Master Thesis
Computer Science
April 2012

Biometrics Technology - Attitudes & influencing factors when trying to adopt this technology in Blekinge healthcare

Irfan Iqbal & Bilal Qadir

School of Computing
Blekinge Institute of Technology
SE – 371 79 Karlskrona
Sweden

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Authors:
Irfan Iqbal
Email : lineofaxis@gmail.com
Bilal Qadir
E-mail:ms24pk@gmail.com

University advisor:
Professor Sara Eriksén
School of Computing. Karlskrona

School of Computing
Blekinge Institute of Technology
SE – 371 79 Karlskrona
Sweden

Abstract:

Context. 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.

Objective. The aim of this research is to explore and clarify the main influencing factors and attitudes concerning biometrics Security technology by analyzing expert opinions. This is done through informal interviews and a web based survey in Blekinge healthcare.

Methods. Literature review was the starting phase to map the current state of research in biometric technology implementation. The literature review helped authors to explore and solve different ambiguities in authors' minds, related to work flow, methods and procedures for different tasks. In our research, we selected five different interviewees from biometric solution supplier companies in Sweden and Denmark, Blekinge healthcare staff, biometric technology technical staff and IT security concerned to express their experiences, opinions and domain knowledge about the implementation of biometrics system in the county of Blekinge. Due to the resource and limited time constraint authors selected survey as a data collection procedure. In survey we planned a questionnaire with the different people related to healthcare. The questionnaire purpose was to collect the quantitative data and our questionnaire was relying on close ended questions.

Results. It is analyzed that people have trust on biometrics system and in future they are agreed to face changing in the current system as well as the people who are related with healthcare system are already aware about biometrics and they will easily adopt the implementation of biometric system in healthcare.

Conclusion. In concern of user acceptance it is analyzed that people have trust on biometrics system and in future they are agreed to face changing in the current system. In concern of implementation authors analyzed that it is very necessary to conduct a study in order to analyze the requirement of different actors that will participate in biometrics systems. In concern of cost Authors observed that for cost benefit advantage in the initial implementation stages the finger print technology could be a better selection as compared to other available biometric technologies. In concern of security there are strong reasons that biometrics could be implemented because there are many secure authentication devices related to biometrics are available in the market that could secure data in best possible way. Authors observed that there is a need of legislations for biometrics as the security measures going to be much higher as compared to the traditional password systems. In concern of privacy authors observed that the organizations are demanding strong authentication and focus on suggesting biometrics because it could provide advantages to patients, healthcare staff and healthcare providers.

Keywords: Biometrics Technology, Attitudes & influencing factors, Blekinge healthcare.

ACKNOWLEDGMENTS

In the name of Allah Almighty who is the most Gracious, Merciful and Creator of the universe. We are grateful to Allah who blessed us with abilities, strength and courage to accomplish this thesis work on time.

Our thanks and sincere appreciation goes to Professor *Sara Eriksén*, the finest teacher and mentor we could possibly want. *Sara Eriksén* provided continuous encouragement, strategic thinking and goal focus throughout my thesis work.

Our special thanks goes to Søren K. Lauritzen (Business Manager/Partner IT2TRUST A/S, DENMARK), Karin Sveheim(Director Markets Precise Biometrics SWEDEN) & Birgitta Billinger Lundberg (Chef Blekinge kompetenscentrum Landstinget Blekinge Karlskrona) for helping and guiding us a lot during our thesis work. It was really difficult to conduct interviews with out their guidance and continuous help. We are also thankful to Babak Goudarzi Pour(Chairman Swedish National Biometric Association, SNBA) for his motivation and help for conducting interviews especially Biometric Solutions Supplier.

We would like say special thanks to all our friends who guided us a lot during research work. A warm and special appreciation goes to Farrukh Sahar for encouragement during the time and really thankful to our families for their kind support, encouragement and prayers. Indeed, without their prayers, it was difficult to make it happen.

Contents

Table of Figures

Table of Tables

1 INTRODUCTION AND BACKGROUND

1.1 Introduction

Biometric technology has been gradually taken initiation and being introduced to secure and restrict access to medical facilities, protect and manage confidential information, reduce fraud by identifying patients and staff in healthcare programs (Marohn 2006). For both patients and healthcare providers, biometrics is now rapidly becoming known as present instead of future of healthcare. Biometrics measure individual's unique physical and behavioral characteristics to identify or authenticate their identity (Faundez-Zanuy 2006), is already being adopted and being viewed for managing access to healthcare information systems, preventing unauthorized use to system's resources and to ensure the security of patient records. Common physical biometrics include fingerprints; hand or palm geometry, retina, iris, or facial characteristics. Behavioral characters include signature and voice (which also has a physical component) (Faundez-Zanuy 2006).

Jain et al. (2004) argue that any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: every person should have the characteristics.
- Distinctiveness: people must be sufficiently different in terms of characteristic.
- Permanence: the characteristic should be sufficiently constant (with respect to the matching criterion) over a period of time.
- Collectability: the characteristic can be calculated quantitatively.(Jain et al. 2004)

The process of resolving a person's identity involves two phases: identification and verification (also known as authentication). Identification is provided and after that it is verified during the process of authentication (Trocchia & Ainscough 2006). Basically there are three individual's identity approaches for verification: something you have (e.g. Debit Card), something you know (e.g. password, PIN) and something you are (e.g. fingerprint), which is unique and cannot be shared (Bolle et al. 2004). Biometrics offer a number of advantages over traditional authentication techniques. There is no password for the user to remember and no identification card to lose (Trocchia & Ainscough 2006).

Currently, biometric is used for identification or confirmation of a person's identity. In identification methods, a subject identity is determined based on the comparison of a biometric sample obtained from the subject earlier and stored in a database. Authentication methods are used for the confirmation of an individual's claimed identity; in this case the comparison is made only with the stored biometric features that correspond to the claimed identity (Stamp 2006). Authentication based on the biometric is used to restrict access to sensitive information, equipment and restricted areas(Schneier 2001).

The Security may be guaranteed by how many roadblocks you put in against imposters and how extensive the roadblocks are to get over. Biometrics is an additional roadblock for any intruder(Keener 2000) because a biometric is the most secure and convenient authentication tool (Faundez-Zanuy 2006), especially in a hospital environment that involves complex security and patient data privacy and access related issues that need to be addressed through compact security techniques. Biometrics has not yet made a huge impact in the worldwide healthcare industry. But due to the increasing pressure on healthcare providers for cutting fraud, improving physical and digital security and reducing cost, the technology is now taking a firm place on the industry's agenda (Atkins 2000).

Concerning applications for healthcare, biometrics can overcome fraud and abuse by protecting and helping in the management of confidential medical records, identifying the patients and securing medical facilities and equipment. Although there has been a lot of recent advancements and apprehensions for increasing security, biometrics authentication still remains to be implemented in a large scale especially in healthcare (Chandra et al. 2008). Despite growing adoption and the several prevention possibilities, to date there has been surprisingly little empirical research on factors influencing the adoption of biometric technology by Healthcare organizations. The objective of this thesis is to explore and gain a better understanding of factors that are significant in explaining the intension to adopt biometrics in healthcare. This is done through a survey study carried out during 2009 and 2010, with a focus on the healthcare organization in Blekinge County, Sweden.

1.2 Background

In 2003, Richardson published a survey that showed that computer security incidents had grown exponentially since 1997, and about 90% of all major organizations are affected by them each year (Richardson 2003). Concerning security, biometrics refers to the authentication techniques that rely on measuring physical and behavioral characteristics (Faundez-Zanuy 2006). This thesis addresses issues of adoption and deployment of biometrics for security, privacy and cost. Biometrics technology is a rapidly growing area of research within computer science.

Regarding the related research work, it seems to indicate that these influencing key factors are emphasized and have been discussed by various researchers and analyzed with the help of different features and surveys by different biometrics companies.

Krawczvk & Jain (2005) explained that security of medical records is becoming a serious problem for the existing medical services as in healthcare sector especially in dealing with electronic medical records when health professional manipulate the data to edit and view patient's record. In order to protect the patient's privacy as per the government regulations, biometric based secure authentication system is proposed and will be capable for providing the necessary security. (Krawczyk & Jain 2005)

In a survey conducted on biometrics in healthcare in the US, Marohn (2006) spotlights the growing use of biometrics in healthcare applications to prevent fraud and abuse. An estimation of at least US$51 billion, or 3% of the nation's annual health care outlay in year 2003 was lost to outright fraud according to the National Health Care Anti-Fraud Association (NHCAA). Various law enforcement government agencies believe the loss could be potentially US$170 billion or 10% of USA's annual expenditure, each year. Marohn suggests that biometrics can ensure the confidentially of medical records through healthcare provider authentication and thus greatly reduce such costs.(Marohn 2006)

The survey conducted by the Card Technology Today in 2008 on Beefing up Security with biometrics indicates that card schemes are now shifting towards further level of security in both private and public organizations. Private organizations have mostly taken initiative but for public sector that demands high security for multiple factors in different application areas like national ID, ePassport and healthcare are being driven largely by International Civil Aviation Organization (ICAO). (2008)

Information systems demand security on individual and network level to access the applications to avoid security problems and liability associated with security breaches. Similarly healthcare organizations must be able to minimize the security risks with individual authentication for access control and ensure data privacy and to maintain data integrity. Biometrics technology offers a comprehensive authentication approach to ensure information security with a strong argument of replacing traditional security measures.(Perrin 2002)

According to Perrin, 'Of course, cost is a key consideration when adopting biometrics-based security systems. For the lower cost systems, such as fingerprint identification for individual workstations, healthcare organizations can expect to spend about 50$ to 100$ per workstation to install biometrics devices and accompanying software. High end systems, such as physical access security to labortories or computer facilities using iris or face and voice recognition systems in a network envirnment, can cost from 150$ to 200$ per access cost.' (Perrin 2002, p.87)

According to Peck (2003), measures need to be taken to secure the patient records and hospital data network in a healthcare industry, where minutes make the difference between life and death, According to the Bruce Peck, Information Security Manager at St.Vincent Hospitals and healthcare center Indianapolis, biometric authentication is a strong solution to meet the objective of making the hospital's computer network more user-friendly for physicians. At the same time, it offers immediate return on investment through higher productivity and lower IT costs because according to the industry analysts IDC, password management costs between $200 and $300 per user per year. Additionally market analysts in Giga Information Group in 2001 found 30 percent of IT help desk cost related to the password management.(Peck 2003)

Win et al. (2006) explains that personal health information security has been emergent in healthcare. Personal health record systems and electronic health record systems allow patients to access their information but this information needs to be secured. Although there are legislations and policies in place in different countries to protect this information privacy, still there is a gap that needs to be addressed with strong security protection mechanism to address and to enhance the protection of personal health information. Different user authentication mechanisms are introduced including biometric scans (fingerprint, face, hand, and retina). (Win et al. 2006)

Marketing manager at API (automating peripherals), Hagen in 2003 at US presents survey results showing that 93% respondents thought that more needed to be done about the authorized access in certain areas of hospital. About 57% were in favor of implementing the biometric technology for restricting access, while 33% thought that hospital pharmacies were a critical area where biometric should be used for access restriction.(Hagen 2003)

In scenarios where provision of care services is shared among multiple actors could be complex and costly in context of securing electronic health records. It involves correct identification of patients, staff and physicians, ensuring the privacy and confidentiality, setting access permissions for healthcare providers and conflict resolution in development of interconnected health information network. A proposed technological solution for all of these issues is biometric technologies due to the ability for unique identification of individuals. In addition, biometric technologies appear to offer several benefits over traditional methods of identification; however work is still in progress for providing a suitable solution for healthcare environment.(Zuniga et al. 2009)

According to Dwivedi et al. (2003), a number of countries are introducing plans for electronic patient record (EPR) systems so that patients and healthcare stakeholders can access the medical records through internet based EPR systems. The author argues that the weak robustness of current healthcare information security is the main obstacle for successful implementing of the EPR concept. Biometrics is considered to be the main information security technology for contribution in proposing multilayered healthcare Information security (HIS) framework in combination with other technologies like smartcard.(Dwivedi et al. 2003)

The survey titled "HIPAA creates healthy opportunity for biometrics" by Richard Norton at the IBIA in USA gave details that the US Department of Health and Human Services released HIPPA (Health Insurance Portability and Accountability Act of 1998) regulations went that into affect on 28 December 2000 was designed to protect medical records and other personal health information kept by healthcare

providers, hospitals, insurers and healthcare clearing houses. According to the International Biometric Industry Association, the challenge is to explain and demonstrate to potential end users, how biometrics can secure the medical information and make compliance with the requirements of the American healthcare system. (Norton 2001)

Chandra et al. (2008) explores utilization, attitudes and concerns of healthcare consumers and providers about biometrics and observes that privacy and need for information protection were identifiable as shared concerns among providers and consumers. With only weak to modest differences among them, physicians, nurses, health professionals and consumers were alike in their expressed thoughts about biometrics as a potential invasion of privacy and about the need for limitation of information availability.(Chandra et al. 2008)

The author talks about the issue about medical identity theft and summarize how it can harm its victims in US. One of the significant harms is false entry to her or his medical history that is caused by the activities of imposters. Incorrect information in health records leads to a number of negative consequences for victims that don't have any help for recovery from medical identity theft. According to the report statistics in healthcare and identity theft, it is estimated that quarter million to a half million individuals have been victims of this crime. The report also explains the reasons why identity theft is challenging to detect. (Dixon 2006)

Biometrics is considered to be capable of both threatening and increasing individual's information privacy (Shen et al. 1997).

According to Forte, there is clearly a high privacy risk concerning biometric solutions (Forte 2003). Since biometrics works with personal data, there are concerns regarding the legal point of view of privacy and personal data protection (Donos & Zorkadis 2004). With biometric systems there might become a privacy protection problem if a third party gets their hands on the databases holding the biometric data (Donos & Zorkadis 2004). For example, if government authorities would use a fingerprint database for their own processing desires (Donos & Zorkadis 2004).

1.3 Problem Area

Healthcare is a strongly regulated area that demands to ensure the confidentiality and integrity of patient's data (Marohn 2006). Within healthcare, information systems need security at all levels including individual physical or network access to applications so in this way, information security of personal health information has been a growing concern in the healthcare sector. Personal healthcare record (PHR) and electronic health record (EHR) systems through which patients can access their health information can be seen as today's healthcare arena (Win et al. 2006). Legislations and policies have been announced and implemented by HIPAA (Health Insurance Portability and Accountability Act)(Agrawal & Johnson 2007), European Data Protection Directive (Lusignan et al. 2007) and 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 individual's data. A comprehensive information system requires security with an individual authentication for controlling access that ensures data privacy and maintains data integrity. According to Perrin (2002), Biometric technology is the technology that offers the most comprehensive approach to ensure information security by replacing traditional security measures (Perrin 2002).

The healthcare sector is today second to the financial sector regarding the number of biometric users in US as the report issued by the European Joint Research Centre. 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. Biometric security

technology is being deployed in many healthcare organizations and hospitals because of its secure identification property that can be used for controlling access of digitized patient's record and limiting access to building and hospital wards, and to authenticate medical and other personnel. However the risk of revealing health information due to biometric authentication devices requires further ethical and political scrutiny.(Mordini & Ottolini 2007)

In the survey titled "The end of a decade", If the biometrics industry is reviewed back in 1999, there were three dominant application areas like time and attendance (42%), computing (25%) and financial industry (15%). After the terrorist attacks of 11 September 2001, US government and other leading nations pledged to invest in security and counter-terrorism. This creates an interest in biometrics to many companies to promote this technology. After that many countries believed to get start producing or planning the rollout of ePassport technology. Within short span of time, it became important component in large scale security and ID implementation. Biometric technology is expected to gain momentum in healthcare applications in European countries in next three years.(The end of decade 2010)

Blekinge health care system provides health care services to the citizens of Blekinge County Sweden. According to (Wahlgren, 2010; Pehrsson, 2010) the recognition of individuals is performed with ID cards and passwords, issued by Blekinge county, 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. All those and other such problems could be minimized by covering the weaknesses associated with the conventional authentication schemes i.e. passwords and cards. Interesting is the fact that biometrics, despite having vital strengths and advantages as compared to other methods, has not got its full appreciation and acceptance from people around the world in the healthcare sector.

Literature suggests that there is a difference in adoption of technologies by different users (Rogers 1995). Some users readily adopt new technologies while others among them take time for the same (Rogers 1995). While there exist some positive factors influencing the use of biometric technology in terms of safety and security, there are also some perceived possible negative factors (e.g.: privacy, inconvenience, etc.) that are causing concerns to users in terms of their acceptance of these technologies. This study will attempt to assess factors like privacy, security and cost related to the adoption of biometric technology using Blekinge healthcare system as an example. The two main stakeholder groups we have been in contact with are biometrics system provider and potential system users on a managerial level within the Blekinge healthcare system.

1.4 Research Questions

Our basic hypothesis is that biometric technology is viable, secure and cost efficient way of addressing safety, security and privacy issues in the healthcare sector. This is a provider biased perspective which we will be testing in our study.

RQ#1. What are the major reasons that biometric technology has had difficulties to breakthrough in healthcare industry?

- RQ1 will address the major reasons for the slow deployment of biometric technology in healthcare industry. Mainly privacy, security, and cost issues will be explored. RQ1 will further help to better perform analysis for RQ2.

RQ#2. What are the attitudes towards biometrics among management towards security, privacy and cost of biometric technology in Blekinge healthcare?

- RQ2 will help to identify the understanding of management and the ordinary users like hospital employees and hospital user like patients, concerning privacy, security and cost issues for deployment of biometric technology in Blekinge healthcare.

RQ#3. How might attitudes and concerns influence the deployment of biometric technology in major security applications of Blekinge healthcare system?

- Depending upon the information gained regarding RQ1 and RQ2, suggestions in form of analysis will be provided for the deployment of biometric technology in Blekinge healthcare.

1.5 Aims and Objectives

The main aim is to explore and clarify the main reasons, influencing factors and attitudes concerning biometrics security technology by analyzing expert opinions.

There are certain objectives set by the authors

- Analysis of the biometric technology and its functional characteristics.
- Exploring implementation importance of biometric technology in healthcare.
- Mapping and analysis of main factors influencing the adoption of biometric in healthcare concerning privacy, security and cost.
- What are the attitudes that need to be addressed on individual and organizational level in Blekinge healthcare system if biometric technology is to be implemented?
- What aspects need to be addressed for suggesting biometric security solutions on user and healthcare organizational level in Blekinge healthcare system?

1.6 Expected Outcome

Expected outcome of our study is a report mapping obstacles for deployment and adoption of biometrics technology in healthcare. Through this study, the mentioned factors cost, privacy and security are explored as potential obstacles and ways to address these factors are suggested. Through using survey together with interviews as a way of mapping attitudes towards biometrics in healthcare, authors expect to achieve a richer understanding of attitudes and influencing factors in this area.

2 RESEARCH METHODOLOGY

Qualitative (Hazzan et al. 2006; Seaman 1999), quantitative and mixed methodologies (Creswell 2009) are different types of methodologies for research work. We have chosen the qualitative research methodology for our research work. The main intent behind choosing qualitative research methodology is that our research work is explorative and involves certain phenomena that involve humans (Hazzan et al. 2006). Explorative approach is necessary because we are focusing on adoption of biometrics and obstacles to this, which has not been extensively explored in research on biometric technology so far. For comprehensive overview of our chosen research methodology, see diagram in figure 1.

