International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

SPOC for M-Healthcare using ABE

Latha PH, Asha N

Senior Lecturer, CSE, Govt CPC Polytechnic, Mysore, India

Assistant Professor, DPGS-CEA, NIE, Mysore

Abstract: ***The design and implementation of Personal Health Records (PHR) and providing security to them while they are stored at third party such as cloud is proposed. Personal Health Record is web based application that allows people to access and co-ordinate their lifelong health information. The patients have control over access to their own PHR. To achieve security of personal health records we use the attribute based encryption to encrypt the data before outsourcing it. A secure and privacy-preserving opportunistic computing framework, called SPOC (secure privacy and opportunistic communication) , for m-Healthcare emergency smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. The SPOC's effectiveness in term of providing high reliable PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency. To achieve fine-grained and scalable data access control for PHRs, attribute based encryption (ABE) technique s used to encrypt each patient's PHI.***

Keywords: Healthcare, Computing, Privacy Preserving, Mobile-Healthcare, personal health records, Attribute Based Encryption, Public domain, Private domain.

1. Introduction on SPOC

The Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health 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. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control.

In our aging society, mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smart phones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease. Specifically, in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with Smartphone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere.

For example, each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others, can be first collected by BSN, and then aggregated by Smartphone via Bluetooth. Finally, they are further transmitted to the remote healthcare center via mobile networks is as shown in the figure 1

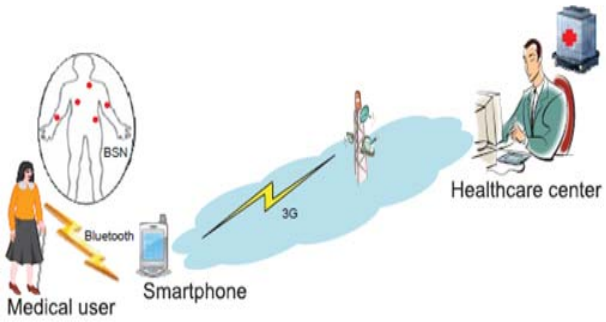

Figure 1: Health monitoring in M-Health care System

2. Existing Approaches

In our aging society, mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smart phones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease [1], [2], [3], [4], [5]. Specifically, in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with Smartphone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere.

When the medical user is at normal situation [6] the sensor nodes can send the PHI data readings to the healthcare centre for every 10 minutes of regular intervals of time and if the patient (medical user) situation is serious then the body Sensor nodes are in busy getting the readings from the patient's body in less period of time and transmit a huge and

large amount of data for every 5-10 seconds in regular time intervals. Where the medical user provided Smart phone is used as a normal phone like we can use it for phoning, chatting, playing videos, listening music and browse internet. Due to which the resources of the mobile like power, battery gets down and in emergency happens unfortunately and it might happen at low probability. Any medical emergency, when all of us take in to 10, 000 emergency cases into account, the common event amount will reach 50, that's not minimal and outstandingly indicates the actual reliability regarding m-Healthcare system is demanding throughout emergency.

MobiHealth [7] aims to give patients a more active role in the healthcare process while at the same time enabling healthcare payers to manage costs more directly. The healthcare BAN and supporting service platform is an emerging technology that promises to support this aim. The actual reliability regarding m-Healthcare system is demanding throughout emergency. A fundamental problem was encountered relating to the use of the Mobile Networks. A second issue related to the use of the HTTP protocol is the fact that every time a request is sent, the communication is blocked until an acknowledgment

Multi-Authority Attribute-Based Encryption (MA-ABE): MA-ABE method allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k [8]

3. Problem Definition

- Since smart phone is not only used for healthcare monitoring, but also for other applications, i.e., phoning with friends, the smart phone's energy could be insufficient when an emergency takes place. So the reliability of m-Healthcare system is still challenging in emergency.
- The raw PHI data are processed, the privacy of PHI would be disclosed.

4. Advantages of Proposed System

The main function of cloud server is to create interface between application and user. The authentication of the username and password is carried out. If user is authentic then he get access to his record. Using attribute based encryption technique we are providing security to the database. A sensitive data is shared and stored on cloud server; there will be a need to encrypt data stored at third party. In Attribute based encryption cipher text labeled with set of attribute. Private Key associated with access structure that control which cipher text a user is able to decrypt. We are using attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of the users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-retrieval to solve, and remain largely open up-to-date.

The main goal of this framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains according to the different users' data access requirements.

