Impact Factor Value 4.046 **e-ISSN: 2456-3463**
International Journal of Innovations in Engineering and Science, Vol 4, No.10,2019
National Level Technical Paper Presentation- PHOENIX-19
Organized by Godavari College of Engineering, Jalgaon - 425003
www.ijies.net

A Survey on Implementation of E-Health Record With Biometric Authentication

Roshani Ashok Sonar [1], Hemraj V. Dhande[2], Hemant Ingale[3], Anil D. Vishwakarma[4], Vijay D. Chaudhari[5]

[1] *M.Tech. (VLSI & Embedded System Design) Scholar* [2,3,4,5] *Asstt. Prof.*
[1,2,3,4,5]*E&TC Engg. dept, GF's Godavari College of Engg., Jalgaon-425003, Maharashtra, India.*

Abstract – *In the health care industry, when it comes to patients safety and security, the most important and talked subjects are patient recognition and patient data truthfulness. Pharmaceutically the fingerprints of every indivisuals are unique and permanent, the use of fingerprint biometrics would provide to be a reliable and accurate method to efficiently identify the patients. The best part of the fingerprint technology is that apart from safeguarding the patient's information, it also protects against fraud and minimizes human intervention. Such use of this technology minimizes the need to enter new information into patients' records, limiting the human element involved with data entry. Thus it make easier to match the patients' records for his/her future visits. Organizations or institions using the Fingerprint Recognition Technology mostly use the fingerprint scanners. Simply,by placing a finger on a self-service kiosk or other reading device, the enrolled patients get registered quickly at the entry point, like the emergency department, inpatient areas or outpatient locations.*

Keywords- Biometrics emergency, Patients' record, E-Health fingerprint, biometrics.

1. INTRODUCTION

Internet of things (IOT) is changing the human life one step ahead. With the new technology level, IOT is change the normal human life to smart life. In the recent years, the use of computer technology strenghthen the health care services has received significant outcomes,it also helps to provide the online healthcare services.The Patient Information Management System (PIMS) is an advanced automated system that is used to manage and record patient information and its administration. It is meant to provide the Administration and Staff, with data in real-time to make their work more interesting and less stressing.

A patients medical record includes identification, history of medical diagnosis, treatment received medication history, dietary habits, genetic information, psychological profiles etc. The above security problems are overcome by using biometrics technology by providing realiable and secure user authentication compared to the traditional approaches. This study analyze the security and privacy issues in e-Health.e-Health boost the quality of healthcare by making patients health information easily accessible, improving efficiency and reducing the cost of health service delivery. There are good reasons for keeping the records private and limiting the access to only minimum necessary information. Biometrics is a significant security mechanism that assigns a unique identity to an indivisual according to some behavioral (signature and voice) or physiological characteristics (fingerprint or face). Hence, biometrics is more reliable and capable than traditional authentication approaches of distinguishing between an authorized person and an exploiter. Biometrics refers to technologies that used to measure and analyse indivisual physical or behavioral characteristics to automate the authentication process of user. Biometric tricks cannot be lost or unremembered; they are tough to duplicate, share, or distribute. Moreover, it requires the presence of the person being authenticated; it is difficult to forge, and unlikely for a user to reject. Biometrics offers a sense of security and convenience both to patients and physicians alike. In order to stay ahead of the emerging security threats posed by e-Health, healthcare organizations are moving from traditional approaches to the utilization of biometrics technology.

This paper explores the safety and privacy issues in e-Health as they continue to abide challenges for the healthcare industry. In addition, it pursue to embark on a review to highlight the applications of biometrics in addressing some of the e-Health security and privacy challenges. The research pointed on biometrics applications in user authentication and health data encoding. We believe that this study will provide a good foundation for further research in the area of healthcare data security and patient privacy protection.

Electronic Health (E-Health)