2.1 Literature Review

Literature review was the starting phase to learn the current state of research in biometric technology implementation. The literature review helped us to explore and solve different ambiguities in authors' minds, related to survey work flow, interview methods and procedures for biometric technology deployment research. Authors used different key search terms relevant to biometric technologies to search published material. The main purpose of the literature review was to provide a proper context for our study based on previous research s from the previous research work done by other researchers. (Dawson 2005) Blekinge Institute of Technology (BTH) Electronic Library Information Navigator (ELIN) was used as net surfing tool to search the data related to biometric technologies. The authors selected research papers, journals and online documents related to biometric technologies and implementation issues from ACM, IEEE, Master thesis reports, biometric technologies reports and Ph.D thesis reports. The literature review process guided the authors to learn the biometric system and its functioning. The literature review also identified important factors for further research.

2.2 Interview

Seaman (1999) explains that interview is one of the techniques that can be used for collecting qualitative data. It is an indirect method because it does not evaluate the biometric services directly through the implemented biometric system. However, we chose this method because our aim is to identify the attitudes and factors influencing adoption/deployment of biometrics.

In our research, we selected five interviewees from biometric companies to express their experiences, opinions and domain knowledge about the implementation of biometrics system, with a special focus on the healthcare system in the county of Blekinge. According to Nielsen (1993), interviews require more time as compared to other data collection techniques but being more flexible, it provides opportunity to interviewers to identify and explain the difficult questions in more depth in order to develop the understanding of interviewee and thus get more in depth and relevant answers.

Interview questions were based on the strategy to gain a deep understanding about company‘s point of view about biometrics and to identify their opinions about why the healthcare sector is not ready to invest in biometrics technology. The main purpose of the interviews is to identify attitudes and factors influencing adoption/deployment of biometrics technology in the healthcare system of the county of Blekinge. During interviews new dimensions were opened that helped us to improve the quality of this study.

In interviews authors added formal and informal questions to identify factors influencing adoption/deployment of biometrics technology in the county of Blekinge. In formal approach, authors designed some set of pre-planned questions to explore the factors influencing adoption/deployment of biometrics technology in the healthcare system of county of Blekinge. In informal approach, the questions

were framed during the discussion based on the reply of the interviewees. In interviews we recorded, observed and noted important factors influencing the adoption/deployment of biometrics technology in the healthcare system of the county of Blekinge. Interviews were conducted in three different ways; email interviews, telephone interviews and live interviews.

2.3 Survey

A survey is a strategy for inquiry and is used as a quantitative research method which provides a numerical description of the opinions, attitudes, and trends of a target population. In survey researchers select samples of population and then generalize the results for whole population (Creswell 2009). Surveys are widely accepted for data collection. Moreover survey is inexpensive to design and it gives rapid turnaround in data collection (Creswell 2009). Due to time constraint, we selected survey as a data collection procedure. For data collection there are different forms of survey available. For data collection the survey may be in oral, written or electronic form. Other forms of data collection are self- administered questionnaires, structured record reviews, structured observations and interviews (Nielsen 1993). We used an online software surveygizmo (McDaniel n.d.) to create a web based survey. We designed a webpage for own questionnaire and administered it online. Online survey is helpful both for administrators and respondents due to its convenience, availability and low cost. We also sent survey MSWord document to some respondents. The survey was conducted with healthcare staff as focus group because the focus group was directly connected with the Blekinge healthcare system.

2.3.1 Questionnaire

In survey the questionnaire is a reasonable way to gather data. A well-designed questionnaire can be utilized effectively to collect information of specific research area. The questionnaire (survey) was conducted with eight different people related to healthcare like physical therapist, project-coordinator, clinical and research administration in different divisions of the healthcare organization of the county of Blekinge. The questionnaire purpose was to collect quantitative data to measure the adoption/implementation of biometric technology in Blekinge healthcare system. Our questionnaire was heavily relying on closed ended questions. For a successful conduction of questionnaire we sent survey questionnaires to people who are closely related to healthcare systems. In questionnaire, the questions concerned privacy, security cost, and user satisfaction issues related to biometrics technology implementation from the perspective of people working within healthcare systems. Once the questionnaires were completed then statistical analysis was performed to analyze the end results of questionnaires.

On the other hand to explore individual‘s opinions about biometrics, questionnaire could be an appropriate way. We decided to combine these methods. Through questionnaires, we can evaluate opinions about ease of use, accuracy, cost, user acceptance, required security level and long term stability that can help for decision and compare all of these with what the companies say and sketch meaningful conclusions.

The purpose was to map attitudes and explore experiences in the area of study. This helped to gather appropriate material for further analysis.

2.4 Triangulation

Triangulation is sometimes used to refer to all instances in which two or more research methods are engaged. Thus, it might be used to refer to multimethod research in which qualitative and quantitative research method are combined to provide a more complete set of findings than could be achieved at

through the administration of one of the methods alone. However, it can be argued that there are good reasons for reserving the term for those specific occasions in which researchers wants to check the validity of their findings by cross-checking them with another method.(Bryman, Triangulation)

2.4.1 Methodological triangulation

Authors adopted Methodological triangulation, which refers to the use of more than one method for gathering data (Bryman, Triangulation). Authors used survey together with interviews as a way of mapping attitudes towards biometrics in healthcare.

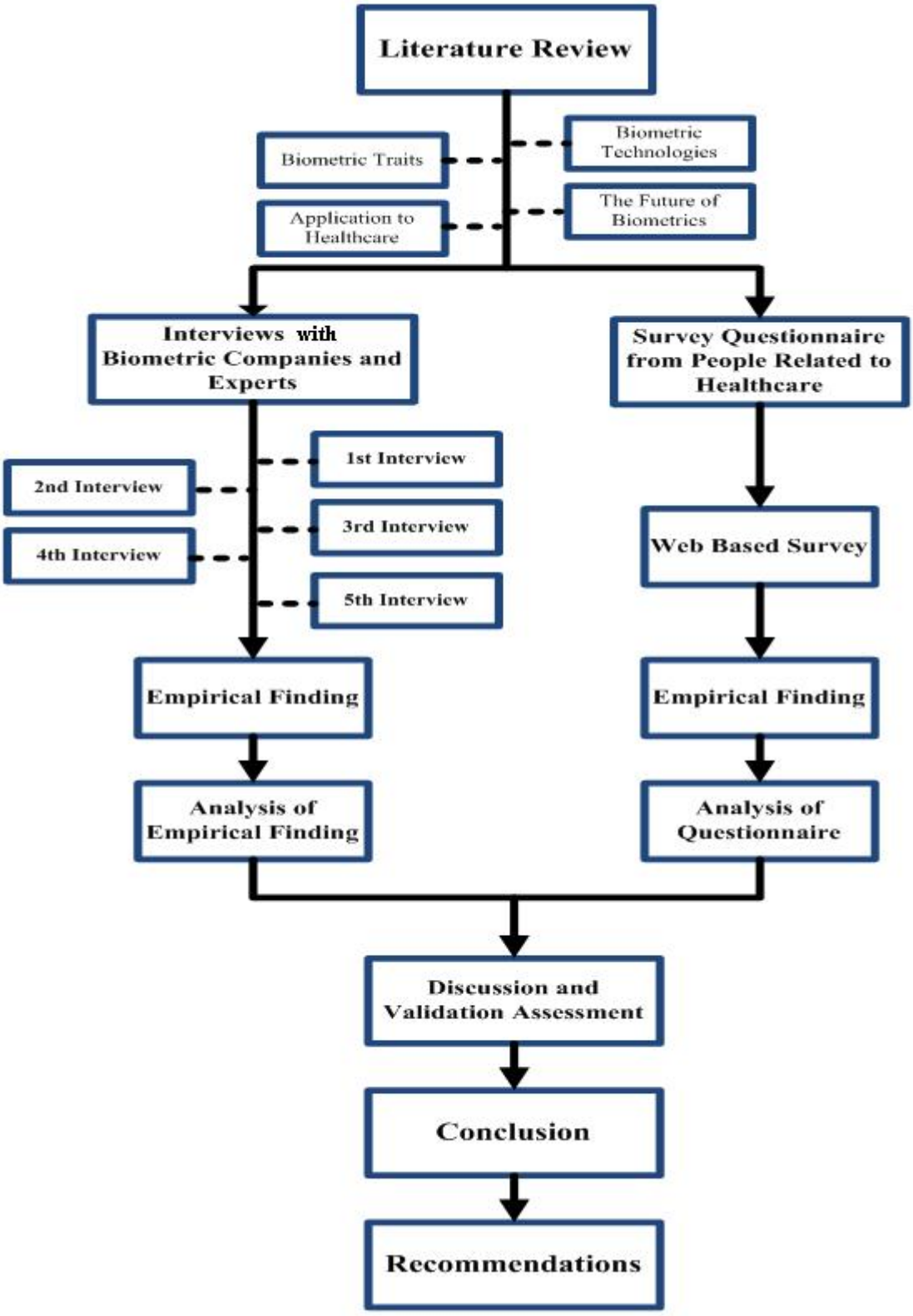


Figure 1-Research Methodology Diagram

3 LITERATURE REVIEW

3.1 Biometrics

With the rising concerns for security, different technologies are being developed and deployed to secure and ease the concerns of organizations and users. Some of these technologies include: smart cards, anti-virus software, biometrics, firewalls, password protected accounts, and intrusion detection / prevention systems, to name a few.

These rising concerns about security also moves technology away from people in terms of "ease of use" of operations. Thus, there is a need to integrate the required functionality of authentication and control to safeguard the data and information and "ease of use". According to Chellappa et al. (1995), biometric technology is one of the innovations that is being claimed to achieve this objective.

Khushk & Iqbal explain that "biometrics can be defined as an automated method of verifying or recognizing the identity of a living person based upon a physiological or behavioral characteristic; that is, it's based upon something we are or something we do".(Khushk & Iqbal 2005, pp.1)

Unlike passwords, biometric identification of an individual for the most part is permanent and cannot be easily changed. This type of authentication cannot be lost, forgotten or easily shared with others as can other objects used for traditional authentication because people normally have their physiological or behavioral characteristics on their person. When utilizing biometric authentication, there are no human resources labor expenses associated with password resets due to lockouts or expiration, which decreases a significant percentage of system management costs.

3.2 Biometric Technology

3.2.1 What is Biometric?

Biometric is used for identification or confirmation of a person's identity. In identification methods, a subject identity is determined based on the comparison of a biometric sample obtained from the subject earlier and stored in a database. Authentication methods are used for the confirmation of an individual's claimed identity; in this case the comparison is made only with the stored biometric features that correspond to the claimed identity (Stamp 2006)

The security field uses three different types of authentication: (Liu & Silverman 2001)

- Something you know—a pass-word, PIN, or piece of personal information (such as your mother's maiden name);
- Something you have—a card key, smart card, or token (like a SecurID card); and/or
- Something you are—a biometric.

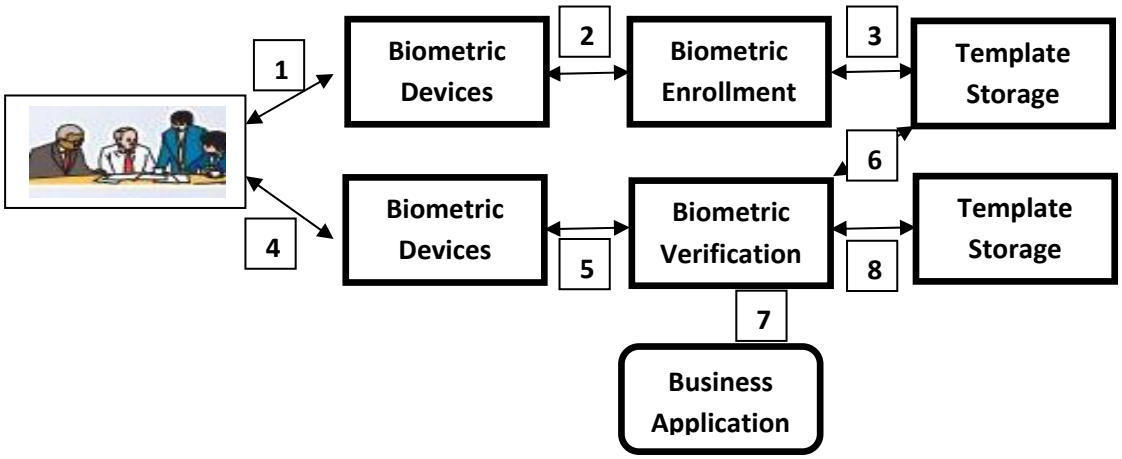


Figure 2-How biometric system works (adopted from (Liu & Silverman 2001, pp.28))

According to Liu & Silverman (2001), there are following eight steps involved in the working of biometric system as explained in above figure 2.

(1) capture the chosen biometric
(2) process the biometric and extract and enroll the biometric template
(3) store the template in a local repository, a central repository, or a portable token such as a smart card
(4) live-scan the chosen biometric
(5) process the biometric and extract the biometric template
(6) match the scanned biometric template against stored templates
(7) provide a matching score to business applications
(8) record a secure audit trail with respect to system use.

3.2.2 Biometric Traits

Faundez-Zanuy (2006) explains that a good biometric trait must accomplish the following set of properties.

Universality: Every person should have the characteristic.
Distinctiveness: Also referred to as uniqueness, see table 3 (Yun 2002). Any two persons should be different enough to distinguish them from each other based on this characteristic.
Permanence: Characteristic should be stable enough (with respect to the matching criterion) along time, different environment conditions, etc.
Collectability: Characteristic should be acquirable and quantitatively measurable.
Acceptability: People should be willing to accept the biometric system, and not feel that it is annoying, invasive, etc.
Performance: Identification accuracy and required time for a successful recognition must be reasonably good.

Circumvention: Ability of fraudulent people and techniques to fool the biometric system should be negligible.

Faundez-Zanuy (2006) identified that biometric traits can be split into two main categories:
Physiological Biometrics: It is based on direct measurements of a part of the human body like fingerprint, face, iris, and hand-scan recognition.
Behavioral Biometrics: It is based on measurements and data derived from an action performed by the user, and thus indirectly measures some characteristics of the human body like Signature and key stroking recognition.

Ratha et al. (2001) include a fourth, combined type of authentication in their list of existing user authentication techniques, see table 1. Ratha et al. (2001) claimsthat fortunately, fingerprint technology in particular and automated biometrics in general, can provide a reliable and accurate user authentication method. They explain that there is rapid advancement in the biometrics field that is concerned with identifying a person based on his/her physiological or behavioral characteristics. Examples of automated biometrics include face, fingerprint, iris, and speech recognition. According to Ratha et al. the user authentication methods can be broadly categorized into three categories as shown in table2.

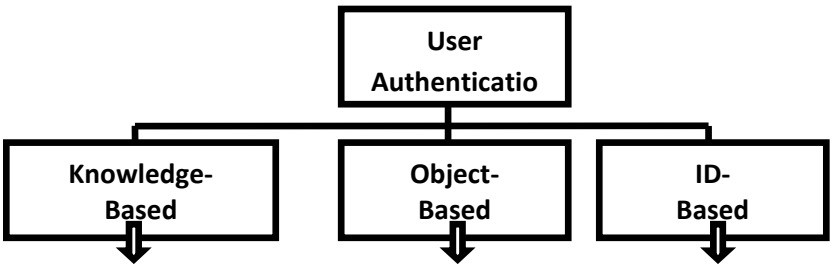
Table1-Existing User Authentication Techniques(adopted from (N. K. Ratha et al. 2001, pp.615))

Method	Examples	Properties
What you know	User ID Password PIN	Shared Many passwords easy to guess Forgotten
What you have	Cards Badges Keys	Shared Can be duplicated Lost or Stolen
What you know and what you have	ATM card + PIN	Shared PIN a weak link (Writing the PIN on the card)
Something unique about the user	Fingerprint Face Iris Voice print	Not possible to share Repudiation unlikely Forging difficult Cannot be lost or stolen

N. K. Ratha et al. (2001) further identified that because a biometric property is an intrinsic property of an individual, it is nearly impossible to share as well as very difficult to secretively duplicate. Authors explain that a biometric property of an individual can be lost only in case of serious accident.

3.2.3 Types of Authenticators

O'Gorman (2003) prefers the following authenticator labels: 1) knowledge-based, 2) object-based, and 3) ID-based. These are described below and illustrated in figure3



Commonly Referred to as:		Password, Secret	Token	Biometric
Support Authentication by:		Secrecy or Obscurity	Possession	Uniqueness and personalization
Security Defense:		Closely Kept	Closely held	Forge-resistant
Example	**Traditional:**	Combination Lock	Metal key	Driver's license
	Digital:	Computer Password	Key-less car entry	Fingerprint
Security Drawback:		Less secret with each use	Insecure if lost	Difficult to replace

Figure 3- User Authentication categories (Adopted from (O'Gorman 2003, pp.2024))

Knowledge-Based Authenticators ("what you know")
The Knowledge-Based Authenticators are characterized by obscurity or secrecy. An example of this type is the memorized password. This type can also include information that is not so much secret as it is "obscure," which can be loosely defined as "secret from most people." Father's name and your favorite car are examples in this category. In this case a security drawback of secrets is that, each time it is shared for authentication, it becomes less secret. (O'Gorman 2003)

Object-Based Authenticators ("what you have")
The Object-Based Authenticators are characterized by physical possession. Physical keys which we call metal keys. The main security drawback of a metal house key is that, if lost, it permits its finder to enter the house. This is why many digital tokens also combine another factor, i.e. an associated password, to protect a stolen or lost token. There is a different advantage of a physical object used as an authenticator; in case it has been lost, the owner sees evidence of this and can act accordingly. (O'Gorman 2003)

ID-Based Authenticators ("who you are")
The ID-Based Authenticators are characterized by uniqueness to one person. A passport, university diploma, credit card, driver's license, etc., all belong in this category. So does a biometric, such as a voiceprint, eye scan, fingerprint, or signature. For both ID documents and biometrics, the central security defense is that they are difficult to copy or forge.(O'Gorman 2003)

There are many biometric technologies in use today and many new technologies being investigated and tested in research laboratories worldwide. Nevertheless, all the technologies share a common process flow as follows:

3.3 Biometric Techniques

3.3.1 Face

A face image can be acquired using a normal camera. It is the most common biometric for identity authentication. The two main approaches that are used to perform face recognition are holistic or global approach and feature-based approach (Chellappa et al. 1995).

Feature-based approach

The feature-based approach relies on the identification of certain fiducial points on the face that are less susceptible to alteration, including the points surrounding one's cheekbones, the side of the nose and the mouth, points at the eyes, etc. The locations of these points are utilized to compute the geometrical relationships between the points. The regions surrounding the points can be analyzed locally also. The results from all local processing at the fiducial points are then collected and combined to obtain the overall face recognition. Since detection of feature points precedes the analysis, the system is robust to position variations in the image. However, automatic detection of the fiducial points is not consistent and accurate enough to yield a high accuracy ratio for the face recognition.

Holistic approach

The holistic approach processes the entire face image simultaneously without localizing the individual points as you can see fig 6. This approach has some variants in the type of technology used, such as neural networks, statistical analysis or transformations. The advantage of the holistic approach is that it uses the face as a whole. This in general yields more accurate recognition results. However, such technique is sensitive to variations in scale and position, and thus requires large training data sets (Chellappa et al. 1995).

