

A DESIGN OF A MULTIMODAL BIOMETRIC SYSTEM TO SECURE EHRs (USING IRIS & PALM VEIN)

¹Engr. Dr. Falohun A.S, ²Afolabi O.Z

Department of Computer Science and Engineering,

^{1,2}Ladoke Akintola University of Technology, Ogbomoso.

Email: ¹asfalohun@lautech.edu.ng, ²afolabizainab507@gmail.com

ABSTRACT

This paper presents a design of a multimodal biometric system to secure electronic health records (EHRs) using iris and palm vein recognition. Considering the beneficial contribution telemedicine has made in the field of basic medical sciences including the flexibility of activities for medical personnel and patients, it is however disheartening and almost unheard of that illegal data acquisition by unknown persons (data breach) is now the order of the day; using patients health and personal details to enhance fraud commission is an issue to be addressed in earnest. The designed system hopes to secure EHRs by capturing the iris and palm vein traits of patients and medical personnel, transferring the record to a system where these records are kept and programmed, to grant accesses to persons whose traits match with the ones on the templates, recording the time access was granted and refused in order to be able to control and monitor all those who gain and attempt accesses illegally. With this information which entails the recording of time accesses were granted / refused it is a lot easier to investigate data breach if at all there is any, given that the public is totally aware that their records are kept even when accesses are not granted.

1.0 Introduction

Telemedicine – the use of telecommunications technology to provide health care over a distance – was first documented in the late 1950's when a Nebraska psychiatrist connected to a prison over 150 miles away using closed circuit television to provide mental health services to the inmates(Wittson et al, 1961). Now the utilization of telecommunications technologies is practiced worldwide in virtually every specialty and is becoming more ubiquitous through use of consumer personal electronics (Whitten et al, 2001), (Grigsby, 1998), (Craig, Patterson , 2005). Over the years, there have been different terms utilized to describe this practice. The term *telehealth* was developed to include healthcare and specialties such as nursing, mental health and nutrition that do not always provide clinical services (McLendon, 2000). *Cybermedicine* and *e-health* are also commonly used terms, but typically describe health care delivered through the internet. Early forms of telemedicine achieved with telephone and radio have been supplemented with video telephony, advanced diagnostic methods supported by distributed client/server applications, and additionally with telemedical devices to support in-home care (Sachpazidis, 2008).

Telemedicine is the use of telecommunication and information technologies in order to provide clinical health care at a distance. It helps eliminate distance barriers and can improve access to medical services that would often not be consistently available in distant rural communities. It is also used to save lives in critical care and emergency situations (Sachpazidis, 2008).

Although there were distant precursors to telemedicine, it is essentially a product of 20th century telecommunication and information technologies. These technologies permit communications between patient and medical staff with both convenience and fidelity, as well as the transmission of medical, imaging and health informatics data from one site to another (Sachpazidis, 2008).

2.0 Categories of Telemedicine

In the past, telemedicine technologies have been separated into two categories: synchronous and asynchronous telecommunication solutions. However, current technologies are converging, allowing an application to be both interactive and real-time, while also storing data for future use and review. This section will highlight some of these telemedicine technologies and their uses.

2.1 Synchronous technologies

The first technologies utilized in telemedicine were synchronous, through a system of cameras and televisions; psychiatrist visits were performed in real-time spanning a geographic distance of over 100 miles. This type of consultation, which can use videoconferencing technology through mobile units, desktop units, or videophones, is still in regular use today and can also include the use of additional peripheral equipment to better enhance the medical care. Some examples of these peripherals include (tele) stethoscopes, (tele) dermoscopes, allowing the far-side physician to examine the patient effectively. Today one of the most popular applications for telemedicine through videoconferencing is telepsychiatry (Hilty et al, 2006). Some other examples of synchronous telemedicine applications include pediatric emergency consults diagnosis (Heath, Salerno, Hopkins et al, 2009) and treatment of strokes (Lerin, Forman, 1999) teledialysis and teledermatology (Whitten, Buis, 2008). This use of technology can potentially save the patient time and improve their access to care and quality of life. While synchronous technology is often what is imagined when thinking about telemedicine, there are also many applications that are asynchronous.

2.2 Asynchronous Technology

The use of asynchronous, or store-and-forward, technologies for health care is increasingly widespread, especially in image transfer and remote monitoring of chronic conditions (Pare et al, 2007). This type of technology allows the patient image (e.g., mammogram, MRI), data to be recorded at one point in time and viewed by a specialist or other health care provider at another time and location. Through technological advances, such as improved broadband infrastructure, high-definition viewing monitors, and high electronic storage capacities, the transfer of digital images is growing and changing the radiology field (Steinbrook, 2007).