Recent advances in the field of telemedicine around the twentieth century covered the way for e-Health. Following that came developments in computerization, digitization of data, and digital networks which help to a multiplicity of e-Health applications. Currently, e-Health contain a whole range of services or systems at the edge of healthcare and information technology such as: telemedicine, which is defined as a remote healthcare delivery system using telecommunication and information technology; which include electronic health information about a patient or individual; consumer health information processing, which is use of medical computing to examine customer needs for information; health knowledge management, which aims to collect, describe, organize, share, and effectively use healthcare knowledge; medical resolution support systems, which are interactive expert systems that serves health professionals with decision-making tasks. The underlying factor in all these technologies is the digitization of data. In that regard, the term (e-Health) suggests digital health information in contrast to a paper-based system. E-Health is an transpire field of medical informatics that refers to the organization and delivery of health services and information using the internet and related technologies. In a broader sense, e-Health include the application of information and communication technologies in healthcare. It involves all digital health-related information, encompassing products, systems, and services. The term health does not solely refer to medicine, disease, or healthcare but also enclose public health and healthcare. The selection of e-Health services achieves different goals including: increased efficiency in healthcare, enhanced quality care, evidence-based medicine, empowerment of consumers and patients by broadening the knowledge base of medicine, encouragement of new relationships between patients and health professionals, education of physicians and patient, enabling information exchange and communication, extending the scope of healthcare and promoting equity in healthcare. In short, it assist health information sharing, ensures effective healthcare, and empowers health consumers to manage their own health. Several studies that have been undertaken in the field of e-Health have clear system architecture in order to represent a proposed e-Health system.

Biometrics

Biometrics (ancient Greek: bios ="life", metron "measure") refers to two very non-identical fields of study and application. The first, which is the older and is used in biological studies, including forest management, is the collection, synthesis, analysis and management of quantitative data on biological communities such as forests. Biometrics in reference to biological sciences has been studied and applied for several generations and is somewhat simply viewed as "biological statistics" [1].

Authentication is the act of initiating or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. A short overview in this field can be cleaved into three parts and they are Past, Present and Future. The physical characteristics of a person like finger prints, face, voice, hand geometry and iris (optic) are known as biometrics. Each biometric scheme has its strengths and weaknesses. The suitable biometric can be selected depending upon the application in various computer based security systems. The important features of the various biometrics are discussed briefly in this section.

The Biometric Recognition Systems are used to recognize the person based on the feature vectors of any one of the biometric that the person possesses. These systems are person authorized systems hence offer more protected and convenient process of identification compared to alternative methods of identification. The computer based security systems are used in various commercial, civilian and forensic applications. Each person has to establish the identity ranging from drivers' license to gaining entry into a country to the passport. The biometric system uses the individual's physical characteristics like fingerprint, hand geometry, face, voice or optic. They are more responsible and secure as they provides the access to authorized users in their physical presence. A simple biometric system consists of four modules: Image/Voice acquisition, Preprocessing, Feature extraction and Recognition systems.

i.Finger Prints

From long time,the finger prints of a person have been used as person Identification. A finger print is the design of rids and hollow on the surface of a finger tip. The finger prints of the identical twins are different. It is obtainable scan the finger prints of a person and can be used in computer for number of applications. This method is conventional and it gives accuracy for currently available Fingerprint Recognition Systems for authentication [2]. This fingerprint recognition system is becoming affordable in a large number of applications like banking, Passport etc.

ii. Face

The commonly used biometric characteristics for person identification is face. The most popular proposal to face recognition are based on shape of facial indication, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. As this technique includes many facial elements; these systems have difficulty in matching face images [3]. The face recognition systems which are used currently impose a number of limitation on how facial images are obtained. This face recognition system automatically detects the correct face image and is able to recognize the person.

iii. Voice

In various applications, the voice recognition systems have been currently used. Voice is a combination of both physical and behavioral biometrics. The features of person voice are depend on the vocal tracts, mouth, nasal activities and lips movement that are used synthesis of sound. These physical characteristics of human speech are steady for individuals. The behavioral part of the speech of person changes over time due to age, medical conditions, and emotional state. The speaker dependent voice recognition systems are text abased; and the speaker independent systems are what he or she speaks [4]. The speaker dependent voice realization system is more difficult to design but provides more protection.

iv. Hand Geometry

The hand geometry recognition systems are depend on a number of measurements taken from the human hand, including its shape, size of palm, length and width of the fingers. This method is very simple and easy to use. As there is no reaction of environment factors such as dry weather or dry skin, this does not appear to have dry negative effects on the authentication accuracy. Also hand geometry information may not be constant during the growth period of the children [5].

v. Iris (optical method)

The biological feature of a human is iris. It is a unique structure of human which remains constant over a person lifetime. The iris is the sperical region of the eye. The left and right side irises of an individual can be treated as separate unique identifier. The iris information can be collected by optical image. The accuracy of iris based recognition system is promising. Each iris is believed to be extraordinary and even the optic of identical twins are also different [6]. The iris recognition system has become more users friendly and cost effective technique. The iris have a very low false acquire rate as compared to other biometrics like finger print, face, hand geometry and voice.