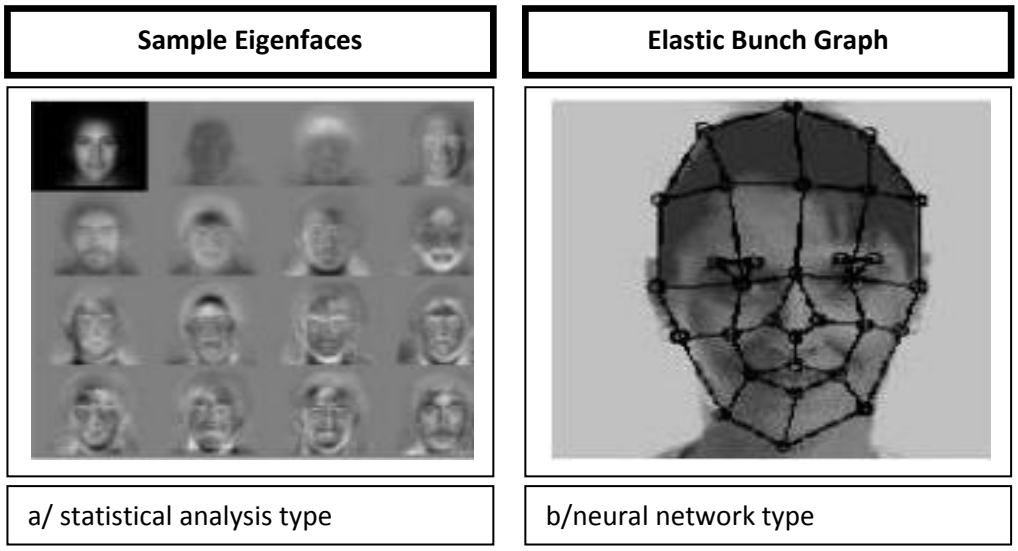


Figure 4-Exmples of Face Recognition Technique (adopted from(Yun 2002), pp.86))

Face recognition is generally accepted by the public because the cost is low, compact and easy to use. The disadvantage is that the accuracy achieved in only case of verification because of one to one comparison

and it is insufficient for identification because one is compared with all in databases and there is a chance of mismatch. The performance will also be affected by variation in face due to aging, hair-style, make-up, glasses, pose and lighting condition in addition to not being able to separate identical twins. (Yun 2002)

3.3.2 Fingerprint

Fingerprint is the oldest biometric method and pioneer in identity authentication and has been in use since 1896 especially for criminal identification. The main idea is based on fingertips that have corrugated skin with line like ridges flowing from one side of the finger to another. The flow of these ridges is non-continuous and it forms a pattern. The pattern of flow gives rise to a classification pattern such as arches, loops and whorls while the discontinuity in the ridge flow give rise to feature points, called minutiae as in figure7. (Yun 2002)

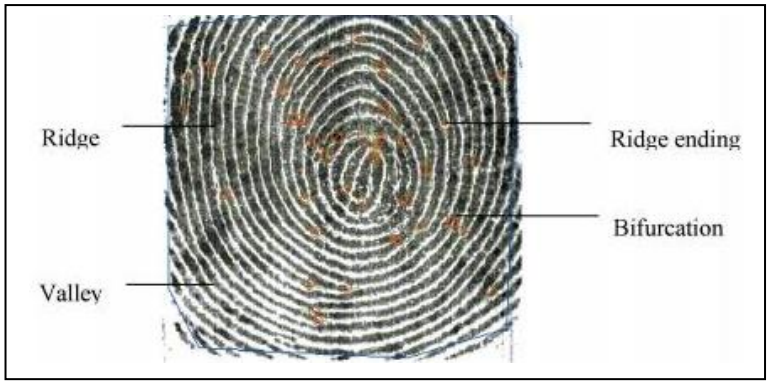


Figure 5- Sample Fingerprint Image (adopted from ((Yun 2002, pp.87))

In general, fingerprint recognition can achieve good accuracy sufficient for both verification and identification. Because of low cost and compactness it is popular consumer product. On the other hand the sensor is not able to capture acceptable quality fingerprint images for people with very dry or wet skin. Furthermore, it is necessary to maintain the sensor keep it clean in order to get consistent performance. (Yun 2002)

3.3.3 Hand Geometry

The hand image is obtained using a camera capturing from the top when the user places his/her hand on a desired surface. User hand can be aligned using reference marks or pegs. Two views are usually taken in a single image, the side view and the top view. The side view is usually captured by the top camera, using a side mirror. From the hand image, the fingers are located and the width, length, thickness, curvatures and their relative geometry measured see figure8.

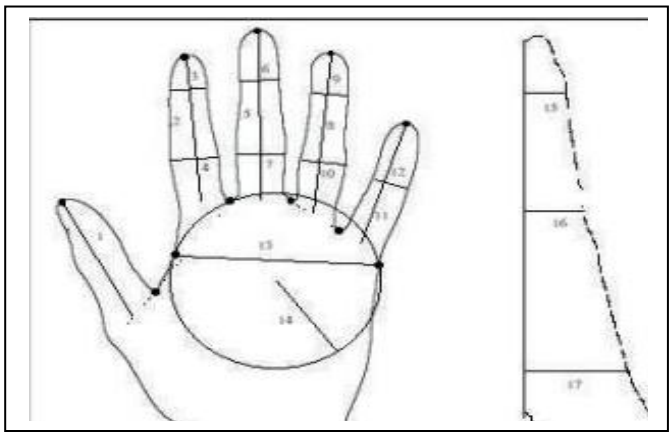


Figure 6-Measurement of Typical Hand Geometry (adopted from (Yun 2002, pp.88))

In some cases the hand geometry template size can be very small. In that case it has acceptable accuracy for verification but not sufficient enough for best identification. The main advantage is that most people can use it with ease and the acceptance rate is good. However, the negative side is that the system is rather bulky and may face problems with users aging and health conditions such as arthritis.(Yun 2002)

3.3.4 Iris

The iris image is usually acquired using a monochrome camera with visible and near infra red light (700 - 900nm). Iris, the colored part of the eye, is composed of a type of tissue called trabecular meshwork. When the iris is examined closely it gives the appearance of layered radial lines or mesh. The visible mesh consists of characteristics such as rings, striations, furrows, crypts etc and it gives the iris a unique pattern. The main point is that the iris pattern remains the same throughout life span and it is also different between twins, even identical twins since the pattern is independent of genetic makeup. (Yun 2002)

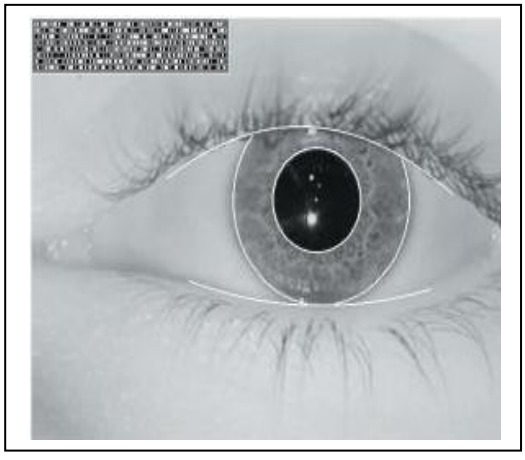


Figure7-A Sample Segmented Iris with iris code at topleft corner(adopted from(Yun 2002, pp.89)

With very low false acceptance rate the iris recognition is very accurate and can be applied to both verification and identification. It is relatively easy to verify whether the iris is from a living subject. The identification speed is also very fast. The other side is that the cost of the system is relatively high and the system is not compact. It also gets affected by poor lighting, reflection and possibly glasses as well as it may not be suitable for young children and people with cataracts. Furthermore, some imaging systems require the user to be motionless for a short time span.(Yun 2002)

3.3.5 Voice

Speaker recognition or voice authentication uses a microphone to record the voice of a person. For authentication the recorded voice needs to be digitized. 'The speech can be acquired from the user enunciating a known speaking (text independent) or text (text dependent)'. In the last case, the text can be prompted by the system or fixed. The text can be read discretely or continuously read out as an entire text. Furthermore, to form a voice template the captured speech is then enhanced and unique features extracted. (Yun 2002)

As the voice is a common means of communication, in combination with an extensive telephone network and microphones the cost of voice authentication can be very low and the system itself very compact. Furthermore, it is relatively easy to use. The other side is that the voice varies with age and there can be drastic change from childhood to adolescence. Moreover emotions and illness may affect the voice as well as room acoustics and environmental noise. Channel mismatch (use of different types and quality of microphones) and variation in microphones is also a major problem for the widespread use of this biometric technology.

Table 2-Comparison of biometric technologies (adopted from(Yun 2002, pp.91))

Biometrics	Univer-sality	Unique-ness	Perma-nence	Collecta-bility	Perfor-mance	Accepta-bility	Circumven-tion
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermo gram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L
H=High, M=Medium, L=Low							

In the above table3, universality indicates how common the biometric is found in each person; uniqueness indicates how well the biometric separates one person from the other; permanence indicates how well the biometric resist the effect of aging; while collectability measures how easy it is to acquire the biometric for processing. Performance indicates the achievable accuracy, speed and robustness of the biometrics

while acceptability indicates the degree of acceptance of the technology by the public in their daily life and circumvention indicates the level of difficulty to circumvent or fool the system into accepting an impostor.(Yun 2002)

3.4 Biometric Performance Measures

In order to examine and compare the performance of biometric technologies, there are some key measures identified below that are usually used to test such systems.

3.4.1 False Acceptance Rate (FAR)

The FAR is also known as "Type I error". FAR is a measure the percentage of impostors that are incorrectly accepted as genuine users. As almost all biometric systems aim to attain correct identity authentication, this number should be as low as possible.

3.4.2 False Rejection Rate (FRR)

The FRR is also known as "Type II error". FRR is a measure of the percentage of genuine users that are incorrectly rejected. In order to minimize inconveniences or embarrassment to the genuine user, this number should also be low as possible. In general, this error is more acceptable because the user can make a second attempt.

3.4.3 Equal Error Rate (EER)

FAR and FRR are related. A stringent requirement for FAR (as low as possible) will inadvertently increase the FRR. The point where the FRR is equal to FAR is given by this measure. Lowering the rate of EER will increase the performance of the system as it indicates a good balance in the sensitivity of the system. (Yun 2002)

3.4.4 Crossover Error Rate (CER)

A comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR. The lower the CER, the more accurate and reliable the biometric device.

Usually FRR and FER used to rate biometric accuracy. Both methods used to check the system's ability to allow limited entry to authorized users. However, these measures vary significantly, depends upon how you adjust the sensitivity of the mechanism that matches the biometric. For example, you can require a tighter match between the measurements of hand geometry and the user's template (increase the sensitivity).This will probably decrease the false-acceptance rate, but at the same time can increase the false-rejection rate. So be careful to understand how vendors arrive at quoted values of FAR and FRR.

Because FAR and FRR are interdependent, it is more meaningful to plot them against each other, as shown in Figure 9. Each point on the plot represents a hypothetical system's performance at various sensitivity settings. With such a plot, you can compare these rates to determine the crossover error rate. The lower the CER, the more accurate the system would be. Generally, physical biometrics is more accurate than behavioral biometrics.

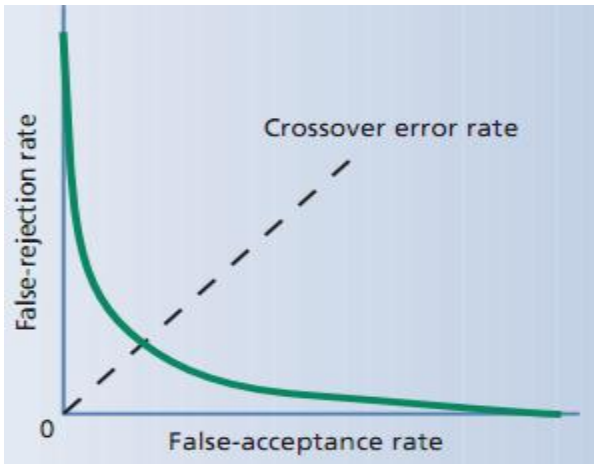


Figure 8-Crossover error rate attempts to combine two measures of biometric accuracy (adopted from (Liu & Silverman 2001, pp.32))

3.5 Issues and Challenges

When dealing with biometric technology, we have to consider some issues, and potential challenges faced by biometric technology. In selecting a specific biometric technology, the following things should be considered:

1. Size of user group.
2. Place of use and the nature of use (such as need for mobility).
3. Ease of use and user training required.
4. Error incidence such as due to age, environment and health condition.
5. Security and accuracy requirement needed.
6. User acceptance level, privacy and anonymity.
7. Long term stability including technology maturity, standard, interoperability and technical support.
8. Cost. (Yun 2002)

3.6 Biometric Technology Applications

There are numerous applications for biometric systems especially related to security related physical and logical access control. These include the following areas:

1. Banking/financial services such as ATMs, payment terminals, cashless payment, automated checque cashing etc.
2. Computer & IT Security such as Internet transactions, PC login etc.
3. Healthcare such as privacy concern, patient information control, drug control etc.
4. Immigration such as border control, frequent travelers, asylum seekers etc.
5. Law and Order such as public ID card, voting, gun control, prison, parole etc.
6. Gatekeeper/Door Access Control such as secure installations, military, hotel, building management etc.
7. Telecommunication such as telephony, mobile phone, subscription fraud, call center, games etc.
8. Time and Attendance such as school and company attendance,
9. Welfare, including healthcare services and benefit payments
10. Consumer Products such as automated service machines, vault, lock-set, PDA etc.

There are major challenges to the adoption and wide roll-out of biometric systems, such as lack of user education, since there are many biometric technologies to choose from and not every technology is suitable for all application contexts as well as the privacy aspects on the use of such technology. According to Yun (2002), over expectation by the user either due to exaggerations by the over-zealous sellers concerning the capability of biometric or ignorance of the users will also slow the market adoption of biometric technology applications. In addition, as the biometric system will not perform according to "user expectations", it will cause lack of trust in the technology. Yun (2002), further explains that the lack of standards and interoperability is also a challenge preventing wide-scale adoption since users especially corporations will definitely not show interest to invest in a technology that will soon become obsolete or lack technical support.

3.7 Biometric Technology and Healthcare

Within the healthcare sector, biometrics technologies increasingly are being viewed as a means of preventing the unauthorized use of system resources, managing access to information systems, and ensuring the security of financial and patient records. Due to the security requirement of the Health Insurance Portability and Accountability Act (HPAA) of 1996 in US and similar legislation in other countries, the need for secure information systems has become a critical issue. It is necessary to have a reliable means in place to verify patient's individual identities when physicians access the electronic patient records to order medications or tests. The use of biometrics allows higher control over physician access to electronic clinical patient records and it also provides higher audit trails for tracking physicians order entries for prescriptions or laboratory tests.

3.7.1 Uses of biometric in healthcare

Access control and authentication technology based on biometric provides more secure method for identification and access control than traditional technologies. Biometric technology also can be utilized to secure and protect patient's privacy in shared care contexts by making information network systems more secure (Atkins 2000; Marohn 2006). According to Gates (2007) and Nyuo Shin et al. (2008), biometric technology considerably reduces the chances of unauthorized access and facilitates the maintenance of appropriate access privileges. It can also provide a suitable solution for guaranteeing accessibility and security to electronic health records. The level of security is increased by preventing the fraudulent access to restricted information as biometric technology uses unique physical features of a person. According to Gates (2007) and Nyuo Shin et al. (2008), biometrics allow the elimination of end-user generation of passwords, which has become a main security issue for current information systems. In general, using biometric technology as access control and authentication method enhances the protection of patient privacy. By adding an accurate authentication technology, unauthorized access to sensitive information is reduced by restricting delegation of access right and impersonation of individuals, besides this, it eliminates cost associated to password maintenance, reduces fraud associated to insurance claims and becomes a long term solution for access system management (Gates 2007; Zuniga et al. 2009)

As the public's attention is primarily focused on the use of biometrics in critical infrastructure and security applications, biometric technologies such as iris recognition, fingerprint, and hand geometry have gained traction in healthcare applications. From an application perspective biometrics can perform the following operations:

- Combat fraud and abuse in healthcare entitlements programmes;
- Protect and help in the management of confidential medical records;
- Identify patients; and
- Secure medical facilities and equipment. (Marohn 2006)

Through healthcare provider authentication biometrics can protect the confidentiality of medical records. With the development of interoperable health information databases implementing biometrics can enable services to be administered in a more universally applicable and regulated manner. With the support of biometrics patients can be identified and linked with their personal medical records for potentially faster access to care, more accurate care, and guaranteed coverage. Moreover in the case of clinical trials biometrics can support better organization of data and maintenance of case report forms. (Marohn 2006)

The implementation of biometrics can reduce additional costs associated with medical record keeping, as well as improving the delivery of medical care to patients, by streamlining all relevant information of patient into electronic databases that can be easily maintained and updated once the overarching infrastructure is developed. Furthermore biometrics could be use for protecting high- risk medical areas, or sensitive supplies areas (Marohn 2006).

Decreased registration time is another considerable advantage of biometrics for both the patient and healthcare provider. Biometrics is also helpful in preventing medical errors before a patient undergoes any medical treatment. According to (Messmer, 2004), a quick scan of the patient's iris or fingerprint would allow healthcare staff to make sure that they have the correct patient before surgery or other medical procedures. Moreover, having a biometric system support to the emergency department staff would assist in identifying many of the anonymous patients.

According to Chandra et al. (2008), there is no doubt that biometrics has considerable potential in health care, in facilitating enhanced information security, cost reductions, improved accessibility, increased quality of care, and even greater geographic equity of delivery.

3.8 The future of biometrics

With the development in technology innovations, the cost of implementing biometrics is expected to decrease dramatically. According to Allan (2005), International Biometric Group of New York projected that global biometric revenue would rise from 2.1 billion dollars in 2006 to 5.7 billion dollars in 2010. According to Li & Xu (2009), this trend will contribute to making biometric technology more accurate, secure and make its usage more widespread.

The implementation of biometrics in healthcare also includes consideration of challenges in management. According to Chandra and Calderon (2005), there are many challenges associated with biometrics that need to be faced and considered when deciding whether or not to implement a biometric system in an organization.

3.8.1 Business or Financial issues

For planning biometrics implementation financial feasibility is an issue because the direct costs of implementing a biometric authentication system are tangible, immediate, and measurable. Chandra and Calderon (2005), explain that the advantages of such a system are long term, qualitative, and difficult to estimate monetarily.

3.8.2 Operational issues

The challenge of operational issues often appears during authentication, enrollment, and storage processes in the biometric authentication system. For example, the security provided by a biometrics system is a

combination of controls that are embedded in the enrollment process. According to Chandra and Calderon (2005), a poorly enrolled system does not allow for effective security through biometric authentication.

3.8.3 System issues

Chandra and Calderon (2005) explain that system issues include the effects of implementing biometrics technology in business processes, system performance, and systems design. According to them, at present, it is rather unclear what the effects of downtime, cyber attacks, and major disasters will be on a biometric authentication system.

3.8.4 People issues

Vijayan (2004) & Chandra and Calderon (2005) argue that at base, people distrust biometric authentication systems. Civil libertarians often oppose biometrics as being a potential tool for demographic profiling, intrusive, and a means of eroding patient privacy. Further biometrics are unlike conventional identifiers such as PINs or passwords because they are linked to a specific person and cannot be replaced, changed, or modified. Users will need help to understand and experience the biometric technology and overcome their concerns about security and privacy. They identified that biometric technology still seems to be too intrusive to many people.

