IoT based Smart Ambulance with Information Extraction and Traffic Controlling System

Shalaka Agarwal, Shivani Sarage, Rasika Shirke

Information Technology, Pcet's Nutan Maharashtra Institute of Engineering and Technology
Savitiribai Phule Pune University, INDIA

ABSTRACT:- A fingerprint based identification solution is best for any application example as now days all services are based on biometric thumb identification. This system integrated with a communication system in order to support and improve the activity of emergency services on large areas, in accidents implying multiple victims. When accident happen then, it is difficult to obtain the victims' identity data. The implemented proposed system allows the obtaining of a personal and health identity of the persons using the thumb scanner. The personal identity may be maintained during the whole post-accident evolution of a patient, in all the hospitals where a specified person was sent. The patient are registered, their data and evolution being stored and finally, directed from the temporary identity to the true identity, if the conditions allow this. The fingerprint becomes, during an emergency take a short time or a longer time interval, the equivalent of an identity card.

Keywords: Biometrics, Emergency, Health record, EHR.

I. INTRODUCTION

Today's medical, hospital, centers use electronic health records for storing and retrieving patient's information. Medical centers provide a relatively easy access to EHR for authorized personnel on site, but this is not the case in the pre-hospital environment. Patients outside a medical center enjoy no benefit from having their information stored in an EHR when emergency medical technicians or private house doctors have no immediate access to such information.

Biometric system has four basic process and that is: first we collect the data from patient, scan patient thumb, identification thumb, and extract data from database. Collection is using of a sensor to capture the biometric traits and then it will convert them to the digital format then extraction will be take the digital data and convert them to detective features into a compact template. Then the comparison process will be comparing the result with the store objects to get best result. Fingerprint is very important technique that widely used for personal identification.

Access to patient information must be done discreetly and must comply with some corporate policies—such as the rules stipulated in the health insurance portability and accountability act (HIPAA) [5]— conditions that must be met for "proper access". Granting any health professional full access to a patients' EHR may pose potential law violation and create privacy and security risks. A study analyzing whether or not different health professionals will comply with the information assurance policy of their respective health clinic reveals that as many as fifteen compliance factors are involved in such a decision [7]. Therefore, granting full access to any health professional is simply not wise. Instead, a limited and/or partial access is the solution. Granting partial or limited access to a patient's EHR outside of hospital grounds has been an area of interest [8], but it has been limited to close contact or carried on solutions. In this paper, we focus on granting proper access to a patient's EHR remotely with the use of a biometric identification system.

Biometrics as a means of access control has been previously studied and found to be a popular choice for guaranteeing authentication and authorization. This includes: iris, voice, face, fingerprint, and hand geometry recognition. Biometric features possess an if-and- only-if relationship discussed. This makes biometric features the ideal basis for any identification system. In particular, fingerprint extraction is relatively easy in comparison with other biometric features. Fingerprints also possess great hardware and software support in industry [1]. Hence, we choose fingerprints as an adequate biometric identification feature for the environment in mind. Note that biometric identification not only can be used for the health data privacy preservation, it can also contribute in preserving the privacy of the token data (e.g. social security number) itself.

We propose a solution that enables emergency medical technicians to have simple and fast, and reliable access to patients' medical information. The idea is to provide the technicians with a mobile system through which they gain access to necessary attributes of patients' EHR using the patient's fingerprint. Reliability is employed by exploiting the uniqueness of a person's fingerprint as a means of access control as well as by precision of fingerprint

scanners. Privacy of patients is preserved by enforcing an arbitrary privacy policy, the system requires patients to provide only their fingerprint; they need not to carry with them an additional token—such as a health card, driving license, etc.—to receive the service. Simplicity and efficiency of the system is justified through the course of implementation and experiments.

II. PROBLEM STATEMENT

To develop a system which will give information about medical history of patient in emergency for quick action and proper treatment the ambulance itself which will save precious time of patients.

III. LITERATURE REVIEW

There are several approaches to access electronic health records (EHR) in emergency situations. In Himadri Nath Saha [1], an IOT-based live monitoring system for patients with the risk of heart attack and critical condition of patient health cannot been monitor accurately. In Tishko N. Muhamad [2], this paper tries to offer a simple high performance approach to perform fingerprint recognition. This approach based on two main stages; the first one is the real data collection of human fingerprint samples and the second stage is concentrated on design and implementation of high performance fingerprint recognition approach and also time consuming. In Bernard Fong [3], the smart ambulance consists of a network of connected medical devices, sensors and extends to consumer health devices worn by patients. [3] There is no focus on traffic controlling system in order to make patient arrive hospital on time. In Sabeen Javaid [4], smart traffic management system is proposed to control road traffic situations more efficiently and effectively. It changes the signal timing intelligently according to traffic density on the particular roadside and regulates traffic flow by communicating with local server more effectively. This idea approaches only if higher authorities accessed the permission for traffic controlling in order to avoid lot of time wastage in traffic jams. In Subhash Chandra Kumar [5] the designed system shares the location of patient using GPS module and automatically calls ambulance using GSM module which will carry the patient to the hospital. In accident case personal data of patient cannot be accessed and inform to the patients home.

IV. PROPOSED MODEL

This section clarifies assumptions and the scope of our solution. The granular details and specifications will be explained.

Biometric system works under two specific principles which are verification and identification. Verification in biometric systems is differing from identification, in terms of comparing the obtained biometric information against the saved themes which corresponds to all users in the saved database, while, verification stands to comparison between required identities with the specific attached templates.