2. LITERATURE REVIEW

European experimenter Joao de Barros recorded the first known example of fingerprinting [6], which is a form of biometrics, in China during the 14th century. Chinese merchants used ink to take children's fingerprints for recognition purposes. In 1890, Alphonse Bertillon studied body mechanics and measurements to provide help in identifying criminals. The police used his method, the Bertillonage method, until it falsely identified some subjects. The Bertillonage method was quickly deserted in favor of fingerprinting, brought back into use by Richard Edward Henry of Scotland Yard. Karl Pearson, an applied mathematician studied biometric research early in the 20th century at University College of London. He made important discoveries in the field of biometrics through studying statistical history and interaction, which he applied to animal evolution. His historical work involved the method of moments, the Pearson system of curves, correlation and the chi-squared test. In the 1960s and '70s, signature biometric authentication procedures were developed, but the biometric field survived fixed until the military and security agencies researched and developed biometric technology beyond fingerprinting.

M. Wcislik et al [7] monitors patient's body temperature, pulse rate, ECG wave and patient's body position using ARM cortex M4F micro controller. Android app is made for monitor these values. Bluetooth connection is used for connecting microcontroller and Android phone. In his paper monitor patient's body temperature, Respiration rate, heart rate and body movements using Raspberry Pi board and sensors. Android app is provide support only android phones. Bluetooth is very short distance for communication. It supports only within 100

meters. In this project webpage is created. Using IP address anybody can monitor patient's health status anywhere in the world.

Amir-Mohammad Rahmani et al [8] monitor ECG wave using panda board. Ethernet connection is used for connecting internet to the panda board. In this paper monitor body temperature, Respiration rate, heart rate and body movements using Raspberry Pi board. Panda board is very difficult to operate compare to Raspberry Pi board. Ethernet connection is also very short distance. So author use USB modem for connecting internet to the Raspberry Pi board.

Hoi Yan Tung [9] et al monitors body temperature, ECG, heart rate using DRZHG micro controller. A Dual Radio ZigBee Homecare Gateway (DRZHG) has been present and implemented to support remote patient monitoring. The idea of remote patient monitoring is to concurrently track the status of long-term patients at home by using mobile medical sensors. The sensors collect medical data from patients and feedback the data to the doctors and users. Zigbee module is used for connected to the micro controller. Zigbee module is used for transfer the values to the receiver side. It is send data to only nearest place. But this project internet is connected to the Raspberry Pi board. So using IP address anybody can monitor patients health status anywhere in the world.

Joao Martinhoa [10] et al describe the design and prosperous implementation of a remotely operated physiological monitoring device. The three types of prototype performs acquisition of physiological measurements electrocardiography, finger photoplethysmography, and blood pressure plethysmography. For connecting these sensors Atmega 328 microcontroller is used. For connecting internet to the atmega 328 microcontroller Wifi connection is used. After connecting Wifi connection it will transfer the values. If wifi hotspot is no means it is not transfer the values. Wifi is also works on short distance technique. In project USB modem is used for connecting internet to the Raspberry Pi board. So it is easily connect to the internet in any place and anywhere.

Microsoft Health Vault gives Web facilities such as Microsoft Health Vault and former Google Health provide space to store medical information for any registered user [11]. This type of service is fruitful at storing information, but it depends on the patient's authorization, 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 environment.

The Medical Alert Key explains another approach for storing and sharing medical information is through a flash drive [12]. The Health Key is a USB flash drive sold by MedicAlert. It furnishes storage for medical records. However, when it is inserted into a computer it automatically prompts the user with its fulfilments. Thus, the device is meant to be inserted only into physicians' computer in order to not infringe 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 troublesome 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 [13]. The data can then be recovered 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 unachievable for the basis of a health system.

Another carried-on token approach is called rendezvous-based access control [14]. It rejects using the Internet to access patients' EHR. Instead, the data is counterfeit 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 encoded key, provided by the patient. This approach is efficient at localising patient information because each GSM server stores its data independent from others. However, it is not constructive in practice due to its dependency on a carried-on token.

Other approaches require the use of smartphones' Internet capability for accessing web services [11]. Kulkarnim and Agrawal propose a healthcare system for developing countries and nation based on using smartphones as tokens. Smartphones act as a bonfire for health information with the use of external hardware sensors. The system basically consists of smartphone 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. [15]. In their approach, patients must carry their medical record inside their mobile phone. Privacy is protected with the division of access capabilities, so called secret sharing. Secret sharing refers to the case that liberty 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, code to gain the access.

2.1 PROBLEM STATEMENT

The main problem that we addressed was dealing with patient medical document. It is the situation that flock us to techniques of developing this Patient Information Management System to be used to enable them to handle details on policies efficiently and effectively. Problems Encountered during Data collection: sensitive information released to us, few projects and books written about patient records management system. Problems Encountered during System Design: Limited time to finish up the work, limited numbers of computers with the internet in the faculty hence it becomes difficult down load PHP codes from the internet.In all the previous systems so many sensors are used for observing the patient so that the system becomes bulky.