3.8.5 Legal issues

There is a delay between changes in legislation and advancement in technology in context to biometric technology implementation. The reliability of data in biometric authentication systems is one of the major concerns that complicate the legal aspects for biometric technology. According to Chandra and Calderon (2005), there is a very low level of independent verification of the performance evaluation of existing biometric systems.

3.8.6 Physical traits of individuals

Chandra and Calderon (2005), explain that not every individual in an organization will have the prerequisite behavioral or physiological traits for using biometric systems. There have been some reported cases where some biometric system users do not have sufficient/required details on their finger prints for accurate processing by a biometric device. Organizations could face problems in such cases when certain users do not have the sufficient/required biometric, for instance, eyes or fingers. In such cases it would be expected that it would require organizations to accommodate certain users. These accommodations might considerably increase the costs of implementing, maintaining, and updating biometric technology. Furthermore another challenge is natural aging or unanticipated changes and development in physiological characteristics, for example, a surgery or an accident where an individual may lose a hand, finger, or an eye. In such cases the individual would need to be re-enrolled in the system, which will also increase costs.

Chandra and Calderon (2005) explain that the healthcare industry is probably one of the businesses that is best suited to gain benefits from biometric technology. It is essential for healthcare providers to protect patient’s medical data which is also reinforced with strict state and federal regulations.

4 Empirical Finding

4.1 Interviews

The aim of our interviews with representatives of the biometric systems providers and experts was to learn more about the current state of biometrics systems in the healthcare sector and to explore their opinions about attitudes and factors influencing adoption/deployment of biometrics systems in this sector.

In our research, we selected five interviewees to express their experiences, opinions and domain knowledge about the implementation of biometrics system in the healthcare sector in the county of Blekinge.

The selection was made based on our ambition to interview different stakeholder representative, who could give us information about different perspectives on biometrics in healthcare organization. It was not easy to gain access to conduct interviews in the healthcare organization. In the end, we were able to conduct five in depth interviews with people representing different types of knowledge which we felt was relevant for our topic. These five interviews gave us number of different perspective on the current situation concerning biometric technology and/or attitudes toward security in healthcare.

4.1.1 Purpose

In this research we made five extensive interviews with the purpose to identify the attitudes and factors influencing the adoption/deployment of biometrics technology in the healthcare system in the county of Blekinge. All the interviewees have explicitly gives us permission to use their names and affiliation in our report.

4.1.2 Selection of Interviewees

Based on our research questions, we chose five people. These were people who either have a key position in biometric industry or in healthcare organization are experts within academia in the area of biometrics.

The first interview was conducted on 1st May, 2010 with Mikael Nilsson, from Section / Unit: School of Engineering (ING), Dept of Electrical Engineering, Blekinge Institute of Technology (BTH), Sweden. He was working at BTH as Head of Biometric lab in Ronneby campus, Sweden and he is also an Assistant Professor. The reason behind his selection as an interviewee is that he has been supervising practical lab experiences with biometric technology. Mikael could give us information about the technology.

The second interview was conducted on 18th May, 2010 with Karin Sveheim, from Biometric company The Precise Biometrics, Sweden. She was working as a Director, Markets in that company. The reason behind his selection as an interviewee is that he has been working as a biometric secruity solutions provider. Karin could give us a provider's perspective on biometric technology.

The third interview was conducted on 21st May, 2010 with Søren K. Lauritzen, from IT2Trust A/S, Denmark. He was working as a Business Manager/Partner in that company. The reason behind his selection as an interviewee is that he has been working as a biometric security solutions provider especially for healthcare sector.

The fourth interview was conducted on 1st June, 2010 with Birgitta Billinger Lundberg, from Landstinget Blekinge, Sweden. She was working as a Chef Blekinge kompetenscentrum. The reason behind her

selection as an interviewee is that she has already aware about security and privacy concerns related to patients/staff and cost concerns related to organization. Birgitta is a healthcare administrator at the Blekinge and has long experience of developmental work in the healthcare organization. She is not an expert on technology. She knows a lot about attitudes to technology in healthcare.

The fifth interview was conducted on 7th June, 2010 with Peter Svensson, from Blekinge Kompetenscentrum, Sweden. He was working as responsible for System Integration. The reason behind his selection as an interviewee is that he is well aware of current authentication system and he also involved in the integration of old authentication system into new systems with the support of biometric to provide more secure solutions using smart cards. Peter could give us an initiated overview of the existing security system.

4.1.3 Interview Execution Planning

The five interviews were conducted and recorded at five different times at five different places. Time duration of first interview and second interview was 60 minutes, third interview was 55 minutes, fourth interview was 45 minutes and fifth interview was 50 minutes. As an introduction, the background of research, research questions and objective of interview were explained to the interviewee at the beginning of interview.

4.1.4 Designing and Conducting the Interview

In interviews authors combined formal and informal questions to identify factors influencing the adoption/deployment of biometrics technology in the county of Blekinge. The authors designed some set of pre-planned questions to explore the factors influencing the adoption/deployment of biometrics technology in the county of Blekinge. This was combined with open-ended questions framed during the discussion based on the reply of the interviewees. In interviews we recorded, observed and noted the important factors influencing to adopt/deploy biometrics technology in the county of Blekinge.

4.1.5 Data Collection

In data collection procedure observations were made during the interviews with the biometrics company representatives, hospital administrator, IT security person and biometric technical personnel. The data during the interviews and observations were video recorded and documented. With the permission of interviewees the video recording was performed carefully during the discussion between the authors and interviewees. The documentation also helped authors to further analyze the data.

4.2 Interview Analysis

4.2.1 First Interview

The first interview was conducted with Mikael Nilsson, from Section / Unit: School of Engineering (ING), Dept of Electrical Engineering, Blekinge Institute of Technology (BTH), Sweden. He is working at BTH as head of biometric lab in Ronneby campus, Sweden and is also an Assistant Professor.

The interviewee explained the importance of three attributes cost, privacy and security during the implementation of biometrics. He said he will recommend physical if we take these three attributes, first of all the security is higher and we will have a better performance of using physical biometrics then behavioral in general and the cost would be same. He said the cost may be slightly higher depending on

the performance of the system. He explained that if we don't have a good performance we will have complaints and in case when we have failure of system then it cost more. He agreed with the importance of implementation of biometrics in healthcare and he has knowledge about the biometrics implementation with respect to its attributes.

According to him voice recognition along with finger prints is the best idea in biometrics and it could provide quite strong security parameters as compared to other traditional techniques.

The interviewee said that instead of considering the level of accuracy and efficiency to ensure security and privacy, I think the issue is cost and the way you use sensors in terms of cost. He said he will choose fingerprint at present. There could be in combination like ID card with fingerprint and/or face image. Face image can provide a check, if you know someone has entered with the fingerprint and you are not sure it is right person so you can have the face as a back-up system. In summary of his opinion, cost is the main factor in the implementation of biometrics system in healthcare and for security reasons a good combination could be ID card with fingerprint and/or face image.

Regarding the biometrics technology implementation he said there is always cost involved. For example, he explained in fingerprint you need a capacity of sensors its quite simple if you go out and check the fingerprint the cost of its sensor and compare to good digital camera there is a huge difference. He said face and iris cost more because these methods require special cameras, so the cost is low for fingerprint the security is in middle, convenient and fairly good. He said you have to think about when anybody touches the sensor device, there is a risk of spreading contagious deceases. In summary, he was of the opinion that for initial implementation stages the finger print technology could provide cost benefit as compared to other available biometric technologies.

He also said in when we are dealing with facial recognition system, it's natural that the face change with the age so that's why we have to update the system and it will also the affect the cost. So according to his views, the cost is the biggest factor affecting the adoption/deployment of biometrics systems. In summary of his opinion, not only implementation cost but also the maintenance cost could affect the adoption of biometric technology in healthcare.

Regarding the cost factor he said the cheapest technology is the keystroke because you have keyboards that are fairly cheap. If you just think about the sensor, the voice you need a micro phone a good microphone, more expensive, in signature you need more like tablets that cost more than a keyboard at least. The main cost is fall back system because the systems are not 100 percent accurate. Second thing is you need to educate those people who will use it and the persons who will be responsible. In summary of his opinion, the failure of the system and its maintenance cost is also an issue and the other aspect is we need to educate people first in order to successfully deploy biometrics technology in healthcare.

In reply to the question that on the website NEC is a company giving a solution with an error rate of 0.001, he explained that it depends on what test they do for it to check its accuracy and performance based on different algorithms. It could be very easy task if you have voice of two persons and each person has a different word then you don't get any error basically you have to think about how you do the test when you get those numbers and the validation of the tests is done. He explained that if all people are well aware about the issues related to biometrics and everything functions completely fine then he is in favor of biometric system. In summary, for successful implementation of biometric technology the biometric system must be as error free as possible.

The interviewee explained that in biometric systems technical aspects still need improvement, the sensors have to follow some standards so there will be no problem of interoperability among different sensors and there will be no any problem during the adoption of new system. The biometric system has to be self

learner when the user is dealing with the system and the system must provide guidance to the user when the user is operating the system It is analyzed that there is need of interoperability among biometric technology based devices and there is a need for standards which will decrease the update cost of biometric systems.

The interviewee explained the issue of false positive and false negative. He said you always have these issues but they can be very small so the fall back or the error of the system can be very low. He suggested that we can increase security if we combine biometric with a very short password because in this way hackers have to break two systems so the level of the security will increase, so you have to increase the complexity of the system to enter. He said in general if you are just using biometrics it could be difficult to avoid hackers. He said you also have to consider the number of system users; this has direct effect on the system. If you have millions of users then the error probability could be very high. In summary, he was of the opinion that in order to increase the security, the biometric system could be combined with a password system. Before deploying a biometric system, it is necessary to focus on number of users because it directly effects the error rate, If we have a high number of users then it will increase the error rate.

The interviewee said biometrics is more trustworthy compared to traditional log-in and password schemes. He said we can technically convince decision makers like in general you will invest money for password handling by the IT person but if the system of biometrics works well you will have higher security with lower cost.

He identified that they do not have any legislation or rules for biometrics in Blekinge county IT policy or in Sweden. He said one of the main obstacles of adoption/deployment of biometrics technology is that they do not have legislation for biometrics and the biometrics security is going to be much higher. The companies which are supplying standardization like in US they already have specific rules and in Sweden there is a need for adopting rules and legislation in this area too. In summary, he was of the opinion that there is a need of legislations for biometrics as the security measures going to be much higher as compared to the traditional password systems.

4.2.2 Second Interview

The second interview was conducted with Karin Sveheim, from Biometric company (The Precise Biometrics), Sweden. She was working as a Director, Markets in that company.

According to Karin, Precise the biometrics company representative, there are many reasons for the deployment of biometrics technology in healthcare sector. Biometrics will increase security and privacy of patient data and information. It also ensures the right identity of the patient (vast number of mistaken or duplicate identities and patient records), and more convenient procedures for staff as well as it provides cost savings advantages. It is summarized that biometrics will help to ensure the right identity of person, provides cost advantages and provides adaptable procedures for biometric users.

The interviewee explained there are threats and challenges that compel the implementation of biometrics. The main challenge is that healthcare records are not to 100% electronic today. A lot of records are written by hand. Digital files are a clear pre-requisite for using biometrics. Overall, the uncertainty surrounding biometrics in terms of privacy, reliability, cost and convenience have to be addressed. Thus, to summarize that there is a need of healthcare records to be 100% electronic because it is pre-requisite for biometric implementation in the healthcare sector to protect patient information.

The interviewee identified that organizations are demanding strong authentication and focus on suggesting biometrics because for staff it offers fast and convenient access to computer systems and patient files, for healthcare providers it offers cost savings compared to complex password systems, increased IT security (no shared passwords, no written down passwords, etc) and, also refers to accountability and traceability of the system. For the patient it refers to the integrity of sensitive information that will be preserved and biometrics will also minimize the chances of errors related to duplicate records or errors related to identity. In summary, the interviewee was of the opinion that organizations are demanding strong authentication and focus on suggesting biometrics because it could provide advantages to patients, healthcare staff and healthcare providers.

Further, the interviewee explained that their Match-on-Card solutions combine fingerprint recognition and smart card technology. The smart card brings security, portability and scalability to the system, the biometrics brings ease of use, speed of transaction, and personal use. Combined it brings protected privacy as biometrics is always handled by the card and makes the token personal. The features and technology is to some extent generic but integrated in its applications it is adopted for healthcare use. It is summarized that the combination of smart card with biometrics could provide considerable advantages in sense of ease of use, speed of transactions, personal use without compromising privacy and security.

The interviewee thinks that the biometrics solution can fulfill the requirements of healthcare sector regarding privacy and security of patient's record, especially in combination with a smart card. Using a database of biometric information will always be sensitive and carries the risk of intrusion and abuse. Combined with a smart card, the cardholder is always in possession of his/her own sensitive data. Thus, to summarize, the combination of smart card with biometrics could provide sense of security to cardholder regarding his/her own sensitive medical data.

The interviewee identified that the National Healthcare security policy and legislation is important to build customer trust. She also explained her views regarding the ROI (Return on investment) in context of biometric in healthcare sector. She said that if an IT system should be built for security based on passwords, these have to be so complex an organization will have to spend a lot of time managing password distribution, password resets, etc, not to mention the loss of productivity on the other end. A password based system is never free of charge. You can calculate a cost of approx 200 USD per year per user in Password related costs. You can typically calculate the ROI on a biometric solution within a year. In summary, interviewee was of the opinion that the National Healthcare security policy and legislations is important to build customer trust. Biometrics also has advantages regarding return on investment as compared to password based system.

The interviewee explained views regarding the cost of the biometric solution compared to card system. She said, her company is advocate of combining fingerprint and smart cards. Unless you combine the biometrics with the card, there will be a lot more costs associated with the surrounding infrastructure in terms of fingerprint terminals having to be secured (i.e limited supply) and other mechanisms surrounding data protection. By using the card, you can freely choose between different readers.

Important to note is that the organization should be independent of card supply (especially if distributing cards to patients, i.e. large numbers of users) so they can also choose card suppliers according to new needs and budgets. Then it could be a good idea to make sure the biometrics is added as a Java applet so they don't have to replace this component as it would require re-enrollment, etc. It is summarized that because of huge number of expected users the organization should be independent on card supply and the biometrics should be a self contained add-on, making it easy to change card supplier if necessary.

The interviewee identified the main influencing factors for deployment of biometric in healthcare. The factors are governmental legislation, a need for a stronger focus on healthcare administration costs and a need for a faster move to electronic healthcare records.

The interviewee said that there is a need to conduct a study in order to analyze the need of different actors that will participate in the use of these biometrics systems.

The interviewee said that the use of biometric in healthcare industry seems to be undergoing a slow revolution but she thinks that the government legislation will push healthcare providers toward using the technology in a variety of ways of safeguarding patient data to securing physical locations. According to her biometrics is slow to adopt in all areas of application, also in high security demanding environments. It is nothing unique. It is the 10-year maturity cycle that new technology faces. She said that the most influential reason to succeed is cost. In summary, the interviewee was of the opinion that the government legislation will push healthcare providers toward using the biometrics technology in a variety of ways for safeguarding patient data and the most influential reason to succeed is cost advantage.

The interviewee said that for the successful implementation of biometrics there is a need to focus interests of all actors (patients, healthcare staff and. healthcare providers). According to the interviewee, the health care sectors rules and legislation will affect the suggested biometric solutions.

4.2.3 Third Interview

The third interview was conducted Søren K. Lauritzen, from IT2Trust A/S, Denmark. He was working as a Business Manager/Partner in that company.

According to Lauritzen, the biometrics company representative we interviewed, there are many reasons the biometrics needs to be implemented. Biometric devices like fingerprint scanners are a very secure way of authenticating users and at the same time very easy to use. All users carry their identification with them and it is not an easy task to steal this identification method. Furthermore, the healthcare organizations have access to a lot of sensitive data about their patients and it is important to make sure that all data is secured in the best possible way. Thus, to summarize, there are strong reasons that biometrics could be implemented because there are many secure authentication devices related to biometrics available in the market that could secure data in best possible way.

The interviewee explained there are threats and challenges that threaten the implementation of biometrics. The security threats are it is very easy for the “wrong” people to get access to systems, networks, computers if these are only protected by a simple user id/password system. Specially in cases where the “right” users also have a lot of different systems where they need to validate themselves with user ids/password, as they tend to either create their own password-synchronization tool and/or write down their passwords on handy notes. In summary of the interviewee’s opinion that due to the threats and challenges to traditional password schemes there is strong needs of biometrics to be implemented.

According to interviewee, the privacy threats are that healthcare organizations have a lot of sensitive data about their clients/patients and this information can be useful for people outside these environments (for example for use for blackmail, tabloid stories, employment issues and fraud in general) and it is therefore important that the privacy of the clients/patients is protected in the best possible way. It is summarized that due to privacy of the clients/patients data there is a strong need of biometrics to be implemented.

The interviewee identified that organizations are demanding strong authentication because the healthcare industry involves a lot of sensitive data that has to be available only to the relevant people and you need

to make sure only these people can get access to the sensitive information – but you also need the information to be available to sometimes many different people with short intervals (local doctor, hospital doctor, nurse, surgeon and so on). He explained that the organizations are suggesting biometrics because digital personal fingerprint readers as a means of biometric authentication are fast, reliable and most of all secure and hence providing the healthcare organizations with the strong authentication needed to secure sensitive information.

The interviewee said that current biometrics solutions can fulfill the requirements of healthcare regarding privacy and security of patient's record he given the example of DigitalPersona that already has several customers in the healthcare sector utilizing their solution to secure the privacy of patient's records (some official references are listed here: http://digitalpersona.com/biometrics/solutions/healthcare/).

The interviewee also explained views regarding the ROI (Return on investment) in context of biometric in healthcare sector. He said that it is not an easy task apart from the increased security you get from using a biometric solution, the following issues should be considered and taken into account when evaluating: less time wasted on password reset (both for IT personel and medical employees (doctors, nurses and so on)); faster and easier access to the relevant information/systems as the employee only needs to scan a finger to be authenticated. DigitalPersona can provide both the fast and reliable fingerprint reader and the centralized management system to handle all the users. In summary, interviewee was of the opinion that with the increase in security using biometric solutions the issue of ROI (return on investment) should be considered and taken into account.

Interviewee explained the views about costs of the biometric solution compared to card system. He said it depends very much on what kind of system you want to use. For both solutions you would need some kind of centrally managed administrative platform to handle users and what they need access to. The cost of these admin systems needs to be compared also and you need to make sure the systems can give the same administrative functionalities when comparing them. Then you need to compare the cost for hardware: fingerprint readers versus ID cards. Usually you would only need maximum one reader per employee (sometimes even less as they might share computers), but you would definitely need at least one ID card per employee plus some extra when they destroy, lose, forget their original ID cards and in that regards also calculate the added cost of time spent taking care of issuing new cards and so on. With DigitalPersona you have the possibility to take advantage of embedded/integrated swipe readers in many laptops which means you don't need separate fingerprint readers for these computers.

Interviewee identified the main influencing factor to deploy Biometric in healthcare. The factors are it will increase security as well as provide easy and quick logon (and switching between users).
According to her there would be many benefit after the deployment of biometrics, it will increase security in regards to authentication of users and thereby giving them access to the right information; fast access to the relevant information and the possibility to take advantage of roaming users (i.e. access to data from different computers). Thus, to summarize, biometric could provide many benefits in sense of providing security, access to right information and access to data from different locations.