A store-and-forward application that is growing in popularity is remote monitoring or home-telecare. This allows patients to upload specific health readings, such as blood pressure, weight, and glucose readings, from their home to their health care provider over a phone line or Internet connection (Field, Grigsby, 2002). Many remote monitoring systems can flag and alert health providers, caretakers, and patients if a reading is out of the patient's normal range (Crossley et al, 2008). Remote monitoring has had a significant impact on the hospital re-admittance rate, specifically emergency department admittance of patients with congestive heart failure (CHF) (Whitten et al, 2009). Remote monitoring of CHF patients can alert both the health care providers and individuals of an impending episode and prevent an emergency incident before it happens (Whitten, Mickus, 2007). As chronic diseases are becoming more prevalent, remote monitoring can provide an important platform for disease management and encourage prevention behaviors.

2.3 Recent Health Technologies

The current technologic solutions heading toward a hybrid of synchronous and asynchronous methods of delivering health care in the future. As many telecommunication applications are converging, it is becoming more difficult to have a strict definition of the types of technology. This paper hopes to broaden the view of telemedicine awareness, downsides and securing telemedicine data. A new trend many scientists are working on is the development and testing of types of wireless "smart" sensors for monitoring the health status of individuals. These sensors are non-invasive or minimally invasive and provide real-time monitoring of patient vitals, such as heart rate, blood pressure, falls, temperature, perspiration and blood glucose (Harasanyi, 2001). Some examples of these sensors include a "smart band-aid," digital pills, and clothing that is embedded with nano sensors (Topol, 2009). While these sensors may be shifting the way that health care is delivered, they first must be assessed for data accuracy and quality assurance. Sriram and colleagues (Sriram et al, 2008) suggest that there are three components that determine the complete accuracy and data quality of sensors: sensor factors, human factors and system architecture. Technology will continue to be an important tool for health care delivery, as past research has suggested that hospitals that are more "wired" have a better customer satisfaction rating (Whitten et al, 2008)

3.0 Downsides of Telemedicine

Just like every new and primitive technology, principles, propositions are characterized by benefits they also have certain drawbacks otherwise known as downsides; telemedicine is not left out. Though not an exhaustive list below are some telemedicine downsides:

- The cost of telecommunication, data management equipment and of technical personnel who will employ it (Hjelm, 2005).
- Potentially decreased interaction between medical experts and patients (Hjelm, 2005).
- An increased risk that protected health information may be compromised through electronic storage and transmission (Hjelm, 2005).
- Decreased time efficiency due to the difficulties of assessing and treating patients through virtual interactions such as; teledermatology consultation (Moffatt, 2011).
- Potentially poor quality of transmitted records such as images or patient progress reports (Strehle, Shabde, 2006).

- Decreased accesses to relevant clinical information are quality assurance risks that can compromise the quality and quantity reimbursement from insurer or government programs in some fields.
- Inability to start treatment immediately such as bacterial infection.

4.0 Awareness on Telemedicine Data Breach

The data breach at Community Health Systems that exposed the names, Social Security numbers and other personal details on more than 4.5 million people is a symptom of the chronic lack of attention to patient data security and privacy within the healthcare industry.

For more than 10 years, the Health Information Portability and Accountability Act (HIPAA) has required all entities handling healthcare data to implement controls for protecting the data, yet many organizations pay little more than glancing attention to the rules because of the relatively lax enforcement of the standards.

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services has begun cracking down recently on hospitals and other healthcare entities that have suffered security and privacy breaches. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 introduced some significant penalties for noncompliance with data security requirements.

Yet, many health organizations don't see data security as a major concern until a breach. So far this year, healthcare entities have reported to the HHS at least 150 incidents involving compromises of personal data.

"The industry has a long culture of not recognizing the incredible value of healthcare information," to those who want to misuse it, said Deborah Peel, a physician and founder of the advocacy group Patient Privacy Rights.

Apart from a lack of real enforcement of any of the privacy and security provisions in HIPAA, the industry has also suffered from the lack of an auditing requirement for security, Peel said.

HIPAA doesn't require even large healthcare organizations to submit to a third-party audit of their data security controls. "Only if you have a breach or someone reports you are you likely to come to the attention of HHS," Peel said.

Companies in other industries, such as financial services, have to go to great lengths to externally validate their systems and provide audit reports on request, she said. "There is no such requirement in healthcare," even though the information handled by the industry is highly sensitive and far more valuable in the underground market than financial data.

