ISSN 2395-1621

BIOMETRIC APPROACH FOR PATIENT HISTORY EXTRACTION

[#1]Shubham Nayak, [#2]Manoj Dhorepatil, [#3]Aishwarya Ankolikar, [#4]Suraj Bandal,
[#5]Prof. Sunita Nandgave

[1]srajnayak6111@gmail.com
[2]dhorepatilmanoj@gmail.com
[3]aishwaryaankolikar@gmail.com
[4]surajbandal78@gmail.com

[#1234]Student, Department of Computer
[#5]Assistant Professor, Department of Computer
GHRCEM, Pune.

ABSTRACT

Patient Efficient and privacy-preserved access to the health record of patients is necessary to correctly practice medicine. This research addresses two concerns in emerging health software systems. First, electronic health records are not yet remotely accessible without using a token (e.g. health card). Second, patients' privacy must be preserved even in special situations such as emergency cases. This system proposes to exploit biometric identification to access a central health record database featured by privacy policies. The experiments the scenario in which an ambulance reaches an unconscious patient who needs pre-hospital medical care for which their health record is retrieved from the database.

Keywords : Biometrics, Emergency, Health record, EHR.

ARTICLE INFO

Article History

Received: 26th May 2018

Received in revised form :

26th May 2018

Accepted: 30th May 2018

Published online :

31st May 2018

I. INTRODUCTION

Today's medical, hospital, enters 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.

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 risk 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 to extract medical history of a patient/person using fingerprint in emergency cases.It is difficult to extract exact information of the person and the man's life might be in danger and the absence of any identity information at the accident place, the necessity to establish and maintain a new, local-given identity, correlated to specific, individual, medical problems, all the time, from the accident place to hospital and eventually, from a hospital to another, presents a particular importance.

III. LITERATURE REVIEW

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

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 MedicAlert. It provides storage for medical records. However, when it is inserted into a computer it automatically prompts the user with 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.

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 smartphones 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. 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 such problems.

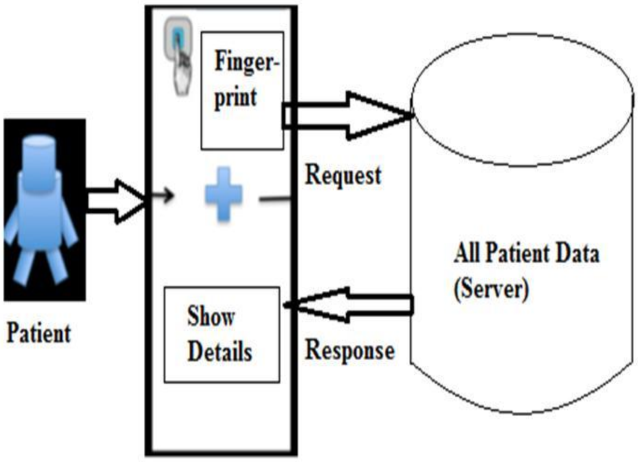


Fig 1: System Architecture

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.