Interviewee explained that there are some threats concerning the implementation of biometric technology in healthcare organizations. The threats are finding a solution that can be used across many different healthcare organizations (hospitals, clinics, private doctors and so on), administrating it and figuring out how to split the payment of such a solution; of course the economics in general for such a solution also plays a role, but in my opinion it shouldn't be as important as it is a matter of security and protecting privacy. It is summarized that the economics in general for biometric solutions also plays a role but it shouldn't be as important when it comes to a matter of security and privacy of clients/patient data.

Interviewee also identified some factors that slow down/prevent the implementation of biometrics in healthcare. The main factor is how a user could use biometric solutions (fingerprint scanners) in sterile environments, if a surgeon wears plastic gloves during an operation it is difficult for that person to access patient records with the use of fingerprint scanning (but then again, it would also be less sterile if he/she needed to type in a userid/password or use an ID card solution that is also used outside the sterile environment). Thus, to summarize, there are still many areas that need to be considered i.e. limitations and restrictions in different environments where the biometric devices could be implemented.

Interviewee explained his opinion that the government legislations will definitely push healthcare providers towards using biometrics technology. He said there will be much more focus on how sensitive information is both stored and accessed (and by whom) and also who has access to physical locations, but she also think that the use of government legislation may vary a lot from country to country and even within each country depending on how the government entity usually handles these issues. It is summarized that because of security and privacy issues regarding patients/clients data the government legislations will definitely push healthcare providers towards using biometrics technology.

He explained her views concerning the question if privacy and security would compromise with less additional cost? He replied that privacy and security can always be compromised, It is impossible to be 100% secure no matter how much money you spend and how many different solutions you implement (hackers can get access to FBI, NASA and organizations like that and they spend a lot of money on security). However it is important to take appropriate measures to make it as difficult as possible to get access to the sensitive data. Even with strong encryption on data and several biometric solutions together with smartcards and passwords there is always the possibility to force/threaten/pay somebody with the right access to deliver the needed information, the cyber criminals are always one step ahead unfortunately. Thus, to summarize, the focus must be on to take appropriate measures to make it as difficult as possible to get access to the sensitive data.

He explained his opinion oncerning the question if biometrics makes a difference of cost with respect to the password management and card system while adopting in healthcare organizations? He said a fingerprint scanning solution will of course cost some money but the solution from DigitalPersona is not necessarily more expensive than a password management and/or card solution. As explained before DigitalPersona has a very powerful management system that can handle the users, control their access rights and manage both separate USB fingerprint readers and integrated swipe readers in many laptops.

4.2.4 Fourth Interview

The fourth interview was conducted with Birgitta Billinger Lundberg, from Landstinget Blekinge, Sweden. She was working as a Chef Blekinge kompetenscentrum.

During the interview Birgitta Lundberg gave her opinions that how she perceives biometrics in heathcare. She said biometrics can give us a way to identify elderly people when they are ill and in need for acute care, even if they don't have safety identification themselves. Biometrics will help the system from home, through the ambulance transport, emergency room to the ward or home again.

The interviewee said that biometrics would be a better way in security aspects when we are dealing with medical records as compared to the password authentication techniques. According to her biometrics would be best way to secure entrance points of special rooms and buildings for both medical staff and patients. Thus, biometrics would be most feasible to implement on entry clearance points.

She said biometrics could serve as a useful platform to address a majority of security, privacy and cost issues. She also said that there is a need of security and privacy at this stage because they have sensitive information such as patient's record etc. She also explained that there are strict Swedish govt. regulations pertaining to the protection and privacy of medical records.

She identified that there is legislation concerning that patient's data will not be used by others. The patient record is owned by the hospital which is responsible for keeping the data safe from others. The patient can get a copy of his record, in some special situations the question can be denied, in terms of the best care for the patient. It is against the law to log in to a patients record if you don't belong to the treatment team or have a special reason.

According to her in a current situation if we implement biometrics then it might be very expensive. For example if we need to sign in with our finger prints to enter in the medical room and everyone in the administration has to follow the same way to enter then it might be very expensive.

According to her biometrics would be a better way to keep the information safe from hackers. From an implementation point of view she said, people need to learn the system and it could be risky if someone is unaware about the system functionality.

4.2.5 Fifth Interview

The fifth interview was conducted with Peter Svensson, from Blekinge Kompetenscentrum, Sweden. He was working as responsible for System Integration.

He said that they still use physical keys at certain places but at many places they have an electronic system. The electronic system is based on plastic cards with a magnetic strip combined with a PIN-code.

The interviewee explained that they manage healthcare information in different ways. They have several computer- based systems that manage information mostly in databases. They have patient records on paper (they are being scanned to be managed within a system that uses the same identification). They store some information regarding a specific diagnostic in their respective systems, for exemple X-ray/ultrasound etc. The protection of this information differs from system to system. They do not have a classification of different types of information, for example highly confidential, less confidential etc.

He said there is low risk of medical identity fraud, theft and abuse in the current healthcare environment. He explained in Sweden you are guaranteed healthcare without private insurances. He explained from that background I would say that medical identity fraud does not exist here in Sweden. He said in his job experience he had not heard about this issue. In fact he never heard about this even from the administration of EHR-system. In summary, he felt, there is very low risk of medical identity fraud, theft and abuse in the current healthcare environment in Sweden

He identified that there is a need of new authentication techniques for maintaining privacy and security challenges. He said we are currently very focused on all the national initiatives in this area (SITHS/BIF/HSA etc), So the "new" techniques are coming now, but they do not involves biometrics. This could be either because we are to unfamiliar with the Biometric technique or that we are not yet mature for it.

He identified that there is a need of awareness about biometric technology among users. He thinks that the top management will focus on the issues concerning the deployment of Biometrics in near future. He said currently we are building a strong foundation for the future regarding national initiatives. We have

currently many projects and useful services for the citizens etc so I think the focus will also be on biometrics technology in the near future.

According to the interviewee, the current Swedish healthcare legislation is enough to deal with privacy and security of sensitive information in healthcare. He also emphasized that the security cannot be assured with user ID and password in public places. Thus there is a need of biometric technology in future in the healthcare area.

According to him, of the three factors (cost, privacy and, security), the cost is the strongest argument (40%), security the next strongest argument (32%) and privacy comes third (28%), in affecting the adoption of biometrics in healthcare organizations. He thinks the cost will be the most important for the adoption. Privacy and security are pretty equal but Security might be slightly more important.

4.3 Survey

4.3.1 Purpose of the Survey

A survey is a strategy for inquiry and use as a quantitative research method which provides a numerical description of the opinion attitudes, and trends of a target population. In using survey as a method, researchers selected sample of population and then generalize the results for whole population (Creswell 2009). In our study, the chosen sample is too small to allow generalization of the results for the whole population. Thus, we are using the survey method here in an exploratory manner as a first step in mapping attitudes in our field of study.

4.3.2 Why used this Strategy of Inquiry?

Survey is widely acceptance for data collection. Survey is inexpensive to design and it gives rapid turnaround in data collection (Creswell 2009). Due to the resource and time constraint we selected survey as a data collection procedure. In our case, as a complement to interviews.

4.3.3 Methodological Triangulation

As explained in research methodology chapter, authors adopted Methodological triangulation, which refers to the use of more than one method for gathering data about research(Bryman, Triangulation). Authors used this survey together with interviews as a way of mapping attitudes towards biometrics in healthcare.

4.3.4 Form of Data collection

For data collection via surveys, there are different forms of survey are available. For data collection the survey may be in oral, written or electronic form. Other forms of data collection are self- administered questionnaires, structured record reviews, structured observations and interview (Creswell 2009).

We used an online software surveygizmo (McDaniel n.d.) to create a web based survey. We designed a webpage for own questionnaire and administered it online. Online survey is helpful both for administrators and respondents due to its convenience, availability and cost. We also sent survey MSWord document to some respondents.

4.4 Questionnaire

In survey the questionnaire is a reasonable way to gather data. A well-designed questionnaire could be utilized effectively to collect information on specific research area.

4.4.1 Conduction of Questionnaire

This chapter explains the questionnaire that we had conducted with eight different people related to health care like physical therapist, project-coordinator, clinical and research administration in different divisions for our thesis. The planning of questionnaire is given in section 4.4.2, the section 4.4.3 describes the questionnaire design and section 4.4.4 identifies the questionnaire distribution. The selection of questionnaire is given in section 4.6.5 and questionnaire analysis in section 4.6.6.

4.4.2 Questionnaire Planning

After the conduction of interview we planned a questionnaire for distribution among a selection of people related to healthcare but not experts on technology or security. We wanted to explore attitudes among employees in the healthcare organization. We could not conduct a large survey, as there were problems of gaining access to respondents. In this situation, we chose a small selection of different people working in healthcare but not experts on technology of security. We wanted to explore attitudes among employees in the healthcare organization. The questionnaire purpose was to gain insight into the healthcare system. Our questionnaire was heavily relying on closed ended questions. For a successful conduction of questionnaire we sent survey questionnaires to people who are closely related to healthcare systems. In questionnaire authors raised questions concerning privacy, security cost, and user satisfaction issues related to biometrics technology implementation with people working within healthcare systems. Once the questionnaires were completed then statistical analysis was performed to analyze the end results of questionnaires.

4.4.3 Questionnaire Design

After collecting the observations from the interviews analysis and discussions with PhD students and our supervisor, authors designed the questionnaire. In designing the questionnaire authors emphasize on simplicity, easiness and easy to understand questionnaires to the people related to healthcare system. The survey questionnaire focused mainly on cost, privacy, security and user satisfactions issues.

4.4.4 Questionnaire Distribution

After designing the questionnaire it was distributed to a selection of people (physical therapist, project-coordinator, clinical and research administration in different divisions) related to healthcare system. Those people are experienced and well aware about healthcare systems that are selected for questionnaire conduction. We received a total of eight responses from selected people out of twelve. As an introduction, the reason of the questionnaire was explained to the people at the beginning of questionnaire conduction.

4.4.5 Selection of Questionnaire

We selected the questionnaire because it is economical and easy to manage regarding design time and further interpretation if we compare it with other data collection techniques. The questionnaires are low-cost to administer and good data collection techniques when money and other resources are limited. We can receive many responses against the online questionnaire in a few days and it is also easy to administer

as well as confidentiality can be easily maintain in self administer questionnaire. In our case, we also hasd the ambition to use triangulation of methods for data collection, which we acheived by using a combinition of interviews and survey via questionnaires.

4.4.6 Questionnaires Analysis

To get the concrete results, authors perform a quantitative analysis of questionnaires. Citizen‘s response against close ended and scaling questions is calculated and given in percentage in Appendix 2. Key facts are described below.

The first question addressed the respondent’s experience of working in healthcare.

How many years of working in Healthcare?

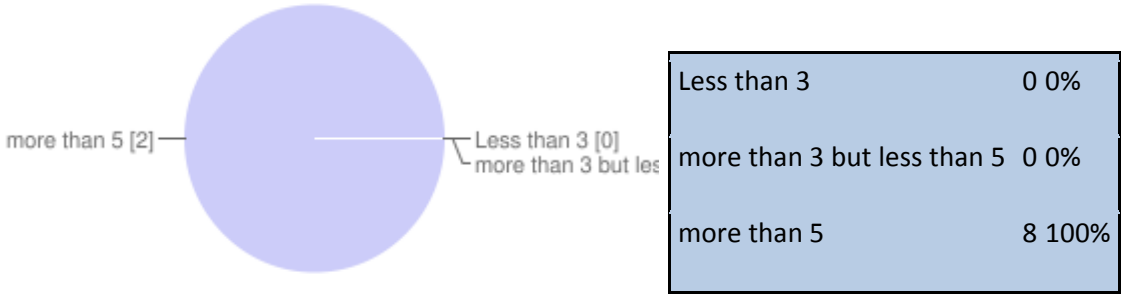


Figure 9-Working Exp-Survey

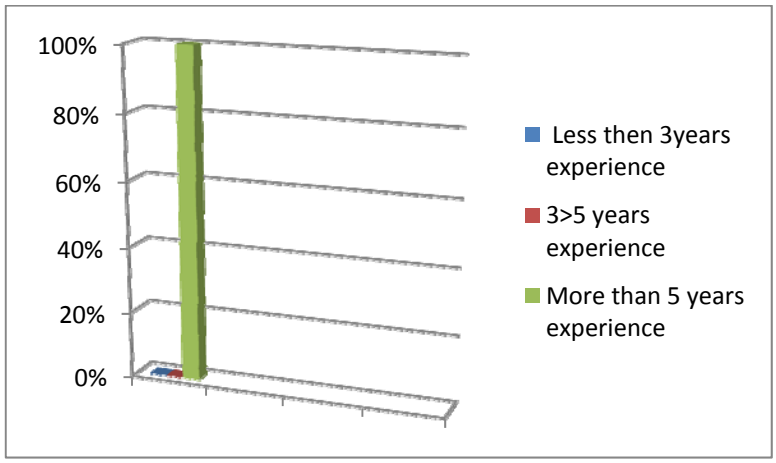


Figure 50. Working Exp-Graph

According to questionnaire findings all the respondents have more than 5 years experience as the aim of the questionnaire was to gain insight into conditions in healthcare, knowledgeable and experienced respondents should conceivably have a positive effect on the validity of the questionnaire results.

I feel that biometrics is secure.

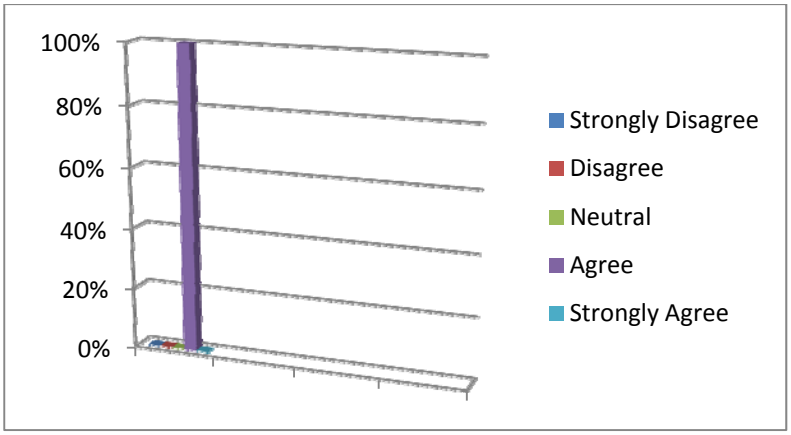


Figure 61-Biometric is Secure-Graph

All of the respondents agreed with the statement that biometrics is a secure way to communicate with healthcare system. This indicates that they have trust on biometrics system and in future they could conceive of facing changes the current system.

I have a privacy concern using biometric system (e.g., fingerprint verification, facial recognition, hand geometry verification, iris recognition, and voice verification).

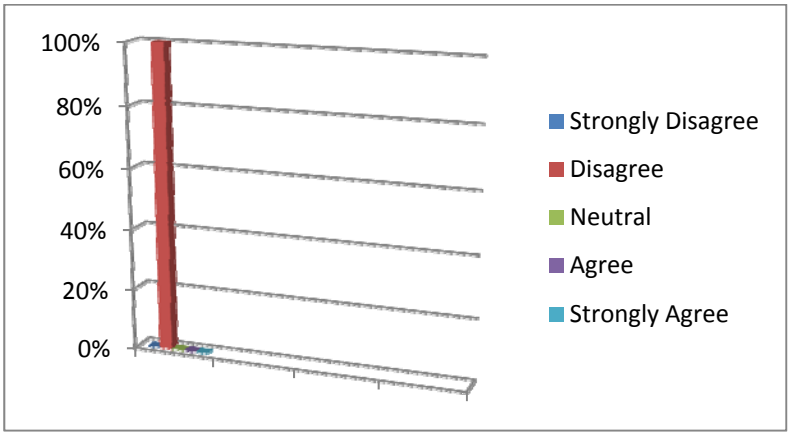


Figure 72-Privacy concern about Biometric Techology-Graph

The respondents all answered that they do not have privacy concern with the biometric system. This seems to indicate that there is awareness about biometrics systems and a willingness to accept such systems in healthcare.

Do you have worries that the disclosure of patient's health information may cause medical theft or abuse?

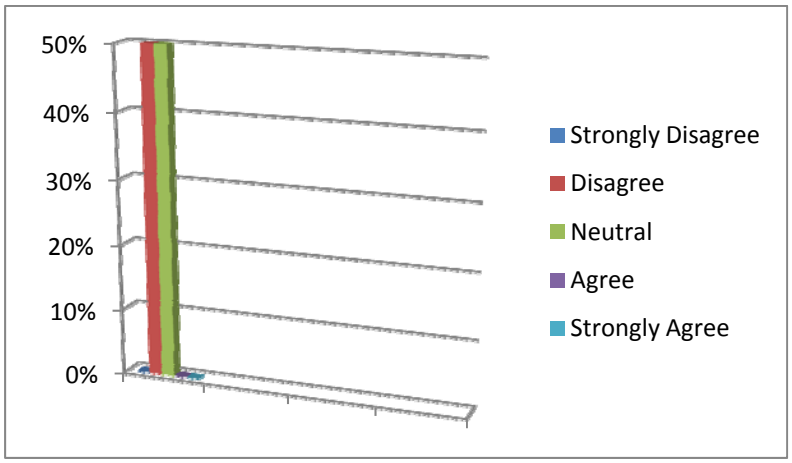


Figure 83-Healthcare Information and Medical theft

Of the eight respondents, four or 50% disagree with the statement that disclosure of patient's health information may result in medical theft or abuse and four or 50% have given a neutral response.

It is analyzed that half of the investigated people have confidence on their health information system privacy while the rest of the people have little doubt about the health information system privacy. This result indicates that there is fairly high trust in the privacy and security of the existing health information systems. However, it could also indicate a lack of awareness of threats to privacy and security in health information systems.

I feel that biometric technologies are more secure than traditional IT security methods

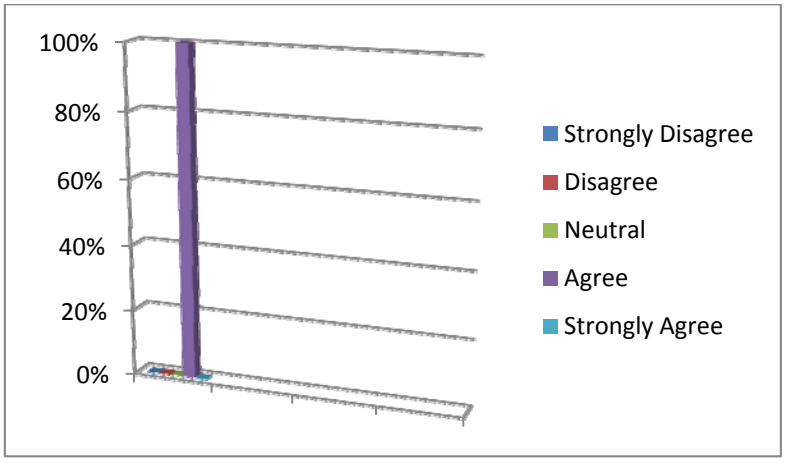


Figure 94-Biometric technology is more secure than traditional

All the respondents answered that they agree to the statement that biometric technologies are more secure than traditional IT security methods. Our conclusion is that majority of the people are already well aware about the advantages and disadvantages of biometric technologies and traditional IT security methods.

It will be a good change to replace passwords and ID Cards with biometrics technology?