"There is a lot of catching up to do. A lot of public trust is going to be lost," before real change happens in the industry, Peel said.

Things will probably have to get worse before it starts getting better, said Phil Lieberman, president of Lieberman Software, a security vendor.

"It will take a Target type of episode where a healthcare provider and their C-suite face demise due to the damage they have caused to their entire population of patients to get some providers to wake up," and invest in real security, Lieberman said.

The unfortunate reality is that most healthcare providers have little concern for having IT security, he noted. "There is no incentive for them to invest, nor is there any material consequence for their failure to protect their infrastructure. HIPAA has had little to no effect in protecting patient data". (Jaikumar, 2014).

4.1 Extent of Data Breach

Given that stolen medical records can bring \$50 apiece on the underground market, the frequency and magnitude of data breaches involving electronic health records is increasing. In an effort to help CIOs and CSOs build a better business case for enhancing security, a group of standards and security organizations have issued a new report on the financial impact of such data breaches.

Protected health information (PHI) data breaches are growing in frequency and magnitude as the healthcare industry moves to adopt electronic health records (EHR), say a group of standards and security organizations. The healthcare industry must take action to better defend PHI if it wants to keep the public's trust, they say.

The Identity Theft Prevention and Identity Management Standards Panel (IDSP) of the American National Standards Institute (ANSI), in partnership with The Santa Fe Group/Shared Assessments Program Healthcare Working Group and the Internet Security Alliance (ISA), on Monday unveiled a report, *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security*, at a press conference kicked off by White House Cyber security Coordinator Howard A. Schmidt. The report is intended to help CIOs, CSOs and IT security, privacy and compliance staff creates a compelling business case for enhanced security to present to business executives.

"When it comes to cyber security, we all have a role whether we're a consumer, the executive of a company or a political leader," Schmidt says. "By working together, we can make sure we make the improvements that ensure the balance between privacy rights and security. While we can't solve all the problems in the world when it comes to cyber security and privacy, we can affect those parts we're responsible for."(Thor, 2012).

4.2 Privacy Protections Critical to Trust

Joe Bhatia, president and CEO of ANSI, added, "Privacy protections are absolutely critical to maintaining consumer trust in this information age. In the U.S., the healthcare delivery system is founded upon trust. This trust, as we all know, is now being severely tested."

According to the 67-page report, which involved a cross-section of more than 100 healthcare industry leaders from more than 70 organizations, nearly 39.5 million EHRs were breached between 2005 and 2008. In addition, within the past two years, the health

information privacy of nearly 18 million Americans-a number roughly comparable to the population of the state of Florida-was breached electronically.

The data points don't end there. Between September 2011 and November 2011, a government benefits program suffered the theft of EHRs of 4.9 million military personnel, the health information of 4 million patients of a reputable West Coast healthcare system were stolen electronically and a major academic medical center inadvertently disclosed the EHRs of 20,000 of its patients. In November of last year, Ponemon Institute completed a survey of 72 provider organizations and found that 96 percent of respondents reported at least one data breach in the past 24 months. On average, Ponemon Institute found that health organizations have experienced four data breach incidents over the past two years.

"Healthcare is one of the most-breached industries," says Dr. Larry Ponemon, chairman and founder of Ponemon Institute. "Healthcare providers and supporting organizations don't currently have sufficient security and privacy budgets, including adequate processes and resources, to protect sensitive patient data."

"The entire healthcare delivery system depends upon a single transaction: your willingness to share the most intimate details of your personal information with your physician," adds James C. Pyles, panel member and principal with Powers Pyles Sutter & Verville PC. "You have to trust that the information won't be used to harm you or your children. If you're dealing in this business of handling health information electronically or any information electronically, you're touching on a very tender nerve that people have."

Pyles added, "It's more than breaches, it also understands, as a business, the expectations of your customers. If you frustrate those expectations, I promise you, you will be sued."

Part of the problem, says Catherine Allen, chairman and CEO of The Santa Fe Group, is that the financial incentives are on the side of those who seek to steal medical records. Allen said medical records go for \$50 a record on the underground market, making them much more lucrative than even financial information. "It's very valuable data," she says. (Thor, 2012)

5.0 Extent of Work on Securing Telemedicine Data

The new report is intended to be a tool to help organizations quantify overall potential data breach costs and to provide a methodology for determining an appropriate level of investment needed to strengthen privacy and security programs and reduce the probability of a breach.

