Secure Solution for Mobile Access to Patient's Health Care Record using Improved l-Diversity Algorithm

[1.] E. Kodhai , [2.] O. Padmapriya,[3.] Nanc Leonide De Rozario , [4.] D. Maheswari
[1.] Assistant Professor, [2,3,4.] Final Year I.T
SMVEC

***Abstract*— Mobile Health Information exchange deems to facilitate the transfer of patients' healthcare information. However one of the major drawbacks is the installation of hardware and conversion of paper documents to electronic ones. The existing system uses l-diversity algorithm to secure individual information However it is limited to only static data release, and is vulnerable to inference attacks due to dynamic data publishing and processing is found to be time consuming. We propose fingerprint authentication technique using descriptor based Minutia algorithm to facilitate user authentication. Using Descriptor based authentication algorithm, we obtain a descriptor with high discriminating ability.**

Keywords— ***Healthcare Information, l-diversity, Fingerprint, Minutia Algorithm, Descriptor***

I. Introduction

Mobile computingbrings about computing capability to a mobile device. Mobile computing involves mobile software and mobile hardware. The need for health information exchange (HIE) is expected to provide a wide range of benefits for patientsas well as doctors.

Developers found it difficult to convert paper charts to Electronic Medical Records (EMR). The first step, however, was to choose a device with which employees would access the EMR. Because there are many devices on the market, each with their own advantages and drawbacks, decision makers narrowed their selection process down by closely studying the workflow. For instance, patient charts are constantly moving around the hospital, from the nurses' station, to a patient's room, to a conference room and back again. The development team felt that for its EMR implementation to be a success, the access devices must mimic the portability of paper charts.

An electronic health record (EHR) is defined as a systematic collection of electronic health information about individual patients. It is in digital format which makes it capable of being shared across various health care settings. In some cases this sharing can occur by way of network-connected, enterprise-wide information systems and other information networks or exchanges.

EHRs includes a range of data, including medical history,demographics, medication, allergies, immunization status, radiology images,laboratory test results, vital signs, personal statistics like age and weight, and billing information.

Patients consider the following factors in a health information exchange system.

A. *Quality*

Several studies questions whether EHRs improve the quality of care. However, a recent multi-provider study in diabetes care, published in the New England Journal of Medicine, found evidence that practices with EHR to provide better quality care.

B. *Costs*

The steep price of EHR and provider uncertainty regarding the value they will derive from adoption in the form of return on investment has a significant influence on EHR adoption. In a project initiated by the Office of the National Coordinator for Health Information (ONC), surveyors found that hospital administrators and physicians who had adopted EHR noted that any gains in efficiency were offset by reduced productivity as the technology was implemented, as well as the need to increase information technology staff to maintain the system[6].

C. *Privacy and confidentiality*

One purpose of electronic medical records (EMRs) is to increase the accessibility and sharing of health records among authorized individuals. Privacy of information collected during health care processes is necessary because of significant economic, psychological, and social harm that can come to individuals when personal health information is disclosed[7].

II. Related Works

Rongxing Lu et al. suggests that the recent advancements mobile Healthcare (m-Healthcare) provide a better environment for health monitoring. However, it also points out that information security and privacy are still primary concerns[1].

Healthcare information exchange (HIE) has been refined from point-to-point messaging to wide-area networks integrating multiple service providers.

Ming Li et al. termed Personal Health record(PHR) as an emerging patient-centric model of health information exchange which can be outsourced to a third party. However, due to privacy concerns, encryption of PHRs is done before outsourcing, to protect the records from unauthorized third party. Yet, risks of privacy exposure, scalability in key management and flexible access havechallenged their proposed model from achieving fine-grained data access control[2].

According to Pham Ngoc Thanh et al, to exchange data in a secure manner, a security mechanism must provided in each OSI layer to prevent sensitive information from attackers. To increase the security of Virtual Private Networks (VPN) further, a strong authentication mechanism must be used, besides the traditional username and password credentials[3].

III. Proposed Work

We propose a secure based mobile healthcare system, which includes authentication and access control. The authentication is based upon the types of users who are authorized to use the application. Security here is provided through IME number of the authorized user and his fingerprint. This secured system will provide security in delivering the EMR of patients

.

This emerging technology in the field of healthcare helps the practitioners, researchers and patients to access the Electronic Medical Record (EMR) from any location through the mobile phone by accessing the information from the remote database, which lags in providing security[5].. We propose a new secure and privacy preserving framework to convert the hospital based centralized system to a distributed system to access patient health records.

The proposed solution enables secure authentication and communication between a mobile device and a healthcare service provider through usage of a two-factor authentication method on a mobile phone. The proposed solution is independent of mobile network provider and type of the mobile device the application is running on, and provides multifactor authentication. This simplifies use without compromising security.An approach to transfer the medical records of an individual is by using the existing infrastructure of mobile operators.

According to Sudiro, S.A et al[4]the ridge, which usually has thicker structure than the valley takes more processing time for extraction. Taking the advantage of the thin structure of the valley, we proposed an algorithm that reduces the time needed for minutiae extraction. The algorithm was developed in Matlab environment using fingerprint images from FVC2004.

