Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.79 – 87

RESEARCH ARTICLE

A Study on Biometric for Single Sign on Health Care Security System

Dr. S. Manimekalai
Assistant Professor in Computer Science, Thanthai Hans Roever College,
Perambalur-621212, Tamil Nadu, India
E-mail: mega_somu@yahoo.com

Abstract - A Health System consists of all organizations, people and actions whose primary intent is to promote, restore or maintain health. This includes efforts to influence the determinants of health as well as more direct health-improving activities. Health care providers are institutions or individuals providing health care services. Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics. Biometrics has revolutionized the healthcare industry; devices can take unique information about you from your eye, your hand print, or your thumb print and use it to identify you. This information can be used to ensure that you are who you say you are, and you have permission to be working with the healthcare information you are trying to access. How can we provide an effective form of authentication that is supremely accurate, fast, and convenient, operates on multiple devices, platforms and software, and thereby, give time back to the doctor? The best solution to these kinds of problems is the use of biometric techniques for authentication. Already there are lots of biometric traits have been used for authentication in hospitals. In this paper, the authors are interested to review about the different biometric techniques used in health care systems.

Keywords - Biometric, Biometric Security, Healthcare, Fingerprint, Cloud

I. INTRODUCTION

A health system is therefore more than the pyramid of publicly owned facilities that deliver personal health services. They have also been described in the United States as "the five C's": Cost, Coverage, Consistency, Complexity, and Chronic Illness. Also, continuity of health care is a major goal.

Health care providers are institutions or individuals providing health care services. Individuals, including health professionals and allied health professions can be self-employed or working as an employee in a hospital, clinic, or other health care institution, whether government operated, private for-profit, or private not-for-profit (e.g. non-governmental organization). They may also work outside of direct patient care such as in a government health department or other agency, medical laboratory, or health training institution. Examples of health workers are doctors, nurses, midwives, dieticians, paramedics, dentists, medical laboratory technologists, therapists, psychologists, pharmacists, chiropractors, optometrists, community health workers, traditional medicine practitioners, and others.

In the everyday world of healthcare providers and facilitators, they are increasingly frustrated by the need to use complicated passwords, tokens, cards or other cumbersome forms of authentication to log in to their EHR (Electronic health records) system or to ePrescribe a drug. In most cases, they are required to authenticate 50-100 times per day. These methods are tedious, time-consuming and hardly secure, as passwords cards and tokens can be hacked or forgotten, shared or stolen, and so on. Thus, quality time with patients is sacrificed.

Biometric

Biometric technology is a secure and convenient identification method and it does not need to remember complex passwords, nor smart cards, keys, and the like. Biometrics is the measurable characteristics of individuals based on their behavioral patterns or physiological features that can be used to verify or recognize their identity. Physical characteristics include fingerprints, palm or hand geometry, iris, retina, and facial characteristics. Behavioral characteristics include signature, keystroke and voice pattern. With the combination of biometric technology products and modern computer technology, it is easy to perform monitoring, management, systems integration, automated management, and security applications.

Human identification leads to mutual trust that is essential for the proper functioning of society. We have been identifying fellow humans based on their voice, appearance, or gait for thousands of years. However, a systematic and scientific basis for human identification started in the 19thcentury when Alphonse Bertillon [1] introduced the use of a number of anthropomorphic measurements to identify habitual criminals. The Bertillon system was short-lived: soon after its introduction, the distinctiveness of human fingerprints was established. Since the early 1900s, fingerprints have been an accepted method in forensic investigations to identify suspects and repeat criminals. Now, virtually all law enforcement agencies worldwide use Automatic

Fingerprint Identification Systems (AFIS). With growing concerns about terrorist activities, security breaches, and financial fraud, other physiological and behavioral human characteristics have been used for person identification. These distinctive characteristics, or biometric traits, include features such as face, iris, palm print, and voice. Biometrics [2, 3] is now a mature technology that is widely used in a variety of applications ranging from border crossings (e.g., the US-VISIT program) to visiting Walt Disney Parks. Biometric recognition is based on two fundamental premises about body traits: *distinctiveness* and *permanence [4]*. The Fig 1 shows the biometric security system.