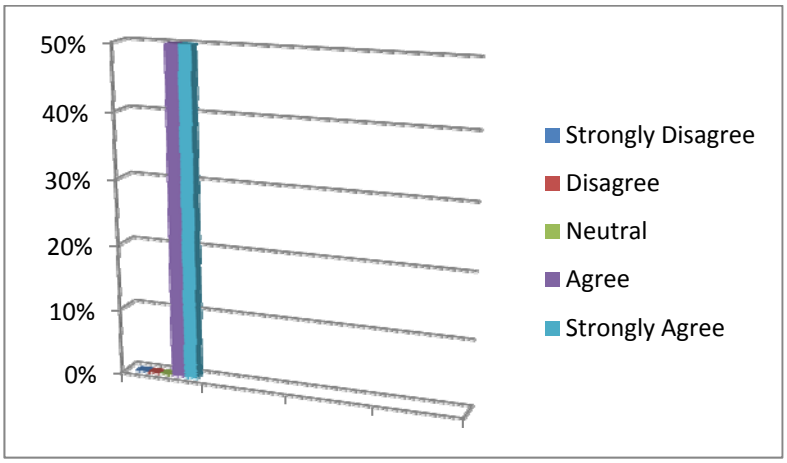


Figure 105-Password and ID cards replacement-Graph

50% strongly agree with the statement that It would be a good change to replace passwords and ID Cards with biometrics technology and 50% agree with this statement.

This seems to indicate that majority of the people are well aware of the biometrics implementation advantages and they are not satisfied with the passwords and ID Cards. Thus, the majority of the respondents have no objection and they are in favor of biometric technology implementation.

My organization needs biometric technologies to avoid medical theft and abuse?

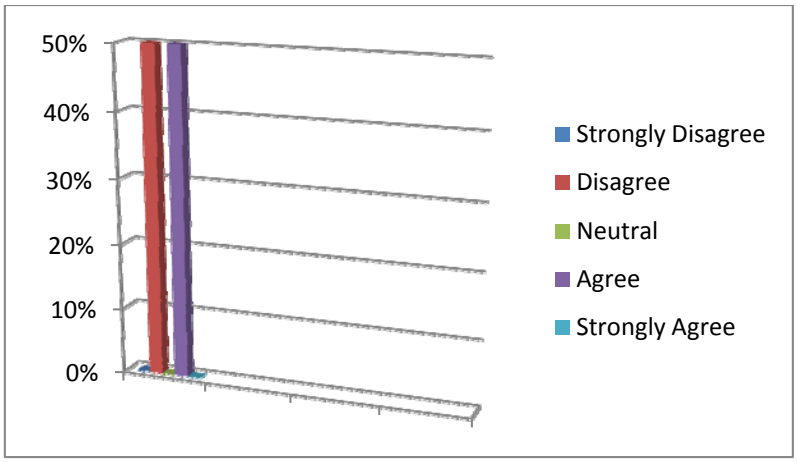


Figure 116-Biometric avoid Medical theft-Graph

Four respondents, or 50% agreed with the statement that their organization needs biometric technologies to avoid medical theft and abuse and on the other hand 50% disagree with the same statement.

Our conclusion here is that if half of the respondents believe there is a need of biometric technology to be implemented in their organization it could be because they trust the current system but they still need more secure technology to completely avoid medical theft and abuse. In addition to this, half of the people are satisfied that their current system is secure enough and it can prevent medical theft and abuse, it could be because they do not have awareness about the main advantages of biometric technology or it could be because they do not want to adopt the changes in the system.

My organization is concerned to secure Patient healthcare information?

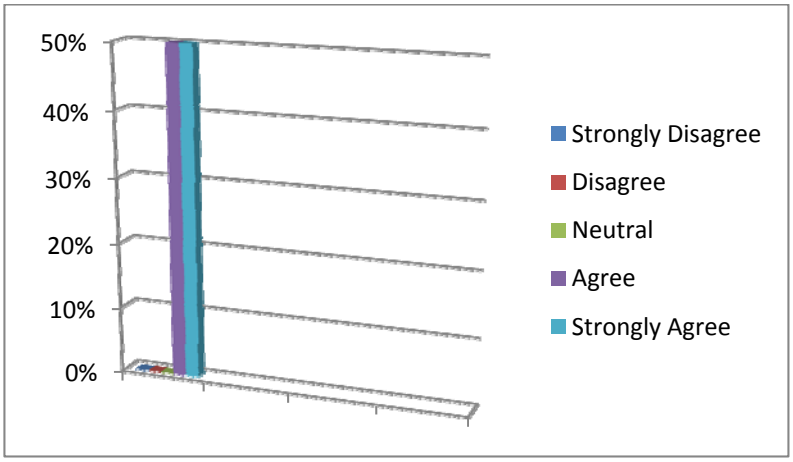


Figure 127-Securing Patient healthcare Information-Graph

All the respondents agreed that their organization is concerned to secure patient healthcare information. Healthcare organizations strongly want to avoid all kinds of medical theft and abuse.

I am willing to use biometric technologies to protect sensitive information in my organization.

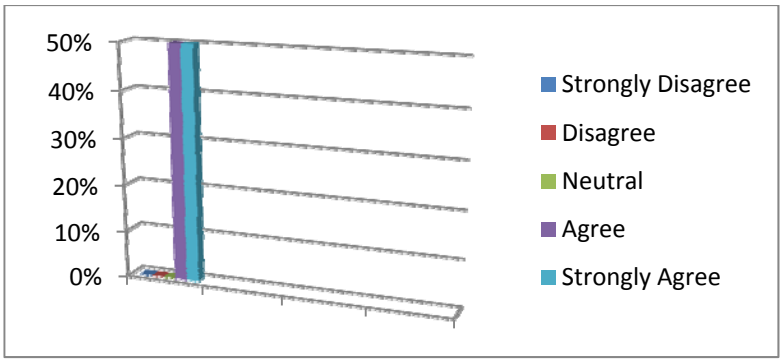


Figure 138-Biometric Technology to protect sensitive information-Graph

All the respondents were positive about using biometric technologies to protect sensitive information at their organization. It is analyzed that people would appreciate to adopt biometric technologies in the future in order to protect sensitive information at their organization.

Both technical staff and administration need to spread awareness for biometric technology in healthcare?

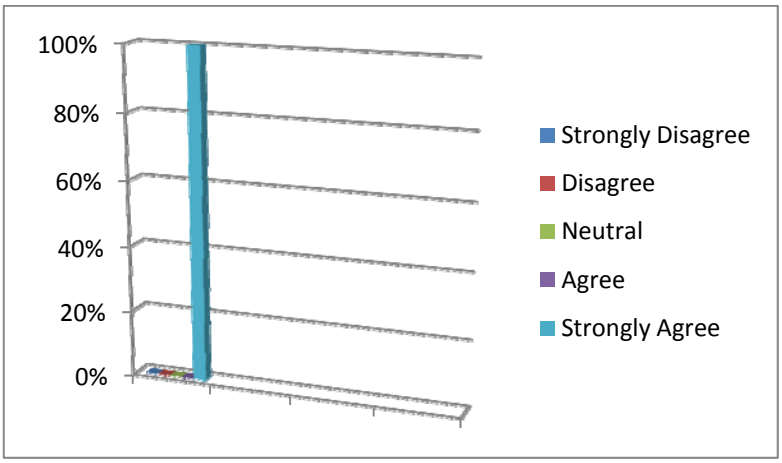


Figure 14-awareness about biometric technology

All of the respondents are agreed that both technical staff and administration need to spread awareness for biometric technology in healthcare. We conclude that there is strong need to spread awareness for biometric technology in healthcare.

Biometric technologies are available in reasonable cost with respect to its outcomes.

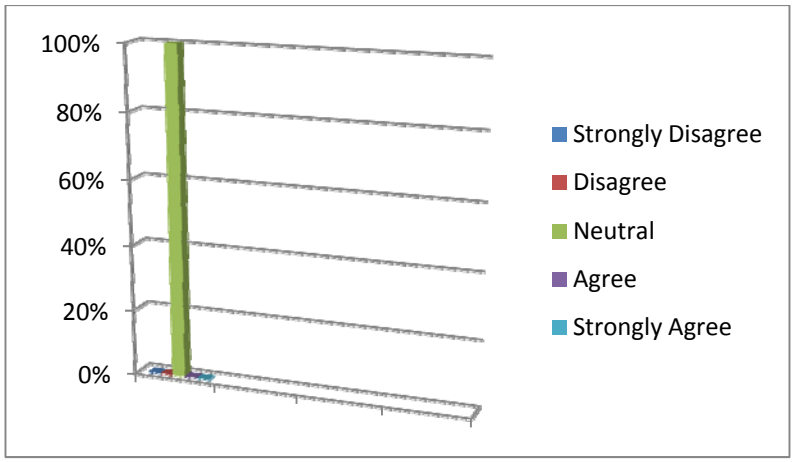


Figure 150-Biometric Technology in reasonable Cost-Graph

The respondents all gave a neutral response concerning the statement that biometric technologies are available at reasonable cost with respect to outcomes. Our conclusion is that the respondents do not have any knowledge regarding the implementation cost of biometrics technology with respect to its outcomes and that lack of cost awareness might a factor influencing attitudes towards implementation of biometrics in healthcare.

The maintenance cost is lower with biometric technologies than with traditional IT security methods.

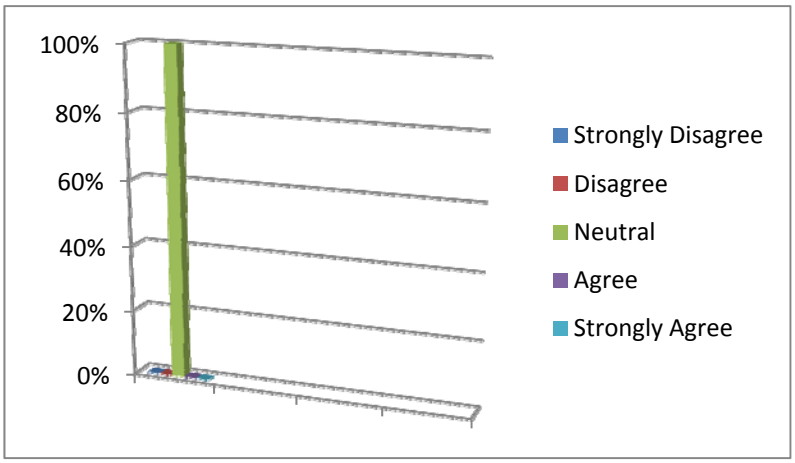


Figure 161-Maitenance Cost compared Traditional IT sec. Methods-Graph

Here again we have deliberately posed a leading question which has given a neutral response from all the respondents. Our conclusion is that many people working in healthcare organizations do not have any awareness/knowledge regarding the maintenance cost of biometrics technology with respect to maintenance cost of traditional IT security methods. From a provider's perspective, this would indicate that there is a need to spread awareness about the cost advantages of biometric technology maintenance as compared to traditional IT security methods.

I would consider biometric technologies to have considerable cost savings over traditional IT security methods.

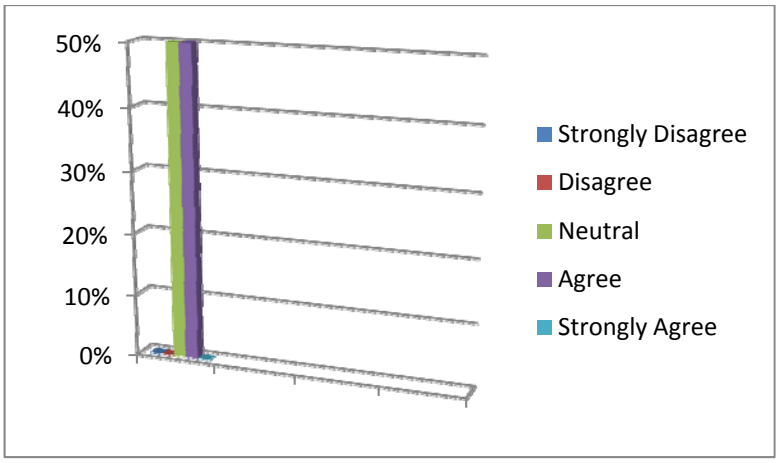


Figure 172-Biometric as Cost Saving-Graph

Half of the respondents agreed that they would consider biometric technologies to have considerable cost savings over traditional IT security methods and half of the respondents have given a neutral response. This would seem to indicate that there is a need to spread awareness about the cost saving advantages of biometric technology over traditional IT security methods, both from a provider's perspective and from a management perspective within healthcare organizations, if there is an ambition from management to implement biometric technologies in healthcare.

I would feel comfortable recommending biometric technologies in my organization.

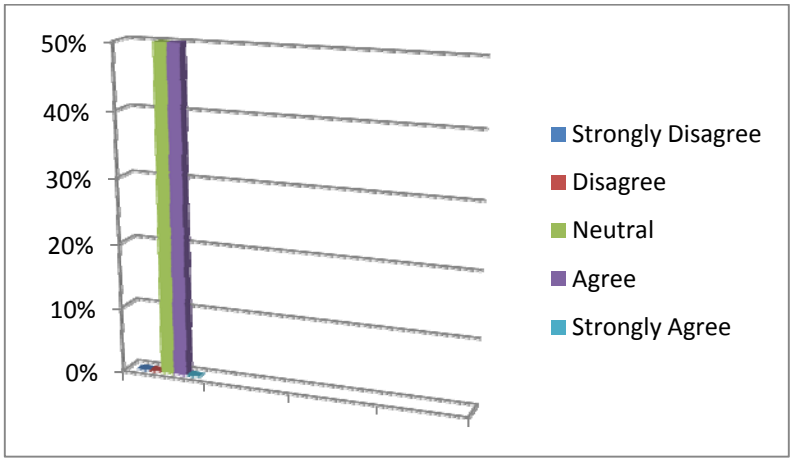


Figure 183-Biometric Recommendation-Graph

Half of the respondents agreed that they would feel comfortable recommending biometric technologies in organization and half of the respondents have neutral response. Our conclusion is, from these replies, that there is a need to spread awareness about the advantages of biometric technology over traditional IT

security methods, if the long-term strategy includes the implementation of biometrics technology in the healthcare organizations.

5 Discussion

5.1 User Acceptance

The results of our study seem to indicate that people within the healthcare organization in Blekinge have trust in biometrics systems and would be willing to face a change of the current system. Also the results imply that people who are related with healthcare system are already aware about biometrics and they will adopt the implementation of biometric system in healthcare if such a strategy is decided upon. It is observed that there is need of improvement of the existing healthcare system. It is identified that majority of the people are well aware of the biometrics implementation advantages and that they trust the current system but they still see a more secure technology to avoid medical theft and abuse. It seems very likely that healthcare organizations could adopt changes in the future in order to secure their systems. In addition it is observed that majority of the people do not have any knowledge regarding the cost advantage of biometrics technology with respect to its outcomes and there is a need to spread awareness about the cost advantages (implementation and maintenance) of biometric technology implementation to increase the user acceptance, if the long-term aim is to successfully implement biometrics technology in healthcare.

5.2 Implementation Issues

Authors conclude that it is necessary to conduct a study in order to analyze the requirements of different actors that will participate in biometrics systems. It is considerable that during the implementation of biometrics we must focus the interests of all actors (patients, healthcare staff and healthcare providers). According to authors observations there are still many areas that need to be explored i.e. the limitations and restrictions in different environments where the biometric devices are expected to be implemented. Authors identified that most important pre-requisite for the implementation of biometrics in healthcare is that the healthcare systems records must be 100% electronic.

After analysis, the interview data and survey questionnaires, author identified that respondents related to healthcare are mainly positive toward the implementation of biometrics in healthcare and they have knowledge about the biometrics implementation with respect to its attributes. Authors observed that for cost benefit advantage in the initial implementation stages the finger print technology could be a better selection as compared to other available biometric technologies. According to authors observations for successful implementation of biometric technology, the biometric system must be error free so that it will increase the acceptance rate.

5.3 Cost

According to authors observations the cost is the main factor affecting the decision about the implementation of biometrics system in healthcare. For security reasons a good combination could be ID card with fingerprint and/or face image. In addition to this, the maintenance cost could also affect the adoption of biometric technology in healthcare. After the implementation, any failure of the biometric system and maintenance cost is also a big challenge. It is observed that to avoid the high maintenance cost there is a need to educate and train people, also biometric devices must follow standards to increase interoperability.

According to the providers of the technology, biometrics will enhance the possibilities to ensure the right identity of people and provide adaptable procedures for biometric users as well as increase the security

and decrease the cost associated with traditional password management. Authors identified that the issue related to ROI (Return on investment) must be considered along with the increase in security that we will get from using biometrics solutions. Authors analyzed that the economical aspect also plays a role in the implementation of biometrics but it shouldn't be as focused when it comes to a matter of privacy and security of clients/patient data. The study indicated that there is a need to train people before they will use the biometric system because sometimes a minor mistake could cost very high. Our result imply that cost would be the most important factor determining choice of technology for identification/authorization, although privacy and security issues would also influence the decision.

5.4 Security

Based on interviews and survey analysis authors observed that people related to healthcare system show trust in their system and they think that there is no risk of medical identity fraud, theft and abuse in the current healthcare environment in Sweden. On the other hand authors identified that there are many considerable reasons that biometrics could be implemented in healthcare. At present there are many highly secure authentication devices related to biometrics available that could secure data in best possible way. Authors analyzed that due to the threats and challenges to traditional password schemes there is an interest in enhancing security by implementing biometrics systems. Authors identified that biometric could provide many benefits in sense of providing security and securing access to right information from different heath care locations. There is a need to focus on taking appropriate measures to secure the sensitive data as much as possible.

To increase the security the biometric system could be combined with password system. Almost all health care organizations have electronic systems but still some places use physical keys. In healthcare organizations in Blekinge, the electronic system is based on plastic cards with a magnetic strip combined with a PIN code. The combination of smart card with biometrics could provide sense of security to cardholder regarding his/her own sensitive medical data as well as concerning access to physical locations.

5.5 Government Legislations

According to authors observation the main influencing factors to deploy biometric in healthcare are Governmental legislation, healthcare admin costs and faster move to electronic healthcare records. The HSA (Healtcare sector Adressregister, http://www.inera.se/Infrastrukturtjanster/HSA) is the foundation of all healthcare informatics communication nationwide in Sweden. In HSA there are a lot of regulations and policies involved for different parties coordinating with each other.
According to authors observations for biometrics implementation there is a need of new legislation as the security measures are going to be much higher as compared to the traditional password systems. On the other hand The National Healthcare security policy and legislations puts a considerable emphasis on the importance of building customer(s) trust. Authors conclude that the government legislation will push healthcare providers toward using biometrics technology in a variety of ways for securing patient data.

5.6 Privacy

As legislation and security issues are increasingly driving the need for stronger authentication, and biometric technology today provides the most secure solution, it seems that biometrics could provide advantages to patients, healthcare staff and healthcare providers. Without compromising privacy and security the combination of smart card with biometrics could provide considerable advantages in sense of

ease of use, speed of transaction, and ease of personal use. Our literature study, interviews and survey in combination indicate that security and privacy issues in healthcare organizations regarding patients/clients data the government legislation will push healthcare providers towards using biometrics technology, as the security cannot be assured with user ID and password in public places.

6 Validity Threats

6.1 Validity Threats

Validity assessment is an important part of any research work. By identifying validity threats and addressing them in the choice and application of research methods, this risk can be minimized. There are four criteria for judging the validity of the qualitative research: credibility, dependability, transferability, and conformability proposed by Guba and Lincoln.

