ISSN 2395-1621

Survey paper on Medical history extraction using Biometrics

[#1]Pooja S. Satav, [#2]Vaibhav Raut, [#3]Rasika Duche, [#4]Devyani Tiwari
[#5]Assistant Professor. Bhagyashree Dhakulkar

[1]poojasureshsatav4075@gmail.com
[2]en.vaibhavraut@gmail.com
[3]rasikaduche06@gmail.com
[4]devyanitiwari009@gmail.com
[5]bhagyashree.dhakulkar@dypic.in

[#12345]Department of Computer Engineering
Dr. D.Y. Patil School Of Engineering and Technology
[SPPU]

ABSTRACT

Time is an important factor in providing medical aid, in case of emergencies. Timely help can save a person's life. We are going to develop real time system which provide medical data about patient in moving ambulance. These details can further be used to care the victim and thus provide an easy and reliant system to the medical department. The proposed system is based on biometric matching of identification parameters for retrieval of medical data of patient. On research of long period of time biometric system has shown advanced future. Biometric should be in the ambulance so driver or nurse could get information about victim and send respective hospital which would help the doctor's to be ready for their treatment. This would also help to make phone call to their relatives which are nominated by the victim at the time of filling information. This information is stored at cloud in authorized hospital. For fingerprint recognition biometric is used and for fingerprint matching minutiae algorithm is used.

Keywords
Fingerprint, Emergency, medical health record.

ARTICLE INFO

Article History

Received: 20th November 2017

Received in revised form :

20th November 2017

Accepted: 23rd November 2017

Published online :

13th December 2017

I. INTRODUCTION

In real world problems time is an important constraint in health related problems time is of at most important as someone's life is at stake. So here we developed a system which can provide real time data about person medical history in a moving ambulance so these details can further be used to cure the victim and these provide an easy and reliant system to the medical department.

Modern hospital system is efficient to provide privacy preserved access to the health record of the patient. Hospitals provide a relatively easy access to authorized patient.

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.

The implemented experiments area real world scenario in which an ambulance reaches an emergency patient within short period of time. The patient health record will be displayed to nearest doctor within less time[7]. It contains relative contact details and addresses to contact in emergency cases.

Biometric System:

Biometric system is a system of using biological data in technology for recognizing human body characteristics based on physiological or behavioral people possesses. Biometric human characteristics allow expertise to build a strong technique for security systems. This system is more applicable in today's recognition technologies because biometric systemcannot be stolen or forgotten. So that the

traditional security ways such as using passwords and ID cards are not strong enough for security purposes in today's technology world .Biometric system works under two specific principle 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 save database, while, verification stands to comparison between required identities with the specific attached templates [11].

Biometric recognition in a general term of technology refers to find pattern or shapes which are already stared it will be ready to compare these patterns and shapes which are used to test the system. There are many uses of biometric systems such as authentication in bank accounts which makes a reliable system. In this situation physical accesses to the bank account

would be more secure and this leads to provide better security [12].

Fingerprint is a means of access control and finds correct details of patient authentication and authorization. It contains: iris, voice, face, fingerprint, and hand geometry recognition. Biometric features possess an if-and- only-if relationship. 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.

Fingerprint recognition:

Fingerprint recognition is a process of decision making two sets of fingerprint ridge true are from the same human. Has proven that it cannot match the fingerprint that is similar in the two human in the world. There are multiple style guides that are used in many different ways of fingerprint which are minutiae, correlation and ridge pattern [13].

Fingerprint Recognition is one of the most widely used biometric system in the modern technology. Biometric system can be used such as verification mode or identification mode rely on the requirement of an application. Verification is different easy and fast process, the system process conducts a one-to-one comparison and so verification is faster. Identification is different of features of query fingerprint image with available fingerprint images in database, the system process conducts a one-to-many comparison [14].

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 which is wasting in the hospital to analyze medical history?The problem that occurs is that if the person is not identified it is difficult to extract exact information of the person and the person's life might be in danger due to the absence of any identity information at the accident place.

III. LITERATUREREVIEW

There are several approaches to access electronic health records (EHR) in emergency situations. This section reviews them asfollows.