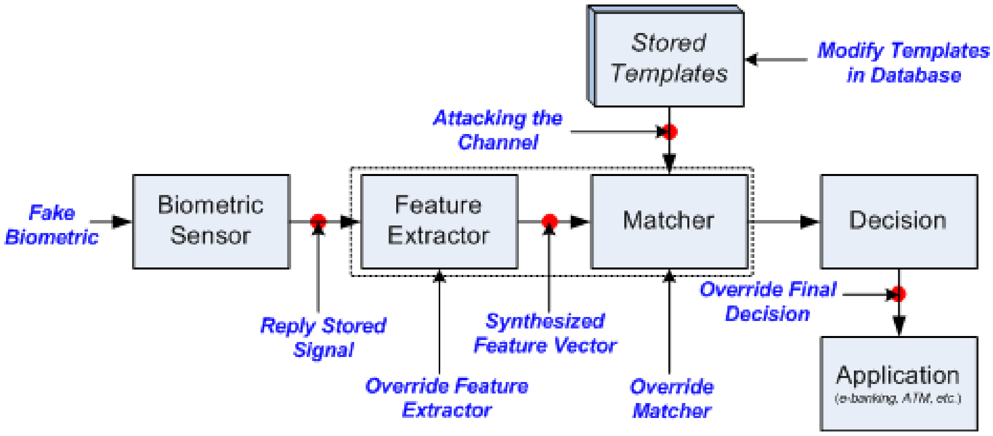

Fig. 1 Biometric Security System

II. BIOMETRIC IN HEALTH CARE INDUSTRIES

Biometric technology represents the future for positive healthcare identification and will enhance the secure use, storage, and exchange of personal health information [5]. Biometric identity solutions deter and reduce fraud by:

- Preventing card sharing and patient identity theft by authenticating the patient in the provider's location.
- In fee-for-service programs, preventing provider billing for "phantom claims" or services when a patient is not at the provider location on the service date.
- Verifying managed care "encounter data" or services from providers so that Medicare and Medicaid programs can rely on this reported data for setting of managed care rates.
- Creating an "audit trail" of check in and check out times for comparison against
  Type of service provided as an indicator of potential fraud called "upcoding."

Some of the main biometric identification technologies and how they're being used in clinical practice are described in the following sections.

1. Electronic record keeping

July 1, 2011 -- Radiologists are the undisputed leaders in adopting electronic record keeping. But the profession is behind the curve with biometric identification, a technology that's generating a sea change in security, IT and making impressive gains in hospital utilization.

Biometric identification eliminates password abuse, removes the need to remember multiple passwords, makes 90-day password changes transparent, and maintains security standards in a virtual desktop healthcare IT environment. When applied to patients, it can dramatically reduce data-entry errors and streamline patient workflow.

Like speech recognition dictation systems, the technology for biometric identification has been commercialized for years. Its primary markets have been law enforcement, the military and defence industries, and corporations with stringent security requirements.

However, this is changing. Healthcare IT represents a large, lucrative, and unsaturated market. Greater adoption of electronic health records (EHRs), which can consist of multiple information systems with unique passwords, combined with more internal security breaches at healthcare facilities, concern about patient identity theft, and increasingly stringent federal regulations regarding patient privacy, have brought biometric identification to the attention of hospital administrators.

1. Palm vein scanning

The palm vein scanning process uses near-infrared light to illuminate the hand's vein patterns and blood flow, which are unique to each individual. The process is fast and identification is accurate. The scanner is easily sanitized with antibacterial wipes.

Data from the scan are encrypted and stored in a database. The database interfaces as an overlay with other healthcare information systems, such as an electronic medical record or RIS (Radiology Information System).

2. NYU Langone Medical Center

On June 5, NYU Langone Medical Center launched its patient palm vein scanning system (Patient Secure, HT Systems) as part of a massive update of the hospital integrated delivery network's healthcare IT systems.

Dr. Edmond Knopp, associate professor of radiology and the informatics champion for the radiology department, spoke "Historically, when a patient came to one of our radiology departments for an examination, let's say an MRI of the knee, the patient would be given all sorts of paper documents to verify," he said. "Now, when that patient arrives at registration, he or she places their palm over the scanner. Verification occurs in seconds, and the patient's entire record is displayed."