Our proposed work is carried out by the following modules

- Information Feeding
- User Substantiation
- Data Transposition
- Response Acquiesce

A. *Information Feeding*

Users register in or application using username, password, security question and device number. After registration, a unique code is generated, which should be used to log into the user's profile. The service requestors also known as end users request for a particular service and search in the registry for the availability of particular service. The server that processes the request is acknowledged to the requestor. Now the location of web service is known but how to invoke a service is unknown. For instance, consider a method to invoke weather forecast in India. The method is "String getCityForecast(intCityPostalCode)". It can also be specified as "string getINDCityWeather(string cityName,boolisFarenheit)". The server will respond to requestor in WSDL whereas the actual invocation is done in SOAP language as in Fig3. A SOAP request for weather forecast of certain city is requested. The server will respond to the requestor by SOAP response which includes the forecast.

B. *User Substantiation*

This module verifies whether the request was sent to the hospital from the registered mobile device or not. The proposed system offers two types of verification i.e. for device and user. The user verification process is determined using the minutia based matching algorithm

1) For i (1 ~ M) and j (1 ~ N),. If rotate[i][j]=400, then repeat this step and choose another Pi and Qj, else go to step 2). If all possible minutia pairs have been considered, go to step 4).

2) Take Pi and Qj as reference minutia. Convert each minutia point in the template minutia set and the input minutiae set to the polar coordinate system.

3) Match the resulting strings Pi" and Qj" with the process which will be introduced below to find the matching score of Pi" and Qj". Record it as m-score[i][j]. Then go to step 1.

4) Find the maximum value of m-score[i][j] and use it as the matching score of the input and template minutiae set. If the matching score is higher than a threshold value, then the input image is considered to come from the same finger as the templateimage, else we would consider these two images as coming from different fingers.

C. *Data Transposition*

The request is forwarded to the hospital only after the validation of user and device. The server that processes the request is acknowledged to the requestor. The server matches the patient ID of the search query with the hospital records and isolates the requested record. In order to speed up private-practice access to patients medical records, ASL was selected and assigned to provide an end-to-end Internet access security solution, which covered system design, implementation and maintenance services.The final set up for the servers are 1 Authentication server,1 database server& 1 web server. Major application areas are accessing and transferring of Patient's discharge summary, progress notes, lab reports,X-ray reports and Drug administration records.

D. *Response Acquiesce*

These records are transferred to the patient's profile and can be downloaded to the device whenever necessary. The user acknowledges the client, of the records received and terminates the connection. If the requested record is not available then record discovery mechanism is used.

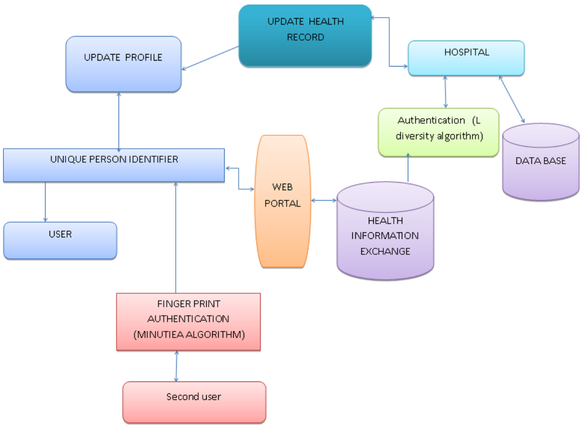
UPDATE HEALTH RECORD
UPDATE PROFILE
HOSPITAL
Authentication (L diversity algorithm)
DATA BASE
UNIQUE PERSON IDENTIFIER
WEB PORTAL
HEALTH INFORMATION EXCHANGE
USER
FINGER PRINT AUTHENTICATION (MINUTIEA ALGORITHM)
Second user

Fig1: Proposed Architecture

IV. CONCLUSION

We have presented a novel approach to transfer EMR using minutiae matching algorithm. Even though l-diversity framework provides privacy, it is not capable of handling multiple sensitive attributes.

REFERENCES

[1] Rongxing Lu, Xiaodong Lin and Xuemin (Sherman) Shen "SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency" IEEE TRANSACTIONS on parallel and distributed systems, 2012

[2] M. Li, S. Yu, K. Ren and W. Lou, &ldquo,Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,&rdquo, *Proc. Sixth Int',l ICST Conf. Security and Privacy in Comm. Networks (SecureComm ',10)*, pp. 89-106, Sept. 2010.

[3] Pham Ngoc Thanh, Information Networking (ICOIN), 2013 International Conference

[4] Sudiro, S.A.; Paindavoine, M.; Yuwono, R.T.; Etp, L. "Performance evaluation of simple fingerprint minutiae extraction algorithm using crossing number on valley structure", *Innovations in Information Technology, 2008. IIT 2008. International Conference*

[5] H. LufeiW.Shi, V.Chaudhary,Adaptive secure access to remote services in mobile environments, IEEE Transactions on Services Computing 1(1) (2008) 49-61.

[6] A. Toninelli, R. Montanari, and A. Corradi,' Enabling Secure Service Discovery in Mobile Healthcare Enterprise Networks," IEEEWireless Com., vol. 16,no.3,pp. 24-32, June 2009.

[7] 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.