"No organization can afford to ignore the potential consequences of a data breach," says Rick Kam, president and co-founder of ID Experts and chair of the PHI Project. "We assembled this working group to drive a meaningful dialogue on appropriate levels of investment to better protect healthcare organizations and PHI."

He added, "One of the things that we realized as we started to work through this process is that the chief information officer, the chief security officer, they're essentially getting outgunned by the criminals. It's not that we don't have the technology or processes or

people to deal with this problem. It's that we don't have enough focus and investment from the executives."

The report provides a five-step method, the PHI Value Estimator (PHIve), for estimating breach costs and what needs to be done to protect organizations. The PHIve provides detailed information about each of the steps, which include: conducting a risk assessment, determining your security readiness score, assessing the relevance of a cost, determining the impact and calculating the total cost of a breach.

"Cyber security is not an IT issue," says Larry Clinton, president and CEO of the Internet Security Alliance. "It is an enterprise-wide risk management issue that needs to be addressed in a much broader sense." (Thor, 2012).

6.0 Proposed Security Schemes

- This scheme employs the use of a multimodal biometrically controlled system to enhance the security of Electronic Health Records (EHRs).
- This system stores a captured template of the iris and palm vein of all authorized persons to EHRs.
- The system is then programmed to ensure that biometric traits of persons wanting to access EHRs are verified before access is granted; it further stores the time, date and identity of the user electronically, it also captures the traits of all users including unauthorized ones who attempt to access records so that they can be investigated and brought to book if found guilty.
- The design of this system is inspired by the theory and elements of a relatively new concept known as Situational Crime Prevention (SCP); this theory is based on rational choice, its elements are increasing the perceived difficulty of crime, increasing the risks, and reducing the rewards.
- According to a Philadelphia survey of the efficiency of the use of SCP in the design of Advanced Traffic Enforcement Systems(ATES) which captures information of road users who run red lights and similar traffic offences, including the time of the crime commission, a 96% compliance was recorded putting into consideration that awareness creation was made before hand.