2.2 PROPOSED SYSTEM

The proposed architecture for healthcare integration offers clear benefits to citizens by improving patient health quality through the provision of appropriate information to help guide medical decisions at the time and place of care.

In our system if the patient come in the hospital is new then the system will ask for new enrollment or the new entry, then we manually enter all the information related to that patient like his/her name, address, aadhar number, blood group, body temperature, pulse rate, blood pressure, diagnosis, allergy, prescription, if the patient is appear at second time then we also enroll the previous admit date and discharge date as well as number of visits. This information is globally appear anywhere anytime, so that the patient does not need to carry their file. Even if the patient changing the hospital then also at that hospital if this system is installed then entering the fingerprint of the patient the previous all history in front of the doctor due to this it is easy to doctor to appropriately treat the patient. It is not necessaryto show all the internel system working like how the fingerprint process will happen etc.

In our system we used raspberry pi 3,one USB to TTL converter and fingerprint module. software part include python as well as putty software. To reduce complexity and to have affordable system we use less hardware.

3. CONCLUSION

In our project, fingerprint verification is considered to protect the medical information and the confidentiality of data. Patient data can be stored and retrieved by connecting to the hospital database and thus it can be access globally by using IOT. The main advantage of ths project is online accessibility of patient database. Another advantage is that it is applicable during emergency conditions. Medical record errors can be reduced by using finger print technique. The patient record management system offers a number of benefits to the user and can capture data, store, view, add and delete the records entered the data can also be posted information to the database. The implementation work is under progress and this paper s submitted as review paper.

REFERENCES

[1] *Smart Cart Alliance Identity Council (2007): Identity and Smart Card Technology and Application Glossary, http://www.smartcardalliance.org, as visited on 25/10/2008.*

[2] *A.K. Jain, L. Hong, R. Bolle, "On-line Fingerprint verification" , IEEE Trans. Pattern Anal. Mach. Intel. 1997.*

[3] *Steve Lawrence C. Lee Giles Ah Chung Tsoi, Andrew D.Back, "Face Recognition: A Convolutional Neural Network Approach", IEEE Transactions on Neural Networks, Special Issue on Neural Networks and Pattern Recognition.*

[4] *Bill Swartz, Neeraj Magotra, "Feature Extraction for Automatic Speech Recognition ", 1997 IEEE Transaction.*

[5] *Michael Goh Kah Ong,Tee Connie, Andrew Teoh Beng Jin,*
David Ngo Chek Ling, "A single-sensor hand geometry and
palm print verification system", Proceedings of the 2003.

[6] *John Daugman, "How Iris Recognition Works", IEEEtransactions on circuits and systems for video technology, vol. 14, no. 1, january 2004.*

[7] *M. Wcislik, M. Pozoga, P. Smerdzynski "Wireless Health Monitoring System", IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. pp 312–317,2015.*

[8] *Amir-Mohammad Rahmani, Nanda Kumar Thanigaivelan, Tuan Nguyen Gia, Jose Granados, Behailu Negash, Pasi Liljeberg1, and Hannu Tenhunen, "Smart e-Health Gateway: Bringing Intelligence to Internetof-Things Based Ubiquitous Healthcare Systems", 2015.*

[9] *Hoi Yan Tung, Kim Fung Tsang, Hoi Ching Tung, Kwok Tai Chui and Hao Ran Chi, "The Design of Dual Radio ZigBee Homecare Gateway for Remote Patient Monitoring", IEEE Transactions on Consumer Electronics, Vol. 59, No. 4, November 2013.*

[10] *Joao Martinhoa, Luís Pratesa, Joao Costaa,Adeetc, Isel, Rua Conselheiro Emídio Navarro 1, Lisbon, Portugal,"Design and Implementation of a Wireless Multi parameter Patient Monitoring System", Conference on Electronics, Telecommunications and Computers – CETC Hosting by Elsevier Ltd 542-549, 2014.*

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

[12] *The Medical Alert Key*
http://www.healthcentral.com/migraine/reviews-202629-5.html

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

[14] *Dillema, F., and Lupetti, S. 2007. Rendezvous-based access control for medical records in the pre hospital environment.*

[15] *Akinyele, J., Pagano M., Green, M., Lehmann, C., Peterson, Z.,*
and Rubin, A. Securing electronic medical records on smart phone. 2009.