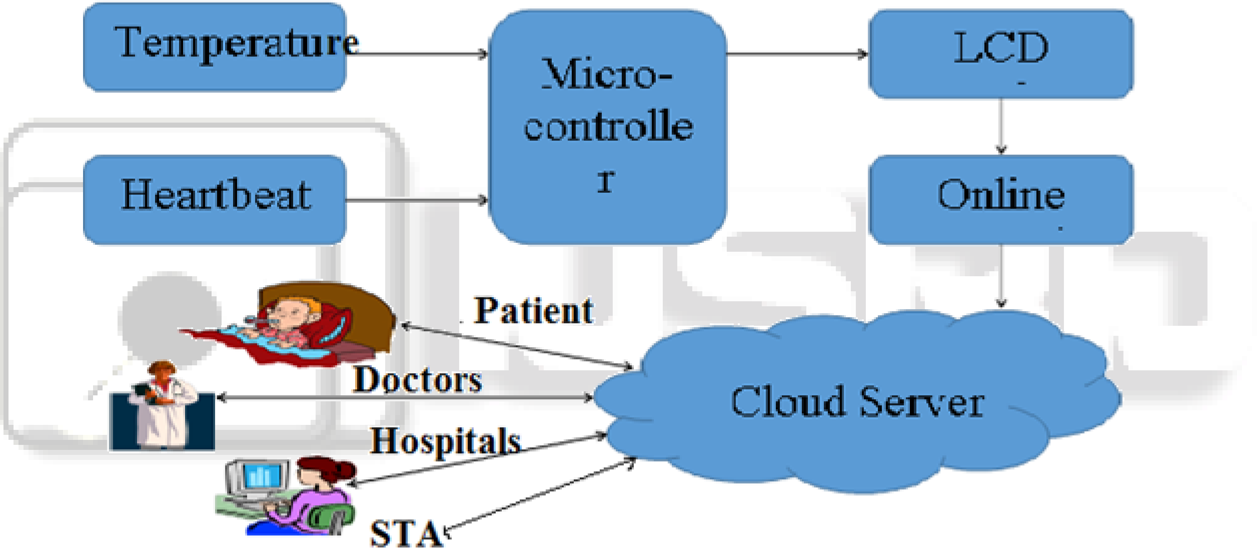

Fig. 1: The Proposed Framework for Patient-Centric, Secure and Scalable PHR Sharing on Semi-Trusted Storage

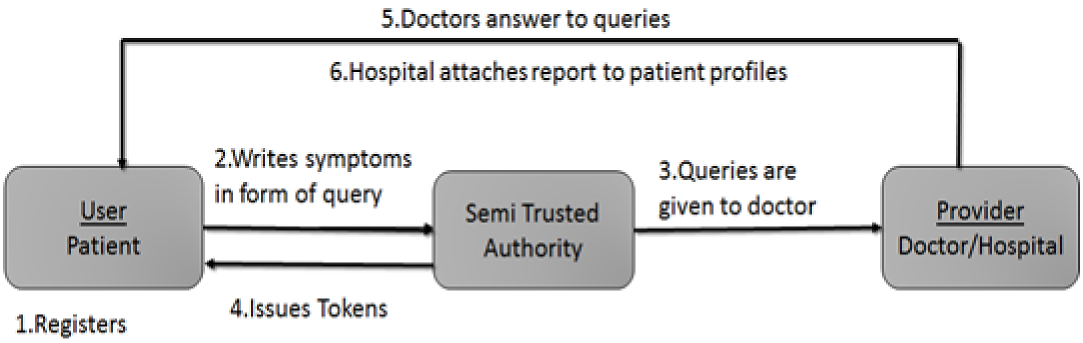
5.Doctors answer to queries
6.Hospital attaches report to patient profiles
2.Writes symptoms in form of query
3.Queries are given to doctor
User
Patient
Semi Trusted Authority
Provider
Doctor/Hospital
4.Issues Tokens
1.Registers

Fig. 2: Interaction between Stake Holder of the System

B. *Interaction between Stake holders:*

There are three major stake holder of the system namely user, semi-trusted authority and provider. The stake holders communicate to provide the proposed functionality. The patient creates his PHR with the help of semi trusted authority (STA). The patient can show its PHR to any viewer (personal or professional) by asking the STA to issue token. The patient can also ask STA to hide any file in PHR using his web account. The hospital can upload file to patient PHR if he is permitted by patient and STA. The patient can also takes online consultation by posting queries to the doctors.STA generates tokens which is given to the patient only when any doctor replies or the medication already exists. The detailed interaction is explained in fig 2.

C. Encryption Algorithm

We propose to use an AES based encryption algorithm which uses Attribute Based encryption (ABE) for hiding particular file. The encryption algorithm is explained below.