6.1.1 Credibility

The criteria for evaluating results tell authors about the findings that are found in this report are showing truthfulness of this system (Guba and Lincoln 2006). We selected five interviewees from biometric companies to express their experiences, opinions and domain knowledge about the implementation of biometrics system, with a special focus on the healthcare system in the county of Blekinge. The questionnaire (survey) was conducted with eight different people related to healthcare like physical therapist, project-coordinator, clinical and research administration in different divisions of the healthcare organization of the county of Blekinge. We adopted Methodological triangulation, to check the validity of their findings by cross-checking survey together with interviews as a way of mapping attitudes towards biometrics in healthcare.

6.1.2 Dependability

According to Lincoln & Guba, it means occurring of changing in the context of research over time affects the results. It is the duty of the researcher to identify the context and their effects on research.

The authors achieved dependability by selecting the interviewees from the domains of biometrics industry and healthcare organizations and selecting interviewees who are aware of and knowledgeable about biometrics technologies. Also the survey respondents were selected from people of different designation in healthcare system. The questionnaire results may affect the result of this research if this questionnaire is conducted with citizens having different gender, educational and cultural backgrounds.

6.1.3 Transferability

According to Lincoln & Guba, it can be accomplished by describing and identifying the context of the research being performed and the assumptions that were consider for the study. It refer that results obtained from that research are applicable in other contexts.

In case of this thesis, if we want to use these results for some other parts of counties of Sweden then the results can be generalized to their domain because the implementation of biometrics technology in all over Sweden is in starting phase and the healthcare sector in Sweden is organized in a similar way all over the country.

6.1.4 Conformability

According to Lincoln & Guba, Conformability means the degree in which results could be confirmed by other researchers. It refers that the outcomes from the research are the result of the participant‘s bias, inspiration or motivation rather than that of researchers.

To attain thesis conformability, each interview is converted into the text format and then separated into sections for comparisons and analysis purpose. All survey questionnaire answers were also separated into sections for comparison.

7 Conclusion

Authors performed a literature study to get information about the subject area. Later on, interviews were conducted for collecting data from companies and from key actors in the Blekinge healthcare organizations. Interview questions based on the strategy to gain a deep understanding about company‘s point of view about biometrics and to identify, why healthcare organizations are not ready to invest more in biometrics technology and on the other hand to gain insight in to strategies and attitudes in the healthcare organizations concerning biometrics technology. Authors used survey as a strategy for inquiry and used questionnaires for data collection. The questionnaires were conducted with different people related to healthcare to judge the factors such as ease of use, privacy, cost, user acceptance, and required security level. Authors performed triangulation method and used survey together with interviews as a way of mapping attitudes towards biometrics in healthcare.

7.1 User Acceptance

Concerning user acceptance, our study showed that our respondents have trust in biometrics system and in future are willing to face changing the current system. In addition the people who are related with health care system are already aware about biometrics and they will adopt the implementation of biometric system in healthcare. It is identified that majority of the people we asked, trust the current system but they still need more secure technology to completely avoid medical theft and abuse. In addition it is observed that there is a strong need to spread the awareness about the cost advantages (implementation and maintenance) of biometric technology implementation to increase the user acceptance. According to questionnaires responses all respondents agreed with the statement that biometric is a secure way to communicate with healthcare system. They have trust on biometrics system and in future they are agreed to face changing in the current system.

7.2 Implementation Issues

In concern of implementation issues during interviews authors analyzed that it is necessary to conduct a study in order to analyze the requirement of different actors that will participate in biometrics systems. It is considerable that during the implementation of biometrics we must focus the interests of all actors (patients, healthcare staff and healthcare providers). Authors identified that the healthcare system records must be 100% electronic because it is the most prior pre-requisite for biometric implementation. According to questionnaires responses all survey respondents who are related to healthcare system are already aware about biometrics and all survey respondents will easily adopt the implementation of biometric system in healthcare. Moreover during questionnaires authors analyzed that for a successful implementation of biometrics in healthcare, both technical staff and administration needs to spread awareness for biometric technology in healthcare.

7.2.1 Cost

In concern of cost during interviews authors analyzed that for cost benefit advantage at initial biometric implementation stages finger print technology could be a better selection as compared to other available biometric technologies. Not only implementation cost but also the maintenance cost could affect the adoption of biometric technology in healthcare. There is also a need of interoperability among biometric technology based devices and they must follow some standards therefore it will decrease the update cost

of biometric systems. According to questionnaires responses all respondents have neutral response that biometric technologies are available in reasonable cost with respect to its outcomes.

7.2.2 Security

In concern of security during interviews authors analyzed that there are strong reasons for biometrics to be implemented because there are many secure authentication devices related to biometrics are available in the market that could secure data in best possible way. Due to the threats and challenges to traditional password schemes there is strong need of biometrics to be implemented. The biometric could provide many benefits in sense of providing security, access to right information and access to data from different locations. Biometrics would be most feasible to implement on entry clearance points. According to questionnaires responses all respondents agreed on the statement that biometric technologies are more secure than traditional IT security methods. All questionnaire respondents are strongly agreed that it will be a good change to replace passwords and ID Cards with biometrics technology. After questionnaires responses, it concludes that healthcare organizations strongly want to avoid all kinds of medical theft and abuse and there are high possibilities that healthcare organizations could adopt changes in the future in order to secure their systems.

7.2.3 Government Legislation

Authors observed that there is a need of legislation for biometrics as the security measures are going to be much higher as compared to the traditional password systems. The National healthcare security policy and legislation is important to build customer trust. The government legislation would push healthcare providers toward using the biometrics technology in a variety of ways for safeguarding patient.

7.2.4 Privacy

In concern of privacy authors observed during interviews that healthcare organizations are demanding strong authentication and focus on suggesting biometrics because biometrics could provide advantages to patients, healthcare staff and healthcare providers. The combination of smart card with biometrics could provide considerable advantages in sense of ease of use, speed of transaction, personal use without compromising privacy and security. There is a need of biometrics technology as the security cannot be assured with user ID and password in public places.

According to questionnaires responses all respondents do not have privacy concern using biometric system. Moreover in questionnaires responses it is analyzed that half of the respondents have confidence on the privacy of their current healthcare information systems and on the other hand half of the respondents have little doubt about the privacy of their current health information system.

8 Recommendations

8.1 User Acceptance Issues

Recommendations:

- Both technical and administrative staff needs to spread awareness for Biometric technology in healthcare.
- There is a strong need to spread the awareness about the cost advantages of biometric technology implementation.
- There is a strong need to spread awareness about cost advantages of biometric technology maintenance as compared to traditional IT security methods.
- For successful implementation of biometric technology the biometric system must be error free so that it will increase the acceptance rate.

8.2 Implementation Issues

Recommendations:

- It is very necessary to conduct a study in order to analyze the requirement of different actors that will participate in biometrics systems.
- It is considerable that during the implementation of biometrics we must focus the interests of all actors (Patients, healthcare staff and. healthcare providers).
- Authors analyzed that it is very necessary to conduct a study in order to analyze the requirement of different actors that will participate in biometrics systems.
- There are still many areas needs to be explored i.e. the limitations and restrictions in different environments where the biometric devices expected to be implemented.
- Authors identified that the healthcare system records must be 100% electronic because it is the most prior pre-requisite for biometric implementation.
- For cost benefit advantage in the initial implementation stages the finger print technology could be a better selection as compared to other available biometric technologies.

8.3 Cost Issues

Recommendations

- It is observed that to avoid the high maintenance cost there is a need to educate people.
- All biometric devices must follow some standards to increase interoperability.
- To gain the cost benefit in initial stages a good combination could be ID card with fingerprint and/or face image.
- Authors analyzed that the economical aspects also plays a role in the implementation of biometrics but it shouldn’t be as focused when it comes to a matter of privacy and security of clients/patient data.

8.4 Security Issues

Recommendations

- The authors identified that there are many considerable reasons that biometrics could be implemented in healthcare. At present there are many highly secure authentication devices related to biometrics are available that could secure data in best possible way.

- Authors analyzed that due to the threats and challenges to traditional password schemes there is strong needs of biometrics to be implemented.
- Authors identified that biometric could provide many benefits in sense of providing security, access to right information from different heath care locations.
- According to authors the biometrics would be most feasible solution to implement on entry clearance points.
- The combination of smart card with biometrics could provide sense of security to cardholder regarding his/her own sensitive medical data.
- According to author observation to increase the security the biometric system could combine with password system.

8.5 Government Legislations Issues

Recommendation

- According to authors observations for biometrics implementation there is a need of new legislations as the security measures are going to be much higher as compared to the traditional password systems.
- The National healthcare security policy and legislations is also considerable to build the customer trust.
- Authors analyzed that the government legislation can push healthcare providers toward to use biometrics technology in a variety of ways for securing patient data.

8.6 Privacy Issues

Recommendations

- Authors analyzed that organizations are demanding strong authentication and biometrics could provide advantages to patients, healthcare staff and healthcare providers.
- Authors analyzed that without compromising privacy and security the combination of smart card with biometrics could provide considerable advantages in sense of ease of use, speed of transaction, and personal use.
- According to Authors analysis as the security cannot be assured with user ID and password in public places so biometrics technology implementation would be a good step.

9 Future Work

In our study, we have identified some of the main issues and challenges that need to be addressed in order to implement biometrics technology successfully in the healthcare sector in Sweden.

One area for future research work would be to carry out a more extensive stakeholder analysis in this area, as it is obvious that there are different perspectives concerning cost and benefit analysis for biometrics technology in this domain. We also argue that there is a need to conduct a more extensive study in order to analyze the requirements of different actors (patients, healthcare staff and healthcare providers) that would be affected by and participate in the use of biometrics systems.

- In a broader perspective on biometric technology, there are still many areas (banking, immigration etc.) which need to be explored concerning limitations and restrictions in different environments where biometric devices are expected to be implemented.
- There is also a need for research in to on-going standardization in this area, as standardization is necessary for ensuring the interoperability among biometric devices which in turn is necessary to make biometrics a worthwhile investment for healthcare providers.
- There is need to develop better algorithms in order to minimize FAR and FRR.
- There is further a need to conduct in-depth studies on adoption of biometrics regarding technical aspects

REFERENCES

Allan, R., 2005. Biometrics Wields a Double-Edged Sword. *Electronic Design*, 53(14), 77-81.

Atkins, W., 2000. A bill of health for biometrics? *Biometric Technology Today*, 8(9), 8-11.

Bender, P., 2005. Biometrics is important tool for HIPAA compliance. *Biometric Technology Today*, 13(4), 3.

Bolle, R.M. et al., 2004. *Guide to Biometrics*, New York: Springer-Verlag. Available at: http://books.google.com/books?id=NTJle3OodUsC&lpg=PR13&ots=1ZRWCbWaSA&dq=Guide%20to%20Biometrics.%20SpringerVerlag%2C%20New%20York&lr&pg=PR29#v=onepage&q=Guide%20to%20Biometrics.%20Springer-Verlag,%20New%20York&f=false.

Bryman, A., Triangulation. Available at: http://referenceworld.com/sage/socialscience/triangulation.pdf [Accessed 01 Jan 2011]

Beefing up security with biometrics, 2008 *Card Technology Today*, 20(5), 14-15.

Chandra, A. & Calderon, T., 2005. Challenges and constraints to the diffusion of biometrics in information systems. *Commun. ACM*, 48(12), 101-106.

Chandra, A., Durand, R. & Weaver, S., 2008. The uses and potential of biometrics in health care Are consumers and providers ready for it? *International Journal of Pharmaceutical and Healthcare Marketing*, 2(1), 22 - 34.

Chellappa, R., Wilson, C. & Sirohey, S., 1995. Human and machine recognition of faces: a survey. *Proceedings of the IEEE*, 83(5), 705-741.

Creswell, J., 2009. *Research design: Qualitative, quantitative, and mixed methods approaches* 2nd ed., California: Sage Publications, Inc.

Dawson, C., 2005. *Projects in Computing & Information Systems: A Students Guide*,

Dixon, P., 2006. Medical identity theft: the information crime that can kill you. *The World Privacy Forum*.

Donos, P. & Zorkadis, V., 2004. On biometrics-based authentication and identification from a privacy-protective perspective. *Information Management & Computer Security*, 12(1), 125-137.

Dwivedi, A. et al., 2003. Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on. In Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on. pp. 114-117.

Faundez-Zanuy, M., 2006. Biometric security technology. *Aerospace and Electronic Systems Magazine, IEEE*, 21(6), 15-26.

Forte, D., 2003. Biometrics: Future Abuses. *Computer Fraud & Security*, 2003(10), 12-14.

Gates, M., 2007. Biometrics—passing on using passwords. *Radiol Today*, 8(17), 28–31.

Guba, Lincoln, (2006), Guba's and Lincoln Evaluation Criteria, http://www.qualres.org/HomeLinc-3684.html. [Accessed 24 Nov 2010]

Hagen, S., 2003. Healthcare industry prescribes use of biometrics.

Hazzan, O. et al., 2006. Qualitative research in computer science education. *SIGCSE Bull.*, 38(1), 408-412.

Independent Biometrics Expertise. *International Biometric Group*. 2010, Available at: http://www.biometricgroup.com/ [Accessed November 17, 2010].

Jain, A., Ross, A. & Prabhakar, S., 2004. An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1), 4-20.

Keener, R.E., 2000. Put Your Finger on the Right Solution. *Health Management Technology*, 21(12), 20.

Khushk, K. & Iqbal, A., 2005. An Overview of Leading Biometrics Technologies Used for Human Identity. In Engineering Sciences and Technology, 2005. SCONEST 2005. Student Conference on. pp. 1-4.

Krawczyk, S. & Jain, A.K., 2005. 5th International Conference on Audio - and Video-Based Biometric Person Authentication, AVBPA 2005, July 20, 2005 - July 22, 2005. In Lecture Notes in Computer Science. Hilton Rye Town, NY, United states: Springer Verlag, pp. 1110-1119.

Liu, S. & Silverman, M., 2001. A practical guide to biometric security technology. *IT Professional*, 3(1), 27-32.

Marohn, D., 2006. Biometrics in healthcare. *Biometric Technology Today*, 14(9), 9-11.

McDaniel, S., Online Survey & Questionnaire Software - Web Survey Tool - SurveyGizmo.com. Available at: http://www.surveygizmo.com/ [Accessed December 11, 2010].

Mordini, E. & Ottolini, C., 2007. Body identification, biometrics and medicine: ethical and social considerations. *Annali dell'Istituto Superiore di Sanita*, 43(1), 51-60.

Messmer, E. (2004), "Healthcare looks to biometrics", *Networkworld*, December, available at: www.networkworld.com

Nielsen, J., 1993. *Usability Engineering*, Academic Press.

Norton, R., 2000. HIPPA creates healthy opportunity for biometrics. *Biometric Technology Today*,9(1), 5.

National strategy for eHealth Sweden, 2007. Available at: http://www.regeringen.se/content/1/c6/06/43/24/f6405a1c.pdf [Accessed 02 Sep 2009].

O'Gorman, L., 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12), 2021-40.

Panpan Li & Renjin Zhang, 2010. The evolution of biometrics. In 2010 International Conference on Anti-Counterfeiting, Security and Identification (2010 ASID). Piscataway, NJ, USA: IEEE, pp. 253-6. Available at: http://dx.doi.org/10.1109/ICASID.2010.5551405.

Peck, B., 2003. Rx for Password Headaches; Biometric authentication solution lets physicians be their passwords. *Health management Technology*.

Perrin, R., 2002. Biometrics technology adds innovation to healthcare organization security systems. *Healthcare Financial Management*, 56(3), 86-8.

Pehrsson, T., 2010. IT-Strategist at the County Council Blekinge, Wämo Center Karlskrona, Blekinge County – Sweden.

Rakesh Agrawal & Christopher Johnson, 2007. Securing electronic health records without impeding the flow of information. *International journal of medical informatics*, 76(5), 471-479.

Ratha, N.K., Connell, J.H. & Bolle, R.M., 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM SYSTEMS JOURNAL*, 40(31).

Richardson, R., 2003. Computer Crime and Security Survey. *Computer Security Institute*, Eighth Annual. Available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf.

Rogers, E.M., 1995. *Diffusion of innovations* 4th ed., New York NY 10020: The Free Press. Available at: http://books.google.com/books?id=v1ii4QsB7jIC&lpg=PR15&ots=DI-qxIYrdO&dq=Rogers%2C%20E.%20M.%20(1995).%20Diffusion%20of%20Innovation&lr&pg=PR15#v=onepage&q=Rogers,%20E.%20M.%20(1995).%20Diffusion%20of%20Innovation&f=false.

Schneier, B., 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems* 2nd ed., Wiley, New York. Available at: http://www.researchandmarkets.com/reports/600772/.

Seaman, C., 1999. Qualitative methods in empirical studies of software engineering. *Software Engineering, IEEE Transactions on*, 25(4), 557-572.

Simon de Lusignan et al., 2007. The roles of policy and professionalism in the protection of processed clinical data: A literature review. *International journal of medical informatics*, 76(4), 261-268.

Stamp, M., 2006. *Information security: principles and practice*, John Wiley & Sons, Inc. Available at: http://books.google.com/books?id=Bh45pU0_E_4C&lpg=PR15&ots=b98RQ08o MR&dq=Information%20Security%3A%20principles%20and%20practice&lr&pg=PR15#v=one page&q&f=false.

Trocchia, P.J. & Ainscough, T.L., 2006. Characterizing consumer concerns about identification technology. *International Journal of Retail & Distribution Management*, 34(8), 609-620.

Turk, M. & Pentland, A., 1991. Eigenfaces for Recognition. *Journal of Cognitive Neuroscience*, 3(1), 71-86.

Vijayan, J., 2004. Corporate America Slow to Adopt Biometric Technologies. , 38(32), 1-2.

Weicheng Shen, Khanna, R. & Woodward, J., 1997. Prolog To Biometrics: Privacy's Foe Or Privacy's Friend? *Proceedings of the IEEE*, 85(9), 1479.

Win, K., Susilo, W. & Mu, Y., 2006. Personal Health Record Systems and Their Security Protection. *Journal of Medical Systems*, 30(4), 309-315.

Wiskott, L. et al., 1997. Face recognition by elastic bunch graph matching. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(7), 775-779.

Wahlgren, U., 2010. IT-Security, Project Manager, Wämo Center Karlskrona, Blekinge county – Sweden.

Yadan Li & Xu Xu, 2009. Revolutionary Information System Application in Biometrics. In Networking and Digital Society, 2009. ICNDS '09. International Conference on. pp. 297-300.

Yong Nyuo Shin et al., 2008. Designing Fingerprint-Recognition-Based Access Control for Electronic Medical Records Systems. In *Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on*. Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on. pp. 106-110.

Yun, Y.W., 2002. The ‘123’ of Biometric Technology. *Biometrics Working Group of Security & Privacy Standards Technical Committee*, 80-96.

Zuniga, A.E., Win, K.T. & Susilo, W., 2009. Biometrics for Electronic Health Records. *J Med Syst*.

APPENDIX

Appendix A

Søren K. Lauritzen,
Business Manager/Partner
IT2TRUST A/S
Roskildevej 522
2605 Brøndby, DANMARK

In your opinion biometrics should be implemented in healthcare? YES or NO. If No explain why? If Yes explain why?

According to Soren the biometrics company representative there are many reasons the biometrics to be to be implemented fingerprint scanners is a very secure way of authenticating users and at the same time easy to use. All users carry their identification with them at all times and it is close to impossible to "steal" this identification method. Furthermore, the healthcare organizations have access to a lot of sensitive data on their patients and it is important to make sure these data are secured in the best possible way.

Which are the specific areas facing security threats within healthcare that demand the implementation of biometrics?