The radiology department was part of the hospital-wide launch, and NYU's patient registration protocol requires that patients provide two forms of identification, including a photo ID. A digital photo is taken in addition to scanning the patient's palm.

Knopp believes that the technology will be particularly advantageous to facilitate unscheduled walk-in patients who need routine x-ray exams. He also pointed out that if patients enrolled in the system arrive unconscious or otherwise unable to identify themselves, the system could identify them immediately.

3. University of Wisconsin

On October 2010, The University of Wisconsin Hospital and Clinics in Madison introduced palm vein scanning here more than 2 million patients annually who receive treatment. Enrolment in the university's SAFE (Secure, Accurate, Fast, Efficient) system is not mandatory for patients, but it is encouraged. Children can be enrolled when they reach 5 years of age. The palms of these paediatric patients will be scanned annually through age 15 to accommodate their growth.

4. Fingerprint identification systems

Fingerprint identification is the most common type of biometric identification in hospitals and other healthcare facilities. These systems may be used exclusively by medical staff, for patient identification, or for both [5].

Having a biometrically validated single sign-on maintains HIPAA security requirements, reduces physician frustration, and -- most importantly -- saves time. The company references a 400-hospital survey that it commissioned to analyse the effects of single sign-on functionality. Conducted by the Ponemon Institute, the survey revealed that clinicians, on average, had to memorize between five and six unique passwords, and they spent between eight and 15 minutes per day logging into healthcare IT systems. Over the course of a year, this equated to 103 to 203 hours of unproductive time, Ting said.

"A fingerprint identification system shows in Fig.2 incorporates something you know, something you have, and something that is unique to you and cannot replicate," Ting said. "It can be used at a workstation, with a mobile tablet, or in a virtual desktop environment."

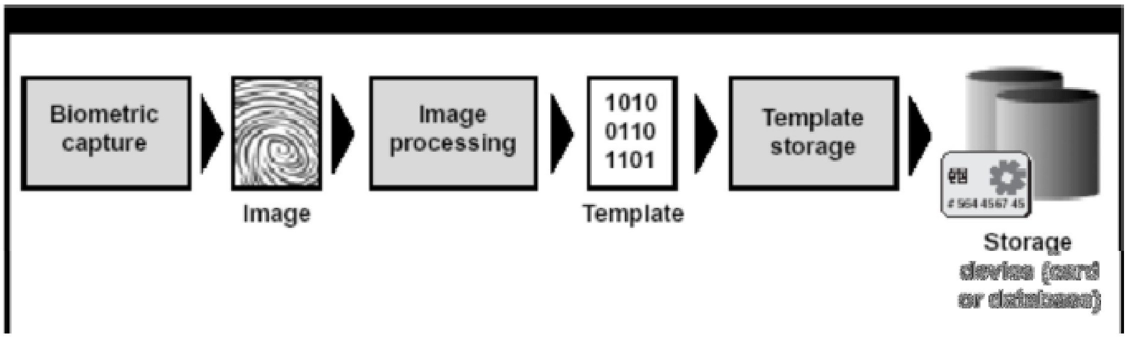

Fig.2 Enrolment Process

5. Fingerprint ID for Arizona radiologists

Radiology Ltd. in Tucson implemented Imprivata's OneSign authentication management system as a way to automate the launching of programs that radiologists use.

"The system has greatly reduced the problems associated with launching multiple customized programs, as well as remembering passwords," explained Ron Cornett, imaging informatics administrator. This large radiology practice operates nine imaging centers, in addition to providing radiology services at two hospitals.

Approximately 50 radiologists are enrolled in the system, which does not include technologists. The system enables the IT department to track users in a shared desktop environment, lock the workstation, and smoothly transition between users, Cornett said. The fingerprint identification system is also integrated with the hospitals' RIS and PACS.

"The Imprivata product uses a screen scrape-type technology and provides a graphical user interface that lets you train the software to recognize the login screens, fill them in, and manage them," he said. "Once a login has been learned, it can be deployed to policies, users, and groups."

6. Fingerprint ID for radiologic technologists

An effort to add radiologic technologists (RTs) to the fingerprint identification system failed at Radiology Ltd. The technologists shared workstations and logging on and off proved to be impractical [8].