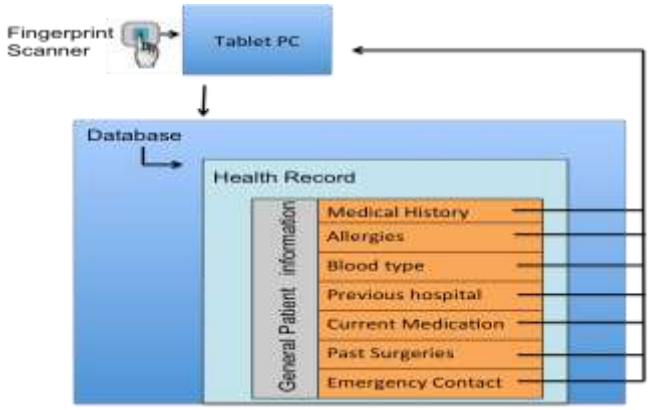

Figure 1: Health record retrieval with privacy-preserved policies

4.1 Using the system

There are two hardware components, two software components, and a set of privacy-preservation policies in our system architecture. First, the biometric terminal user collects the patients fingerprint image. Then, they select the *identify command* from the system user interface. It is important to note that collecting a patient's fingerprint during this scenario study is feasible even if the patient is found unconscious. The fingerprint image is then sent as a SQL query to the central database through the biometric terminal's connection for matching. After this process, the result is either the set of privacy preserved values from a record or a not found message.

Database Design & Population

The database is designed in first normal form and created by MySQL open source software. Relations are populated by fingerprints and notional electronic health records (EHR) for a more realistic scenario in experiments. Each EHR has an ID number, binary data column (fingerprint image), and several attributes specifying different medical information or history of patients.

Data Base:

Many methods are used for fingerprint data collection. In the implemented approach to collect data from individuals patients. These fingerprints data define any thump of patient. The data was collected from more people. The traditional fingerprints data are converted into electronic data to be ready for the processing for emergency extraction.

V. CONCLUSION

This paper provides insight on how use of biometrics together with new hardware and software technologies can be of significant advances in the combination of privacy preservation concerns and pre-hospital emergency cases. The proposed system describes a biometric terminal that exploits mobile technology to send fingerprint of patients from an emergency scene to a central database, and receive the health information of the patient to provide proper care to them in pre-hospital environment.

ACKNOWLEDGMENTS

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. Shraddha Kirve Madam for time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Futronic, FS88 FIPS201/PIV Compliant USB2.0 Fingerprint Scanner http://www.futronic-tech.com/product_fs88.html

[2] Griaule Java Software Development Kit 2009 http://www.griaulebiometrics.com/ page/en-us/fingerprint_sdk

[3] Microsoft Health Vault http://www.healthvault.com/ Personal/index.html.

[4] The MedicalAlert Key http://www.healthcentral.com/ migraine/reviews-202629-5.html

[5] U.S. Department of Health & Human Services, HIPAA Privacy Rule Summary, http://www.hhs.gov/ocr/privacy/ hipaa/understanding/summary/i ndex.html

[6] Akinyele, J., Pagano M., Green, M., Lehmann, C., Peterson, Z., and Rubin, A. 2009. Securing electronic medical records on smart phone. SPIMACS '09 Proceedings of the 1st ACM workshop on Security and privacy in medical and home-care systems, (Hyatt Regency Chicago, IL, November 9- 13I, 2009), ACM New York, NY.

[7] Cannoy, S. D. and Salam, A. F. A framework for health care information assurance policy and compliance. Communications of the ACM, vol. 53 Issue 3, March 2010. 126-131.

[8] Dillema, F., and Lupetti, S. 2007. Rendezvous-based access control for medical records in the pre hospital environment. In HealthNet 07' Proceedings of the first ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, (San Juan, Puerto Rico), ACM New York, NY.

[9] Hinkamp T. System providing medical personnel with immediate critical data for emergency treatments. Patent Application Publication 11/510,317, 2007.

[10] Kulkarni, S. and Agrawal, R. 2008. Smarphone driven healthcare system for rural communities in developing countries. HealthNet '08 Proceedings of the 2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, (Breckenridge, Colorado, June 17, 2008), ACM New York, NY.

[11] Salter, J. and Schroeder M. The Protection of Information in Computer Systems. Proceedings of the IEEE, 63(9), 278-1308 (1975).

[12] Sharma, D. and Kumar, A. Multi-Modal Biometric Recognition System: Fusion of Face and Iris Features using Local Gabor Patters. International Journal of Advanced Research in Computer Science; vol 2, No. 6, Nov-Dec 2011. 166-175.

[13] Shrili-Shahreza, S. New Anti Spam Protocol Using CAPTCHA. Networking Sensing and Control IEEE International 15-17, April 2007.

[14] Sukhai, N. 2004. Access Control & Biometrics. InfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development, ACM New York NY.

[15] Maltoni, D., Maio, D., Jain, A.K and Prabhakar, S. Handbook of Fingerprint Recognition 2nd. Springer Publishing Company, 2003.

[16] Paik, M., Samdaria, N., Gupta, A., Weber, J., Bhatnagar, N., Batra, S., Bhardwaj, M., and Thies, W. 2010. A biometric attendance terminal and its application to health programs in India. NSDR '10 Proceedings 4th ACM Workshop on Networked Systems for Developing Regions, (San Francisco, CA, 15-18 June, 2010), ACM New York, NY.

[17] Pankanti, S., Prabhakar S., and Jain, A. On the individuality of Fingerprints. IEEE Transactions on pattern analysis and machine intelligence, vol. 24, No. 8. August 2002.

[18] Prabhakar S., Pankanti, S., Jain, A. Biometrics Recognition: Security and Privacy Concerns. IEEE Security & Privacy, IEEE Computer Society, March- April 2003. 33-42.