1) Public Domain (PUDs)
2) Private Domain (PSDs)

The PUDs consist of users who make access based on their professional roles, such as doctors, Nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

In both types of security domains, we utilize Attribute Based Encryption (ABE) to realize cryptographically enforced, patient-centric PHR access. Especially, in a PUD multi-authority ABE is used, in which there are multiple "attribute authorities" (AAs), each governing a disjoint subset of attributes. Role attributes are defined for PUDs, representing the professional role or obligations of a PUD user. Users in PUDs obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. To control access from PUD users, owners are free to specify role-based fine-grained access policies for her PHR files, while do not need to know the list of authorized users when doing encryption. Since the PUDs contain the majority of users, it greatly reduces the key management overhead for both the owners and users.

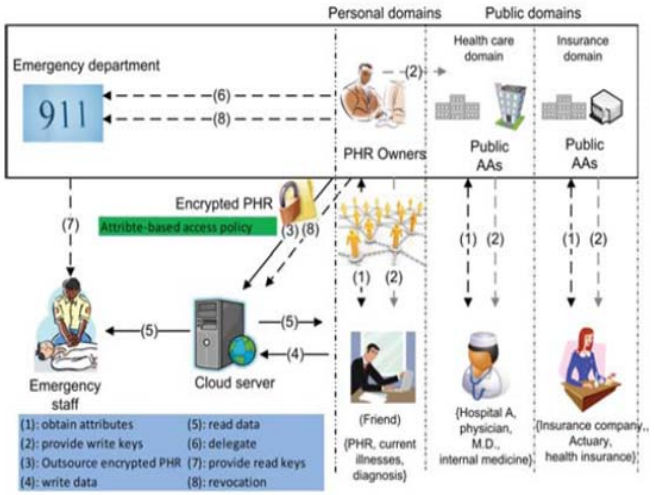

Figure 2: The proposed framework for patient-centric, secure and scalable PHR sharing on semi trusted storage under multi owner settings.

In opportunistic communication (OC), the resources available on other opportunistically contacted medical users'

smart phones can be gathered together to deal with the computing intensive PHI process in emergency situation. The Human Health monitoring smart Phone of the patient registers the Internet Protocol address (IP) of the server and the opportunistic user smart phone and sends the emergency message to the opportunistic user via router.

Using attribute based encryption technique we are providing security to the database. A sensitive data is shared and stored on cloud server; there will be a need to encrypt data stored at third party. In Attribute based encryption cipher text labeled with set of attribute. Private key associated with access structure that control which cipher text a user is able to decrypt. We are using attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of the users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-retrieval to solve, and remain largely open up-to-date.

Advantages of proposed system

- Quickly find out information of patient details.
- In case of emergency doctor and other emergency Department quickly get all the details all the informative details and start treatment.
- To provide easy and faster access information.
- To provide user friendly environment
- To provide data confidentiality and write access control
- Patient PHR Information can be sent to monitor center via smart phones.

5. Components and Modules

This system will provide an efficient User and monitor canter communication. The following Figure 5.1 represents the block diagram of overall System Design.

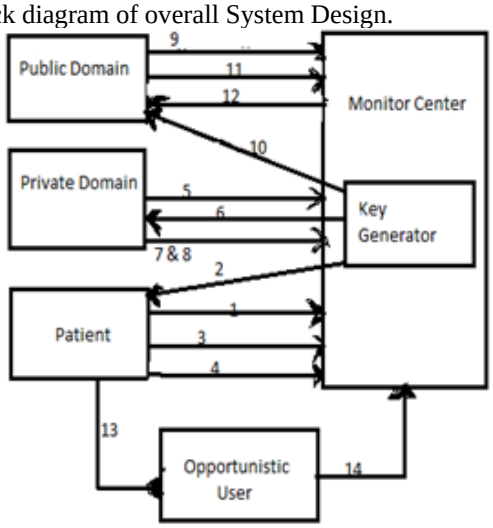

Figure 5.1: System Architecture

1 Patient Registration
2Obtain the key
3 User Login for Authentication
4 Upload the PHR and Encrypted PHR is stored
5 Private Domain i.e., doctor registration
6 Obtain the key
7 Doctor Login
8 One that has Privilege can decrypt and edit the PHR.
9 Public Domain i.e., Insurance, emergency, and etc registration
10 Obtain the key
11Public user login
12 One that has privilege can decrypt and view the PHR.
13 Human Health Monitoring Smart phone send the PHR to Opportunistic Smart Phone
14 Opportunistic smart phone send this PHR to Monitor Center

SPOC includes the following modules:

- Server Module
- Public Module
- Private Module
- Opportunistic module

5.1 Server Module

The Server module is the one which acts as a repository of all the receiving information which involve in the conversation with the Users. It accepts the IP address and the port number of the web application.