Washington Radiology Associates (WRA), however, use the fingerprint identification system (DigitalPersona Pro, Digital Persona) it deployed in December 2010 exclusively for RT use. With seven imaging centers in the District of Columbia, Maryland, and Virginia performs more than 30,000 exams each month for residents of the greater metropolitan DC area, maintaining workflow efficiency was a high priority [7].

"The biometric solution has saved time for our technologists," Nguyen said. "It has eliminated the multiple logins required by our RIS for starting and ending patient exams. It has also eliminated password entry user error that we commonly saw. The technologists have adapted well and truly appreciate the convenience of this system."

Interestingly, radiologists do not use the fingerprint identification system. It was determined early on that with a single sign-on system already in place, it would not benefit the radiologists' daily clinical routine.

7. Proximity authentication

In 2010, Proxense markets its Prox Access proximity authentication and biometrics system for use by physicians, clinical staff, and administrative staff. Users wear an ID badge that activates and deactivates a workstation at a specified distance of 1 to 20 feet using radio frequency technology. The ID badge can also include an embedded fingerprint that must match one with a fingerprint scanner for an added layer of security.

8. Right Patient

Right Patient is a multi-modal biometric patient identity and medical data integrity platform for health care providers to prevent duplicate medical records, eliminate medical identity theft and health care fraud at the point of service, and raise patient safety levels. This unique, user-friendly solution is easy to install and seamlessly interfaces with existing electronic health record (EHR) systems such as Siemens, Meditech, McKesson, Cerner, Quadramed, CPSI, and more! Right Patient™ also supports fingerprint, finger vein, palm vein, iris, facial recognition, and voice depending on your needs to ensure high levels of patient ID accuracy. Both government and private hospitals can easily deploy this affordable international standard solution to ensure improved patient identification accuracy and high patient safety levels. Benefits of right patient include, Easy to set up and quickly enroll patients and Increases patient safety.

Features

- Multimodal biometric authentication (fingerprint, finger vein, palm vein, iris, facial recognition)
- Seamlessly interfaces with any EHR software
- High Speed Performance – 2.3 million iris templates/Sec, 1.7 million fingerprint templates/Sec, 600,000 finger vein templates/Sec, 60,000 palm vein templates/Sec

9. Bio Key

BIO-key’s technology is deployed in leading hospitals, clinics and private practices. Healthcare providers utilize BIO-key's fingerprint biometric technology to enhance security, increase convenience, and meet compliance requirements of the DEA and State Board of Pharmacy. Doctors, nurses and administrators use BIO-key to access EHR records and to provide compliant two-factor authentication for electronic prescribing of controlled substances. Additionally, our technology is used to provide secure access to thousands of medication dispensing cabinets in hospitals throughout the world.

BIO-key’s superior one-to-many matching capability allows any organization to enroll a health care provider, or patient and accurately recover their records without requiring any further form of identification. This is a revolutionary method to manage patient information, care and payments.

BIO-key technology achieves high accuracy through its patented Enhanced Image Technology; as more than 1,600 individual data points are extracted from each fingerprint. Our speed, efficacy and accuracy are independently tested and verified by NIST (National Institute of Standards and Technology), a division of the U.S. Dept. of Commerce. BIO-key is a consistent and frequent top-rated performer.

III. ISSUES

Table 1 shows the issues that have been addressed in the biometric health care industries [6].

TABLE 1
HEALTH CARE BIOMETRIC ISSUES

Author & year	Issue
Rogers 1995	Literature suggests that there is a difference in the adoption of technologies by different users. Some users readily adopt new technologies while others among them take time for the same
Perrin 2002	Biometric technology is the technology that offers the most comprehensive approach to ensure information security by replacing traditional security measures
Marohn 2006	Healthcare is a strongly regulated area that demands ensure the confidentiality and integrity of patient’s data
Win et al. 2006	Personal health care record (PHR) and electronic health record (EHR) systems through which patients can access their health information can be seen as today’s healthcare arena
Agrawal & Johnson 2007	Legislations and policies have been announced and implemented by HIPAA (Health Insurance Portability and Accountability Act) (
Lusignan et al. 2007	National Strategy for eHealth, Sweden (National strategy for e Health Sweden 2007) which requires the organizations to have mechanisms that ensure the highest level of security and protection for accessing, managing and exchanging of an individual’s data
Mordini&Ottolini, 2007	Identifying the patients with a high degree of confidence can be combined with complying to three basic requirements, 1) reducing medical errors; 2) reducing risks of fraud; 3) improving capacity to react to medical emergencies.
Wahlgren, 2010; Pehrsson, 2010	The recognition of individuals is performed with ID cards and passwords, issued by BlekingeCounty, Sweden. There have been problems reported that are associated with the passwords and ID cards. The identity thefts, health care fraud and misuse of sensitive health care information are not new words that one comes across today.