1. KeyExpansion—

Here, using Irondale's key schedule we derive roundkeys with the help of cipher keys. AES uses a separate 128 bit round key block in each round

2. InitialRound
   1) AddRoundKey—Using bitwise XOR, each byte is combined with a block of round key,
3. Rounds
   1) SubBytes—Each bytes is replaced by a substitute by looking at the lookup table
   2) ShiftRows-Last three rows are shifted cyclically, certain steps at a time.
   3) ColumnMixing—the four bytes in each column are combined
   4) RoundKeyAdding
4. Final Round
   1) SubBytes
   2) ShiftRows
   3) RoundKeyAdding.

The algorithm is explained in Fig 3.

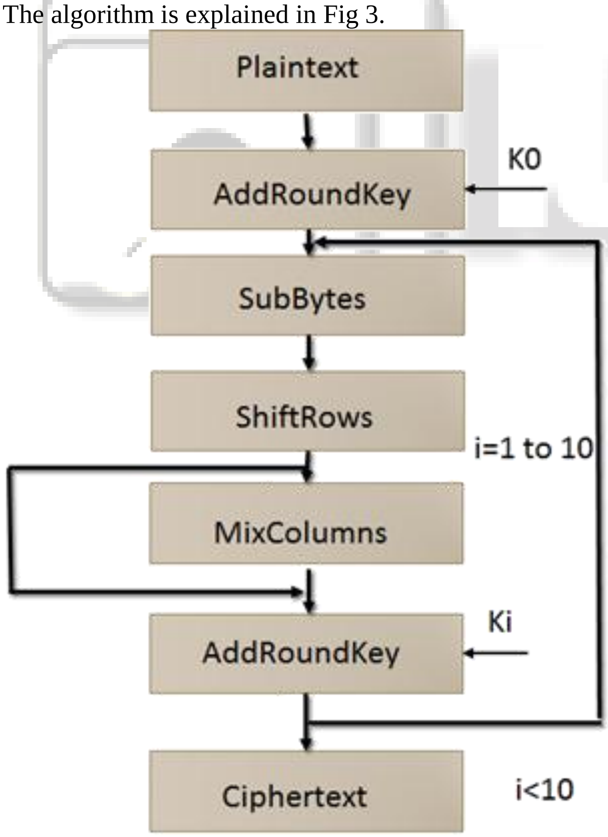

Fig. 3: Encryption Algorithm

1) Attribute Based Encryption:

Attribute based encryption helps in encrypting and decrypting a particular attribute in a file. We propose attribute based encryption to help patients encrypt particular attributes in their PHR.This will ensure privacy of patients record when it is shared with institutions/caregiver.

D. Hardware for Real Time Health Data:

We measure real-time health data of a patient such as temperature and heartbeat using temperature sensor and heartbeat sensor. The data measured from the below mentioned sensor are displayed on the 8 bit microcontroller and transmitted to computer using Zigbee transmitter. A log file is created in the system that can be uploaded to PHR whenever required. We can also measure other health data using available sensor's in mobile phone and use it to upload to patient's PHR.The hardware arrangement is shown in figure 4

1) Temperature Sensor DS 1620

The DS1620 sensor measures temperature using band gap. The temperature reading is provided in a 9–bit, two's complement reading by issuing a READ TEMPERATURE command. The READ temperature command with 9bit, two's complements helps in temperature reading.

2) Heartbeat Sensor MC 8051 LLDR

The Light dependent sensor (LDR) helps in measuring of heartbeat. The resistance of a light dependent resistor is inversely proportional to the intensity of light received by the LDR. The greater the intensity of light the less will be resistance. A light emitting diode which is part of the heartbeat sensing device blinks each time a variation in resistance is observed. The amount of blood flowing through our blood vessels varies whenever the heart pumps blood. This helps by absorbing light when blood vessels are more and reflecting the remaining light which is detected by LDR .During each pulse the LDR receives less light. Subsequently, the resistance of the LDR varies. This variation is observed and amplified using an op amp circuit.

3) Zigbee Transmitter/Receiver

ZigBee is an IEEE 802.15 standard based communicator for transferring data. It is low-powered, and can transmit data over long distances. It has advantage over other technology as it requires low data rate with a very long battery life and is very secure.. ZigBee transfers data at 250 kbit/s, which is best suited for our requirement.A Zigbee transmitter which is part of hardware arrangement is used to transmit the information appearing on LCD to Zigbee receiver.The receiver is connected to the user's system using UART (A universal asynchronous receiver/transmitter).The UART takes bytes of data and transmits the individual bits in a sequential fashion.