Algorithm of Server Module

- Step 1: Create socket and wait for connection
- Step 2: Accepts the request for Registration of SPOC web application.
- Step 3: Run and Check log whether server is started or not

5.2 Public Module

The Public Module is used to decrypt the PHR and can just view the information, only those who have access privilege given by the owner.

Algorithm of Public Module
Step 1: Create socket for communication with the server.
Step 2: New public user registration
Step 3: Get the secret key
Step 4: Authentication of public user
Step 5: valid authentication, the public user can decrypt and view the PHR data

5.3 Private Module

The Public Module is used to decrypt the PHR and edit the information. The edited information is encrypted and stored at the server; this can be done by those who have access privilege given by the owner.

Step 1: Create Socket and establish connection with Sender.
Step 2: New public user registration
Step 3: Get the Secret Key

Step 4 Public user login
Step 5: valid user Decrypt the PHR and edit the PHR.
Step 6: The edited PHR is encrypted and stored at the server

5.4 Owner module

The owner (patient) Module is used to upload their PHR and stores this encrypted PHR at the server.
Step 1: Create Socket and establish connection with Sender.
Step 2: New owner registration
Step 3: Get the Secret Key
Step 4 owner login
Step 5: valid user upload PHR and encrypt he PHR.
Step 6: The encrypted PHR is stored at the server

5.4 Opportunistic Communication module

This module is used send the messages from human health monitoring smart phone to opportunistic user smart phone and in turn to server via wireless router
Step1: Connect the smart phones and server to wireless router.
Step2: obtain the IP address of the smart phones and server.
Step3: Check whether all IP address is in the same network.
Step4: Register opportunistic IP address and server IP address.
Step 4: Run jar file
Step5: Now Human Health monitoring user smart phone will receive PHR data from the jar file.
Step6: After receiving it sends the PHR data to the server through Opportunistic user smart phone.

6. Conclusion and Future Enhancement

6.1 Conclusion

The personal health record system needs security against attackers and hackers. Scalable and Secure sharing includes basic securities to protect the information from unauthorized access and loss. The secure and privacy preserving opportunistic computing (SPOC) framework for m-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. To fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. This paper proposed the new approach for existing PHR system for providing more security using attribute based The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations.

6.2 Future Enhancement

- Sensor can directly send the data to opportunistic user smart phone via Bluetooth
- Instead of Encrypting attribute keys using AES, both AES and MD5 can be incorporated

References

[1] Toninelli, R. Montanari, and A. Corradi, “Enabling secure service discovery in mobile healthcare enterprise networks,” IEEE Wireless Communications, vol. 16, pp. 24–32, 2009.
[2] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network,” in Proc. BodyNets’10, Corfu Island, Greece, 2010.
[3] Y. Ren, R. W. N. Pazzi, and A. Boukerche, “Monitoring patients via a secure and mobile healthcare system,” IEEE Wireless Communications, vol. 17, pp. 59–65, 2010.
[4] R. Lu, X. Lin, X. Liang, and X. Shen, “A secure handshake scheme with symptoms-matching for mhealthcare social network,” MONET, vol. 16, no. 6, pp. 683–694, 2011.
[5] M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, “Wireless body sensor network using medical implant
[6] band,” Journal of Medical Systems, vol. 31, no. 6, pp. 467–474, 2007.
[7] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, “Opportunistic computing for wireless sensor networks,” in IEEE Proc. of MASS’07, pp. 1–6.
[8] Y. Ren, R.W.N. Pazzi, and A. Boukerche, “Monitoring Patients via a Secure and Mobile Healthcare System,” IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.
[9] Melissa Chase “Multi-authority Attribute based Encryption,” Computer Science Department Brown University Providence, RI 02912

Author Profile

Latha P H has received B.E in CSE in BCE, Sharavanabelagola and pursuing M.Tech in CNE, NIE, Mysore. She is working as Senior Lecturer in the Department of Computer Science and Engineering in CPC Govt Polytechnic, Mysore, India

Asha N has completed her Post Graduation in Computer Network Engineering from VTU. Her research interests are in mobile ad hoc networks and cloud computing. She is working as Assistant Professor in the Department of PG Studies, NIE, Mysore, India