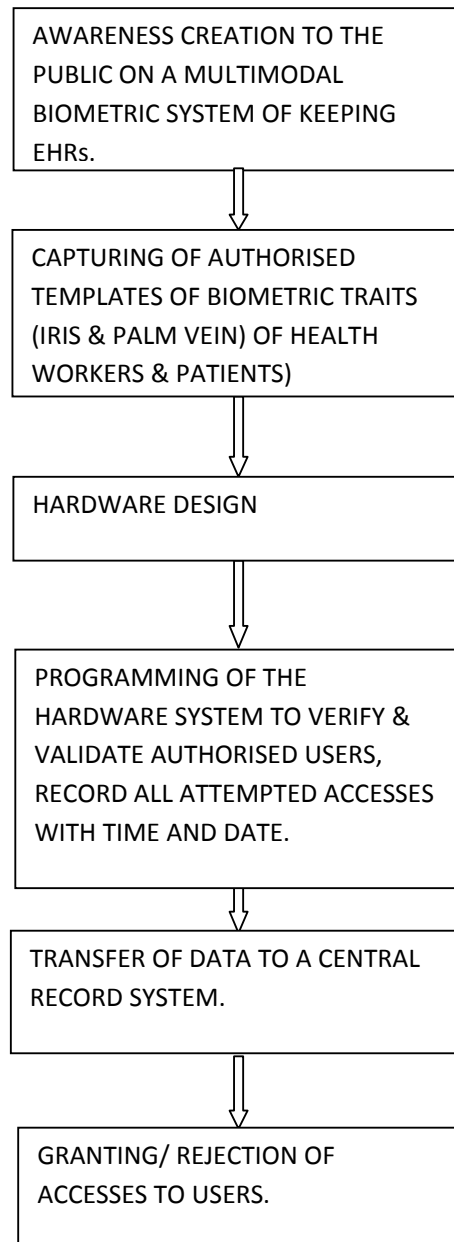


Fig 1

Design of a multimodal biometrically controlled system to secure EHRs

REFERENCES

1. Sachpazidis, Ilias (2008). *Image and Medical Data Communication Protocols for Telemedicine and Teleradiology (dissertation)*. Darmstadt, Germany: Department of Computer Science, Technical University of Darmstadt.
2. . Wittson, Affleck, Johnson .Two-way television in group therapy. *Mental Hospitals*. 1961; 12(10): 22-23 [PubMed]
3. Whitten, Goolittle, Hellmich. Telehospice: Using telecommunication technology for terminally ill patients. *JCMC* [Internet] 2001. Jul [cited 2010 Feb 6]; 6(4). Available from <http://jcmc.indiana.edu/vol6/issue4/whitten2.html>
4. Grigsby. Telemedicine: Where it is and where it's going. *Annals of Internal Medicine* 1998; 129(2): 123-127 [PubMed]
5. Craig, Patterson .Introduction to the practice of telemedicine. *Journal of Telemedicine and Telecare* 2005; 11: 3-9 [PubMed]
6. McLendon. E-commerce and HIM: Ready or not, here it comes. *Journal of the American Health Information Management Association* 2000; 71(1): 22-23 [PubMed]
7. Maheu, Whitten, Allen, editors. , editorsE-health, telehealth, and telemedicine: A guide to start-up and success. Jossey-Bass; 2001
8. Hilty, Yellowles, Cobb, Bourgeois, Nuefeld, Nesbitt. Models of telepsychiatric consultation – Liaison service to rural primary care. *Psychosomatics* 2006; 47: 152-157 [PubMed]
9. Heath, Salerno, Hopkins, et al. Telemedicine for pediatric critical care consultation. *Pediatr Crit Care Med* 2009; 10(5): Epub 2009; doi:10.1097/PCC.0b013e3181a63eac [PubMed]
10. Levine, Forman. "Telestroke": The application of telemedicine for stroke. *Stroke* 1999; 30: 464-469 [PubMed]
11. Whitten, Buis. Use of telemedicine for haemodialysis: perceptions of patients and health-care providers, and clinical effects. *J Telemed Telecare* 2008; 14: 75-78 [PubMed]
12. Burdick. Teledermatology: Extending specialty care beyond borders. *Archives of Dermatology* 2007; 143(12): 1581-1582
13. Pare, Jaana, Sicotte. Systematic review of home telemonitoring for chronic diseases: The evidence base. *Journal of the American Medical Informatics Association* 2007; 14(3): 269-277 [PMC free article][PubMed]
14. Steinbrook. The age of teleradiology. *The New England Journal of Medicine* 2007; 357: 5-7 [PubMed]
15. Field, Grigsby. Telemedicine and remote patient monitoring. *JAMA* 2002; 288: 423-425 [PubMed]
16. Crossley, Boyle, Vitense, Sherfesse, Hardwin Mead.Trial design of the clinical evaluation of remote notification to reduce time to clinical decision: The clinical evaluation of remote notification to reduce time to clinical decision (CONNECT) study. *American Heart Journal* 2008; 156(5): 840-846 [PubMed]
17. Whitten, Bergman, Meese, Bridwell, Jule.St. Vincent's home telehealth for congestive heart failure patients. *Telemedicine and e-Health* 2009; 15(2): 148-153 [PubMed]
18. Whitten, Mickus. Home telecare for COPD/CHF patients: Outcomes and perceptions. *Journal of Telemedicine and Telecare* 2007; 13: 69-73 [PubMed]

19. Harasanyi; Sensors in biomedical application: May they change the quality of life. *Sensor Review* 2001; 21(4): 259-267
20. Topol. The new healthcare: Smart band aids, digital pills, wrist bands. 2009. [cited 2009]; Venture Beat. Available from: <http://venturebeat.com/2009/09/20/the-new-healthcare-smart-band-aids-digital-pills-wrist-bands-promise-to-track-your-health/>
21. Sriram Kotz Rahan Sastry Yarvis .Challenges in data quality assurance in pervasive health monitoring systems. Paper presented at the Future of Trust In Computing conference; June/July2008; Berlin, Germany
22. Whitten, Mylod, Gavran, Sypher.“Most Wired Hospitals” rate patient satisfaction. *Communications of the ACM* 2008; 51(4): 96-102
23. Håkansson, Gaveline. What do we really know about the cost effectiveness of telemedicine. *Journal of Telemedicine and Telecare* 2000; 6(Suppl. 1): 133-136 [PubMed]
24. Hjelm, (2005). *Benefits and drawbacks of telemedicine*. "Journal of Telemedicine and Telecare". *Journal of Telemedicine and Telecare* **11** (2): 60–70. doi:10.1258/1357633053499886. PMID 15829049.
25. Moffatt (2011). "Barriers to the up-take of telemedicine in Australia – a view from providers". *The University of Queensland, School of Medicine*.
26. Strehle, Shabde (2006). "One hundred years of telemedicine: does this new technology have a place in paediatrics?". *Arch. Dis. Child.* **91** (12): 956–9. doi:10.1136/adc.2006.099622. PMC 2082971. PMID 17119071.
27. Jaikumar (2014). "Health care Organisations Still too Lax on Security". Originally by Computer World.
28. Thor (March, 2012).