Web services such as Microsoft Health Vault and former Google Health provide space to store medical information for any registered user [3]. This type of service is effective at storing information, but it depends on the patient's credentials, e.g. username and password. It lacks the ability to access information in real world situations where patients may forget such credentials or may simply be unable to provide such information in a given circumstance.

Another approach for storing and sharing medical information is via a flash drive [4]. The Health Key is a USB flash drive sold by Medical Alert. It provides storage for medical records. However, when it is inserted into a computer it automatically prompts the user with its contents. Thus, the device is meant to be inserted only into physicians' computer in order to not violate privacy of is content. This is a high risk to a patient's privacy because of possible misuse by strangers. Robbery and theft may result in identity theft. Also, it is difficult to keep such information up to date.

Some approaches suggest a carried-on token—e.g. wearing a smart band—such as the one proposed by Hinkamp in which patent suggests a health system built around the smart band, which stores patients' health data [9]. The data can then be retrieved by a server network and displayed on a screen. While this proposition provides a good solution for real time access on an emergency situation, it is dependent on the assumption that a patient will be carrying one; thus, it deemed unfeasible for the basis of a health system.

Another carried-on token approach is called rendezvous-based access control [8]. It rejects using the Internet to access patients' EHR. Instead, the data is replicated inside global system for mobile communication (GSM) servers stationed at every emergency environment, e.g. placing one inside an ambulance. Emergency medical technician gain access to the patients' EHR file through the use of a token, which contains the encrypted key, provided by the patient. This approach is efficient at decentralizing patient information because each GSM server stores its data independent from others. However, it is not effective in practice due to its dependency on a carried-on token.

Other approaches require the use of smartphones' Internet capability for accessing web services [3]. Kulkarnim and Agrawal propose a healthcare system for developing countries based on using smart phones as tokens [10]. Smartphones act as a beacon for health information with the use of external hardware sensors. The system basically consists of smartphone handlers or facilitators in each community to which one can go for medical guidance. Although this is not targeted for emergency access, it serves as a precursor to a modernized healthcare system which employs mobile technology. Yet, it is still token-based.

Another example of relying on a smartphone token is described in an approach by Gardner et al. [6]. In their approach, patients must carry their medical record inside their phone. Privacy is preserved with the division of access capabilities, so called secret sharing. Secret sharing refers to the case that privileges of granting access to an object are divided into different layers. For example, when a user wants to access their own health record, they must enter the right combination of password and biometrics to gain the access.

The need for a token-less option is in place. Our solution is based on the approaches introduced by Gardner et al. [6] and Paik et al. [2]. The former proposes using of biometrics for authentication and authorization. The latter proposes to apply biometrics to register and identify people and their attendance. Their approach is tailored for registrar methods in India, as their growing population is overwhelming. The idea is to create a biometric attendance terminal that eliminates the need for keys by using fingerprints: once registered, a visitor can log her attendance by scanning her chosen finger once. None of the approaches focus on accessing EHR's in emergency care or privacy preservation in such cases. Yet, the biometric terminal serves as a good example of how biometrics is effective in suchproblems.

IV. PROPOSED SYSTEM

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

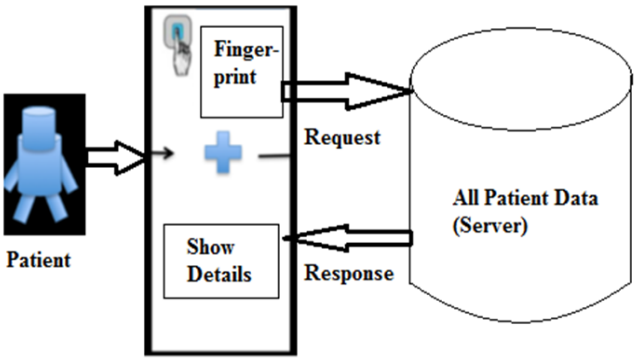

Figure 1. System preparatory events

a. System Architecture

The system architecture is defined as a unimodal biometric system that uses a singular biometric feature.

In this System Architecture we are using one biometric device for taking the finger print of patients. When the accident is happened first we take the finger print of patient. After getting the fingerprint of the patients. System send request to the database for extracting the patients history.