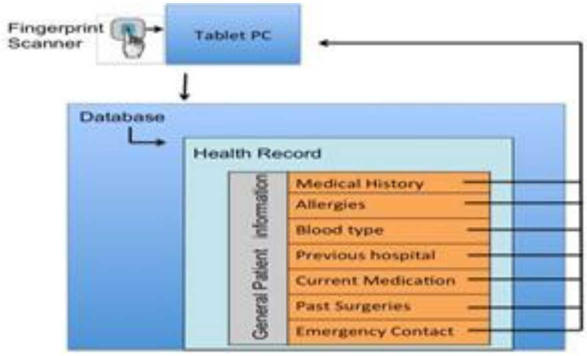


Figure 2: Health record retrieval with privacy-preserved policies

IV. PROPOSED MODEL

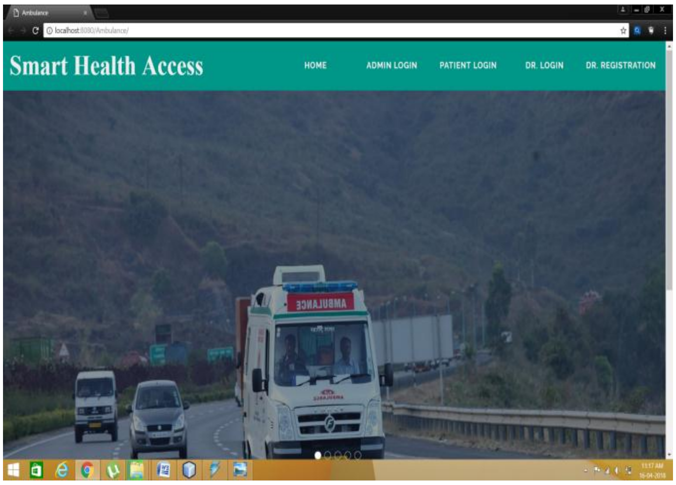
This section clarifies assumptions and the scope of our solution. The granular details and specifications will be explained.

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.

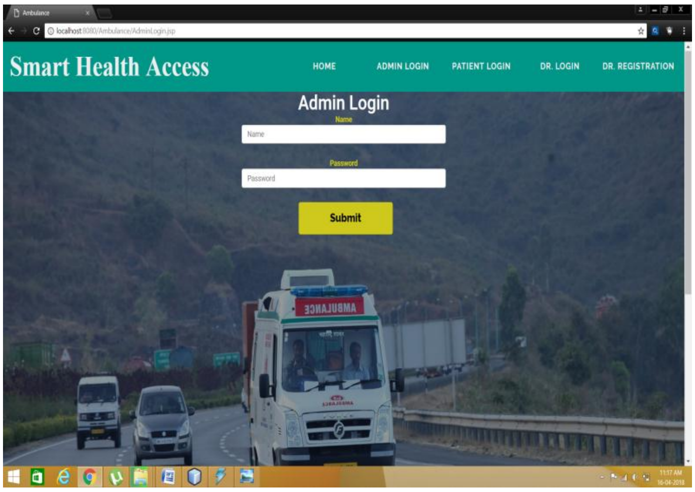
There are two hardware components, two software components, and a set of privacy-preservation policies in our system architecture. First, the biometric terminal user collects the patients fingerprint image. Then, they select the identify command from the system user interface. It is important to note 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

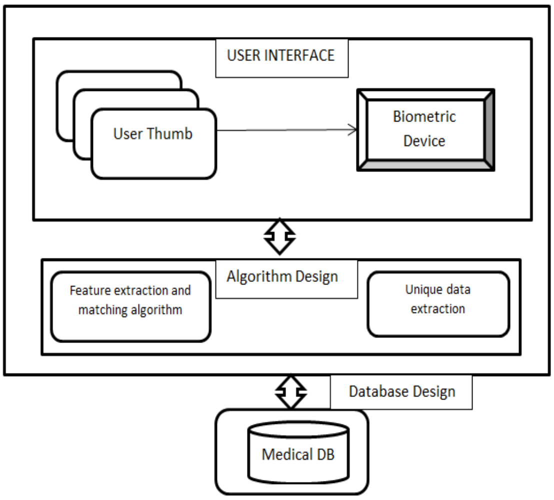
Our system has four components: fingerprint scanner, remote capable device (PC), the matching algorithm, and an electronic health record database.



Home Page



Admin Login



5.1 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.

ARDUINO :

Arduino is an open source computer hardware and software company,project,and user community that designs and manufactures single board microcontrollers. There aew variety of micoprocessors and controllers used for designing the Arduino .The name Arduino comes froma bar in ivreaitly.

Figure3 Arduino

VI. 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.

VII.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.Sunita mam 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 FingerprintScanner. http://www.futronictech.com/ product_fs88.html

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

[3] Microsoft Health Vaulthttp://www.healthvaut.com/ Personal/index.html

[4] The Medical Alert Key http://www.healthcentral.c om/migraine/reviews-202629-5.html

[5] 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 ACMworkshop on Security and privacy in medical and home-care systems, (Hyatt Regency Chicago, IL, November 9- 13I, 2009),ACM New York, NY.

[6] Cannoy, S. D. and Salam, A. F. A framework for health care information assurance policy and complianceCommunications of the ACM, vol. 53 Issue 3, March 2010.126-131.

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