IV. OBJECTIVES OF PROPOSED WORK

The authors have reviewed the biometric health care systems in order to propose a new method for biometric health care system for unconscious state of humans. Health Care System has entered into the cloud. From that we particularly take the problem of Heart attack patients. If they went one place to another (or) suddenly they suffer / had a heart attack, they don't know what happens to do that time if nobody near with the patient. Someone took them into hospital and no details are retrieved from the patient regarding. If the patient is conscious (or) are they have the ID card means the information about the patient will be notified. If there is no information is available it will be the burden for all, especially for the doctors.

In this proposed system, the heart attack patient or unconscious patient doesn't keep any information with them. We simply make the system with patient fingerprint, face recognition and Iris match, from these they should identify the patient with the help of A**adhaar card** information and retrieve the information about the patient. **Aadhaar** is a 12-digit unique number which the Unique Identification Authority of India (UIDAI) will issue for all residents in India. But the thing is the A**adhaar card** also should have all the information about a person. They have to give provisions to the card with several options viz.,

a. Healthcare
b. Government Agencies
c. Banking Sectors
d. Travels
e. Tourist etc.,

All these options may also be included in the **Aadhaar card** while they are registered. This has to be updated with relevant agencies. If it means, Aadhaar card is not only act as a simple card for id proof, but also it has all the information of a particular person. 108 ambulances help the patient to reach the nearest hospital as well as doctors. Likewise, this software can be used to make treatment for the patient with their presence / absence.

V. CONCLUSION

Biometrics is the use of automated methods to recognize a person based on a physiological or behavioral characteristic. The use of biometrics is rapidly becoming the de-facto means of person authentication in healthcare because there is no other method more safe, secure, affordable, or efficient. In the healthcare industry, biometrics are replacing costly, inefficient, and jeopardous IDcard PIN, or password systems, and the facilities embracing it are realizing immediate benefits. Patient safety continues to be one of healthcare's most pressing challenges, although there are many angles from which patient safety can be addressed, the prevention of duplicate medical records and the elimination of medical identity theft stand out as two of the main culprits jeopardizing the integrity of the healthcare industry. This paper studied about the biometric healthcare system issues and some the techniques which are already in use. With the help of the proposed work, a new secured biometric health care system would be introduced in future.

REFERENCES

1. Henry T. F. Rhodes, Alphonse Bertillon, Father of Scientific Detection. Abelard-Schuman,New York,1956.
2. Jain AK, Ross A, Pankanti S, “Biometrics: A tool for information security”,IEEE Trans Inf Forensics Security, vol. 1, no. 2: 125-143, 2006.
3. Jain AK, Flynn PJ and Ross A (eds.) “Handbook of Biometrics”, Springer,2007.
4. Anil K. Jain, Ajay Kumar, “ ‘Second Generation Biometrics’ Biometrics of Next Generation: An Overview”, SPRINGER, 2010.
5. Darrell Shawl,“Biometrics – implementing into the healthcare industry increasesthe security for the doctors, nurses, and patients”, thesis for masters degree, davenport university, November 10, 2013.
6. Irfan Iqbal, Bilal Qadir, “Biometrics Technology - Attitudes & influencing factors when trying to adopt this technology in Blekinge healthcare”, Master Thesis ,Computer Science, April 2012.
7. “Smart Cards and Biometrics in Healthcare Identity Applications”,A Smart Card Alliance Healthcare Council Publication, Publication Number: HCC-12001, May 2012.
8. “Fingerprint Biometrics Help Secure Medical Data at Arizona Hospitals”, August 2011.