In the patient history we are storing medical history of patients like Past surgery, Allergy, Blood type, Previous hospital, Current medication and we are also store personal information of patients like Name, DOB, Age, Gender, Address and relatives Contact Number etc.

Database check the patient fingerprint is valid or not. If the patient fingerprint is valid then database server send back response to the system otherwise database server send the response patient is not register their information in government hospital.

After getting the response from the database server system will display the all information about patients.

System Component Description

System components consist of both hardware and software elements. Hardware components include a fingerprint scanner, and a hosting server computer. Figure 2 depicts our system components architecture linked in functional sequence in order to demonstrate the sequence of events.

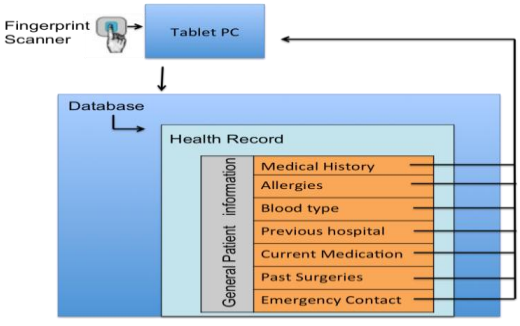

Figure 2: Health record retrieval with privacy-preserved policies

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.

V. IMPLEMENTATION

Our approach will be a junction of four components: fingerprint scanner, remote capable device (PC), the matching algorithm, and an electronic health record database. The system has been implemented with the products listed in Table I.

Table I. Implementation components

Component	Implementation
PC	For Connection
Fingerprint Scanner	Authentication
Fingerprint Matching Algorithm Software	Search exact records from dataset
Controller	Microcontroller

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 thumb 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.

VI. CONCLUSION

We have proposed this system to cater the medical needs of the people in need. This system will store the information of the people in the designated database that can be used to retrieve the information in emergency case. The proposed system makes use of person's fingerprint to store the relative medical information. Also the results and analysis shows that the proposed system yields to better results in comparison of other approaches.

This paper provides insight on how use of biometrics together with new hardware and software technologies which 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.

VII. ACKNOWLEDGMENTS

I wish to express my profound thanks to all who helped us directly or indirectly. Finally I wish to thank to all our friends and well-wishers who supported us in completing this successfully. I am especially grateful to our guide Prof. Bhagyashree Dhakulkarfor time to time, very much needed, valuable guidance.

REFERENCES

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

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

[3]TheMedicalAlertKeyhttp://www.healthcentral.com/ migraine/reviews-202629-5.html

[4]Akinyele, J., Pagano M., Green, M., Lehmann, C., Peterson, Z., and Rubin, A. 2017. 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, 2017), ACM New York, NY.

[5] Canny, 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 2016*.126-131.

[6] Dilemma, F., and Lupetti, S. 2015. Rendezvous-based access control for medical records in the pre hospital environment. In *Health Net 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.

[7] Hinkamp T. System providing medical personnel with immediate critical data for

emergency treatments. Patent Application Publication 11/510,317, 2017.

[8] Kulkarni, S. and Agrawal, R. 2016. Smartphone 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, 2016), ACM New York,NY.

[9] Paik, M., Samaria, N., Gupta, A., Weber, J., Bhatnagar, N., Batra, S., Bhardwaj, M., and Thies, W. 2015. 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, 2015), ACM New York, NY.

[10] 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 2016*

*[11]*A. K. Jain, K. Nandakumar ,A. Nagar, "Biometric template security," EURASIP Journal on Advances in SignalProcessing, Special Issue on Advanced Signal Processingand Pattern Recognition Methods for Biometrics, 2016

[12] B. Yang, D. Hartung, K. Simoens, C. Busch, "Dynamic Random Projection for Biometric Template Protection," Proc. 4th IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp. 1-7, 2015

[13] U. S. Tomar, et al., (2015) "A Proposed Faht Model for Fingerprint Recognition", International Journal of Engineering Science & Research Technology, vol. 4, no. 5: May, 2015.

[14] S. Bhairannawar, B. Raja, K. Venugopal, "An Efficient Reconfigurable Architecture for Fingerprint Recognition", "Hindawi ", Volume 2016, Article ID 9532762, 22 pages.