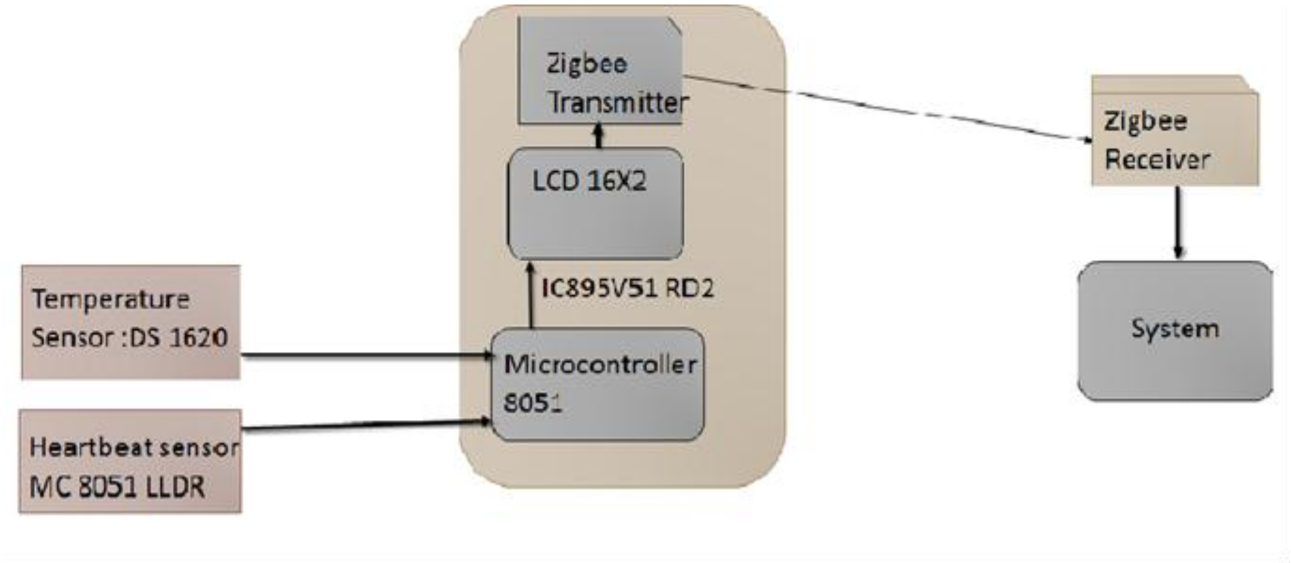

Fig. 4: Hardware and their Interaction

IV. CONCLUSION

In this paper, we have proposed a secure Personal health record storage system with the facility to monitor real time health data. The health record is stored in cloud without compromising security as the data is encrypted with AES algorithm and sensitive fields are encrypted with ABE algorithm. The privacy of involved parties is given high importance. Portable sensors can help in monitoring of day to day physiological data. Other sensor can also be attached which can give cardiac analysis using ECG (Electrocardiogram) which can help hear patient. The system is a robust system which eyes on providing an end to end solution of Personal health record to patients

V. REFERENCES

[1] Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption Ming Li Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE

[2] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in SecureComm’10, Sept. 2010, pp. 89–106.Symposium, ser. IHI ’10, 2010, pp. 220–229.

[3] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in Proceedings of the 1st ACM International Health Informatics

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

[5] MyPHRMachines: Lifelong Personal Health Records in the Cloud International Symposium on Digital Object Identifier: 10.1109/CBMS.2012.6266378; Van Gorp, P ; Comuzzi, M.

[6] Integrating Wireless Sensor Network into Cloud services for real-time data collection ICT Convergence (ICTC), 2013 International Conference; Piyare, R. ; Dept. of Inf. Electron. Eng., Mokpo Nat. Univ., Mokpo, South Korea ; Sun Park ; Se Yeong Maeng;Sang Hyeok Park

[7] Novel Cloud and SOA-Based Framework for E-Health Monitoring Using Wireless Biosensors IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 1, January 2014; Abdelghani Benharref and Mohamed Adel Serhani

[8] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted personal health records in cloud computing,” in ICDCS ’11, Jun. 2011.

[9] “The health insurance portability and accountability act.” [Online].Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[10] “Google, microsoft say hipaa stimulus rule doesn’t apply to them,” http://www.ihealthbeat.org/Articles/2009/4/8/.

[11] “At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded,”2006.[Online].Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26

[12] K. D. Mandl, P. Szolovits, and I. S. Kohane, “Public standardsand patients’ control: how to keep electronic medical records accessible but private,” BMJ, vol. 322, no. 7281, p. 283, Feb. 2001.

[13] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlled encryption: ensuring privacy of electronic medical records,” in CCSW ’09, 2009, pp. 103–114.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in IEEE INFOCOM’10, 2010.

[15] C. Dong, G. Russello, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in Journal of Computer Security, 2010.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access

control of encrypted data," in CCS '06, 2006, pp. 89–98.

[17] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010.

[18] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp. 417–426.

[19] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.

[20] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references) J. Clerk Maxwell,

[21] A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.