Interviewee explained there are threats and challenges that force the implementation of biometrics. The security threats are It is very easy for the "wrong" people to get access to systems, networks, computers if these are only protected by a simple user id/password system – especially if the "right" users also have a lot of different systems where they need to validate themselves with user ids/password, as they tend to either create their own password-synchronization tool and/or write down their passwords on handy notes.
According to her the privacy threats are healthcare organizations user a lot of very sensitive data about their clients/patients and this information can be useful for people outside these environments (for example for use for blackmail, tabloid stories, employment issues and fraud in general) and it is therefore important that the privacy of the clients/patients is protected in the best possible way.

Interviewee identified that organizations are demanding strong authentication because the healthcare industry involves a lot of sensitive data that has to be available only to the relevant people and you need to make sure only these people can get access to the sensitive information – but you also need the information to be available to sometimes many different people with short intervals (local doctor, hospital doctor, nurse, surgeon and so on). She explained that the organizations are suggesting biometrics because Digital Personal Fingerprint readers as a means of Biometric authentication are fast, reliable and most of all secure and hence providing the healthcare organizations with the strong authentication needed to secure sensitive information.

Do you think current biometrics solutions can fulfill the requirements of healthcare regarding privacy and security of patient's record?

Yes. And Digital Persona already has several customers in the healthcare sector utilizing their solution to secure the privacy of patient's records (some official references are listed here: http://digitalpersona.com/biometrics/solutions/healthcare/).

How do you define ROI (Return on investment) in context of biometrics in healthcare?

Not an easy task. Apart from the increased security you get from using a Biometric solution the following issues should be considered and taken into account when evaluating: less time wasted on password reset (both for IT personnel and medical employees (doctors, nurses and so on)); faster and easier access to the relevant information/systems as the employee just have to scan a finger to be authenticated. Digital Persona can provide both the fast and reliable fingerprint reader and the centralized management system to handle all the users.

What do you think about costs of the Biometric solution compared to card system?

It depends very much on what kind of system you want to use. For both solutions you would need some kind of centrally managed administrative platform to handle users and what they need access to – the cost of these admin systems needs to be compared of course and you need to make sure the systems can give the same administrative functionalities when comparing them. Then you need to compare the cost for hardware: fingerprint readers versus ID cards – usually you would only need maximum one reader per employee (sometimes even less as they might share computers), but you would definitely need at least one ID card per employee + some extra when they destroy, lose, forget their original ID cards and in that regards also calculate the added cost of time spent taking care of issuing new cards and so on. With DigitalPersona you have the possibility to take advantage of embedded/integrated swipe readers in many laptops which means you don't need separate fingerprint readers for these computers.

- Biometrics is considerably more expensive
- Biometrics is expensive
- Equal price
- Biometrics is cheaper
- Biometrics is considerably cheaper than card readers

In your opinion, what are the main influencing factors for Biometric deployment in healthcare organizations?

To increase security and provide easy and quick logon (and switching between users)

In your opinion, what could be the benefits in the deployment of biometrics?

Stronger security in regards to authentication of users and thereby giving them access to the right information; fast access to the relevant information and the possibility to take advantage of roaming users (i.e. access to data from different computers).

In your opinion, what are the main threats concerning implementing Biometric technology in healthcare organization?

Finding a solution that can be used across many different healthcare organizations (hospitals, clinics, private doctors and so on), administrating it and figuring out how to split the payment of such a solution; of course the economics in general for such a solution also plays a role, but in my opinion it shouldn't be as important as it is a matter of security and protecting privacy.

In your opinion, what are the factors that slow down/prevent the implementation of biometrics in healthcare?

The main factor is how to be able to use biometric solutions (fingerprint scanners) in sterile environments – if a surgeon wears plastic gloves during an operation it is difficult for that person to access patient records with the use of fingerprint scanning (but then again, it would also be less sterile if he/she needed to type in a user id/password or use an ID card solution that is also used outside the sterile environment).

In your opinion, will government legislations push healthcare providers towards using biometrics technology?

I am sure there will be much more focus on how sensitive information is both stored and accessed (and by whom) and also who has access to physical locations – but I also think that the use of government legislation may vary a lot from country to country and even within each country depending on how the government entity usually handles these issues.

In your opinion, can privacy and security be compromised with less additional cost? If yes, explain why? If no, explain why?

Privacy and security can always be compromised! It is impossible to be 100% secure no matter how much money you spend and how many different solutions you implement (hackers can get access to FBI, NASA and organizations like that and they spend a lot of money on security). However it is important to take appropriate measures to make it as difficult as possible to get access to the sensitive data and hence having the "bad guys" go somewhere else. Even with strong encryption on data and several biometric solutions together with smartcards and passwords there is always the possibility to force/threaten/pay somebody with the right access to deliver the needed information – the cyber criminals are always one step ahead unfortunately.

Give the priority level of three factors (cost, privacy, and security) in the adoption of biometrics in healthcare organizations with proper reasoning. 1..... 2.....3.....

Depends on who is measuring the success. I would say increased security; however the citizens would probably rate privacy whereas the responsible CFO would like to see a good ROI.

In your opinion, does biometrics makes a difference of cost with respect to the password management and card system while adopting in healthcare organizations?
A fingerprint scanning solution will of course cost some money. But the solution from DigitalPersona is not necessarily more expensive than a password management and/or card solution. As explained before DigitalPersona has a very powerful management system that can handle the users, control their access rights and manage both separate USB fingerprint readers and integrated swipe readers in many laptops.

Appendix B

Karin Sveheim
Precise Biometrics
Director, Markets, SWEDEN

How do you see biometrics as strong to be implemented?

Not sure I understand the question.. Are you asking for the reasons to implement biometrics?
In that case, the reasons are:

- Increasing security and privacy of patient data and information
- Ensuring the right identity of the patient (vast number of mistaken or duplicate identities and patient records)
- More convenient procedures for staff
- Cost savings

What are the threats and challenges that force the implementation of biometrics?

The challenge is that healthcare records are not to 100% electronic today. A lot of records are written by hand. Digital files is a clear pre-requisite for using biometrics.

Overall, the uncertainty surrounding biometrics in terms of privacy, relibality, cost and convenience have to be addressed. These are all major challenges.

Why healthcare organizations are demanding strong authentication and focus on suggesting biometrics?

For staff:
- fast and convenient access to computer systems and patient files

For healthcare providers:
- accountability and tracebility of the system
- cost savings compared to complex password systems
- increased IT security (no shared passwords, no written down passwords, etc)

For patient:
- integrity of sensitive information is preserved
- less errors related to duplicate records or errors related to identity

Q : **Do you develop the solution according to the security needs or it is a more generic solution to achieve accuracy, efficiency and performance?**

Our Match-on-Card solutions combine fingerprint recognition and smart card technology. The smart card brings the security, portability and scalability to the system, the biometrics bring ease of use, speed of transaction, and personal use. Combined it brings protected privacy as the biometrics is always handled by the card and makes the token personal.

The features and technology is to some extent generic but integrated in its applications it is adopted for healthcare use.

Do you think current biometrics solution can fulfill the requirement of healthcare sector regarding privacy and security of patient's record?

Yes, especially in combination with a smart card. Using a database of biometric information will always be sensitive and carries the risk of intrusion and abuse. Combined with a smart card, the cardholder is always in possession of his/her own sensitive data.

Do you think that National healthcare security policy and legislations is important to build customer trust?

Yes

How do you define ROI (Return on investment) in context of Biometric in healthcare sector?

If an IT system should be built for security based on passwords, these have to be so complex an organization will have to spend a lot of time managing password distribution, password resets, etc, not to mention the loss of productivity on the other end. A password based system is never free of charge. You can calculate a cost of approx 200 USD per year per user in PW related costs!

You can typically calculate the ROI on a biometric solution within a year.

What do you think about cost of the Biometric solution comparing card system?

We are advocates of combining fingerprint and smart cards.

Unless you combine the biometrics with the card, there will be a lot more costs associated with the surrounding infrastructure in terms of fingerprint terminals having to be secured (i.e limited supply) and other meachanisms surrounding data protection. By using the card, you can freely choose between different readers.

Important to note is that the organization should be independent on card supply (especially if distributing cards to patients, ie large numbers of userse) so they can also choose card suppliers according to new needs and budgets. Then it could be a good idea to make sure the biometrics is added as a Java applet so they don't have to replace this component as it would require re-enrollment, etc.

Did the current Biometric solutions make a difference in cost as compared to the traditional authentication solution?

Don't understand the question? I don't have a real life example to present if this is what you are asking for.

What aspects do you think are the main influencing factor to deploy Biometric in healthcare?

- Governmental legislation
- A stronger focus on healthcare admin costs
- Faster move to electronic healthcare records

Are there any other factors that hinders the implementation of biometrics in healthcare?

There will be different needs for different biometric modalities in different parts of healthcare. Practitioners using rubber gloves will have different needs than a patient. The needs analysis will be important. The use of Biometric in healthcare industry is seems to be undergoing a slow revolution?

Do you think that government legislation will push healthcare providers toward using the technology in a variety of ways for safeguarding patient data to securing physical locations?

Yes

What do you think about the slow deployment of Biometric in the field as healthcare that demand highest level of security?

Biometrics is slow to adopt in all areas of application, also in high security demanding environments. It is nothing unique. It is the 10-year maturity cycle that new technology faces.

Which is the most influential reason to succeed among three (cost, privacy and security)?

Cost

Please discuss if Customers are less interested in devices and more focused on purchasing solutions to their problems?

You have to win both system administrators and people technically responsible for both IT and physical access (most of the time different people, different departments, different budgets, and different agendas), purchasers, the user group, and the final decision makers. They will all have their different interest. In the end, the decision maker have to feel comfortable with the decision and not introduce an organizational or personal risk. Risk reduction/making a safe choice is of the highest interest.

Does healthcare sector rules and legislation effect your suggesting solution? (because you have to assure the solution in accordance with the healthcare policy for security and privacy with low cost)

You will have to promote solutions that comply with e.g HIIPA in the US of course. Compliance to standards and regulations, although sometimes just a check-box- exercise and sometimes even conflicting requirements, is a given. It is a qualifier, not a differentiator.

Appendix C

Birgitta Billinger Lundberg
Chef Blekinge kompetenscentrum
Landstinget Blekinge
Karlskrona

How you perceive biometrics in healthcare?

During interview Birgitta Lundberg give her opinions that how she perceive biometrics in Heath care, She said biometrics can give us a way to identify elderly people when they are ill and in need for acute care, if they don't have a safety identification themselves. That will help the system from home, through the ambulance transport, emergency room to the ward or home again. The alternative is a number for not known a individual, that means that you can't read the records with patient history, medication cards and so on. We can also make a new patients record own by the patient and with possibility to write your own notes.

Are you concerned about the security of medical records when using password authentication techniques?

A more safety way will be better, intelligent cards or biometrics.
She said her ideas that biometrics would be a better way in security aspects when we are dealing with medical records as compared to the password authentication techniques.

Where can biometrics be applied in healthcare with respect to privacy?

Medical records identification both staff and patient’s entry to special rooms or buildings.

Where can biometrics be applied in healthcare with respect to security?

Entry to special rooms or buildings, identification: who has been in the room or building at time

Do you think, biometrics could serve as a useful platform to address all of these security, privacy and cost issues?

yes, all of them, cost in a long time perspective

How do you assure privacy of biometrics e.g. the fingerprint ID will only be used within our healthcare system?

I don't understand the question

Do you feel the need of security and privacy at this stage when you have secret information as patient’s record etc?

Yes

Are there any Swedish Government regulations pertaining to the protection and privacy of medical records?

Oh, yes. A very strict law regulates this issue.

Is there any legislation concerning the patient's data will not be used by others?

The patient record is own by the hospital who are responsible to keep the data safe from others than the staff working with the patient at this very moment. The patient can buy a copy of his record, in some special situations the question can be denied, in terms of the best for the patient. It is against the law to log in to a patients record if you don't belong to the treatment team or have a special reason.

What do you think, is there any legislation for implementing biometrics in healthcare, if not what do you think, should there be legislated in current situation of privacy and security needs?

It could help in a lot of cases, to the medication for example. When a nurse who have the key to the medication room, you will know who have taken a specific drug, narcotics for example. You can sign with your finger print I think. But if a lot of people have to administrate and fallow the "Way" It might be to a too high expense?

How do you perceive the need of new technology in form of biometrics as a way for organizations to meet medical threats?

It can be a safety way of keeping the records information where they should be, not available for hackers.

What do you think about biometrics security solution and their implementation in healthcare in Blekinge county?

It is an interesting idea.

Give the priority level of three factors (cost, privacy, and security) in the adoption of biometrics in healthcare organizations with valid reasoning. 1_____ 2._____ 3 _____.

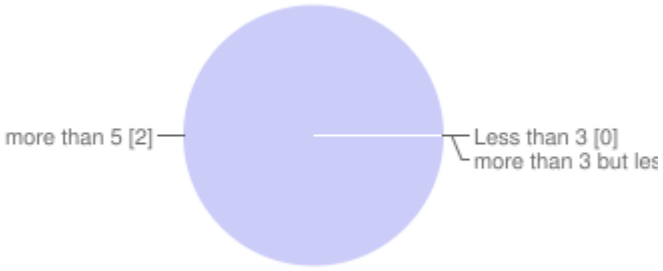
It is high cost initially for getting the system. It is a problem if you are hired as a doctor for short time and something are missed in the system and you are locked out from everything.

APPENDIX D

Questionnaire for Survey with healthcare Personnel

Summary See complete responses

How many years of working in healthcare?



Less than 3	0 0%
more than 3 but less than 5	0 0%
more than 5	8 100%

According to questionnaire findings all people have more than 5 years experience and it will directly effect in positive way on questionnaire findings validity.

What best describes your title & work?

physical therapist clinical and research Administration in different divisions.
Now as a project-coordinator.

I feel that biometrics is secure.

Strongly Disagree	0 0%
Disagree	0 0%
Neutral	0 0%
Agree	8 100%
Strongly Agree	0 0%

All of the people agreed with the statement that biometric is a secure way to communicate with health care system. It is analyzed that they have trust on biometrics system and in future they are agreed to face changing in the current system.

I have a privacy concern using biometric system (e.g., fingerprint verification, facial recognition, hand geometry verification, iris recognition, and voice verification).

Strongly Disagree	0 0%
Disagree	8 100%
Neutral	0 0%
Agree	0 0%
Strongly Agree	0 0%

After the results it is analyzed that all people have their privacy concern using biometric system. It is

analyzed that we have to first focus on privacy concerns then investigate the implementation of biometric system in healthcare.

Do you have worries that the disclosure of patient's health information may cause a medical theft or abuse?

Strongly Disagree	0	0%
Disagree	4	50%
Neutral	4	50%
Agree	0	0%
Strongly Agree	0	0%

Moreover 50% disagree with the statement that disclosure of patient's health information may cause a medical theft or abuse and with the same ratio of 50% have neutral response.
It is analyzed that half of the investigated people have confidence on their health information systems privacy while rest of the people have little doubt about the health information system privacy. It is analyzed that there is need of improvement/updation in the existing system.

I feel that biometric technologies are more secure than traditional IT security methods

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	0	0%
Agree	8	100%
Strongly Agree	0	0%

In addition all peoples are agreed on statement that biometric technologies are more secure than traditional IT security methods. It is analyzed that majority of the people are already well aware about the advantages and disadvantages of biometric technologies and traditional IT security methods.

It will be a good change to replace passwords and ID Cards with biometrics technology?

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	0	0%
Agree	4	50%
Strongly Agree	4	50%

Furthermore 50% strongly agree with the statement that It will be a good change to replace passwords and ID Cards with biometrics technology and with the same ratio of 50% agreed with the statement.
It is analyzed that majority of the people are well aware of the biometrics implementation advantages and they are not satisfied with the passwords and ID Cards. It is analyzed that majority of the people have no objection and they are in favor of biometric technology implementation.

My organization needs biometric technologies to avoid medical theft and abuse?

Strongly Disagree	0	0%
Disagree	4	50%
Neutral	0	0%
Agree	4	50%
Strongly Agree	0	0%

Afterword 50 % of the people agreed with the statement that their organization needs biometric technologies to avoid medical theft and abuse and on the other side 50% disagree with the same statement.

It is analyzed that half of the people need biometric technology to be implemented in their organization it could be because even they trust on the current system but they still need more secure technology to completely avoid medical theft and abuse. In addition to this after receiving reply it is analyzed that half of the people are satisfied that their current system is secure enough and it can avoid medical theft and abuse, it could be because they do not have awareness about the biometric technology main advantages or it could be because they do not want to adopt the changes in the system.

My organization is concerned to secure Patient healthcare information?

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	0	0%
Agree	4	50%
Strongly Agree	4	50%

In addition to this all of the people agreed that their organization is concerned to secure Patient healthcare information. It is analyzed that healthcare organizations strongly wants to avoid all kinds of medical theft and abuse. Moreover it is analyzed that there is high possibilities that healthcare organizations could adopt changes in the future in order to secure their systems.

I am willing to use biometric technologies to protect sensitive information at my organization.

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	0	0%
Agree	4	50%
Strongly Agree	4	50%

Furthermore it is identified that all of the people are agreed to use biometric technologies to protect sensitive information at their organization. It is analyzed that people would appreciate to adopt biometric technologies in the future in order to protect sensitive information at their organization.

Both technical staff and administration needs to spread awareness for Biometric technology in healthcare?

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	0	0%
Agree	0	0%
Strongly Agree	8	100%

Furthermore it is identified that all of the respondents are agreed that both technical staff and administration needs to spread awareness for Biometric technology in healthcare. It is analyzed that there is strong need to spread awareness for Biometric technology in healthcare and people want to know about the advantages regarding the biometric technology implementation.

Biometric technologies are available in reasonable cost with respect to its outcomes.

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	8	100%
Agree	0	0%
Strongly Agree	0	0%

Moreover it is identified that people have neutral response against the question that biometric technologies are available in reasonable cost with respect to its outcomes. It is analyzed that majority of the people do not have any knowledge regarding the implementation cost of biometrics technology with respect to its outcomes and there is a strong need to spread the awareness about the cost advantages of biometric technology implementation.

The maintenance cost is lower with biometric technologies than with traditional IT security methods.

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	8	100%
Agree	0	0%
Strongly Agree	0	0%

In addition to the above question it is identified that people have again neutral response against the question regarding the maintenance cost of biometric technologies. It is analyzed that majority of the people do not have any awareness/knowledge regarding the maintenance cost of biometrics technology with respect to maintenance cost of traditional IT security methods. It is analyzed that there is a strong need to spread awareness about the cost advantages of biometric technology maintenance as compared to traditional IT security methods.

I would consider biometric technologies to have considerable cost savings over traditional IT security

methods.

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	4	50%
Agree	4	50%
Strongly Agree	0	0%

Moreover it is identified that half of the respondents agreed that they would consider biometric technologies to have considerable cost savings over traditional IT security methods and half of the respondents have neutral response. It is analyzed that there is a need to spread awareness about the cost saving advantages of biometric technology over traditional IT security methods.

I would feel comfortable recommending biometric technologies in my organization.

Strongly Disagree	0	0%
Disagree	0	0%
Neutral	4	50%
Agree	4	50%
Strongly Agree	0	0%

20 Moreover it is identified that half of the respondents agreed that they would feel comfortable recommending biometric technologies in my organization and half of the respondents have neutral response. It is again analyzed that there is a need to spread awareness about the advantages of biometric technology over traditional IT security methods.