ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Proposal for Factors Influencing Biometrics Technology Security

Irfan Iqbal

Lecturer, Dept. of Computer Science, Al-Qassim University, Buraidah, Saudi Arabia

ABSTRACT: Biometric technology is being considered as a convenient and secure method of identification which eliminates the need to remember complex password, nor smart cards, keys and the like. This report is designed to help exploring main influencing factors and attitudes concerning this technology by informal interviews and web based survey specially in health care. This report will help in identifying recent security trends in potential organizations/institutions but also forecast its impact on future security concerns. After that the analysis will further help recommending a guide to boom its presence as emerging technology.

KEYWORDS: Biometrics, Attitudes & influencing factors, Security Technology.

I. INTRODUCTION

Biometrics measure individual ‘s unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry, retina, iris, or facial characteristics. Behavioral characters include signature, voice (which also has a physical component). Most commonly, security field uses three different types of authentication: Something you know: Password, PIN, etc Something you have: card key, smart card, etc Something you are—a Biometric A biometric is the most secure and convenient authentication tool. It can ‘t be borrowed, stolen, or forgotten, and forging one is practically impossible.

In this paper, our focus was on ―Biometric Technology Security concerns while applying Biometrics as security measure. It includes observing our domain of interest and then to establish a connection with its relevant application potential. We made divisions by observing its depth and wideness. So the

1st Division: covers the Biometric Security concerns like factors influencing the adoption of Biometric security technologies by decision making when trying to adopt biometric security technology solutions.
2nd Division: Covers the challenges and problem about the effectiveness and acceptability of biometric system while adapting as a new technology.
3rd Division: Covers the proposed research methodology while considering its expected outcome and then how this research can contribute by helping security professionals about its effectiveness.

II. BACKGROUND

A. *AREA OF INTEREST*

The Biometrics generates from the two Greek words, “Bios” means life and “metrikos” means measure. Biometrics measure individual's unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry, retina, iris, or facial characteristics. Behavioral characters include signature, voice (which also has a physical component). [1]

Faundez-Zanuy give explanation about "Biometric security technology," as most commonly, security field uses three different types of authentication:Something you know: Password, PIN, etc. Something you have: card key, smart card,

DOI: 10.15680/IJIRCCE.2017. 0503001

etc. Something you are—a Biometric

A biometric is the most secure and convenient authentication tool. [1]

Liu, S. and Silverman, M. discovered that security systems also use biometrics for two basic purposes: to verify or to identify users. Identification tends to be the more difficult of the two uses because a system must search a database of enrolled users to find a match (a one-to-many search). The biometric that a security system employs depends in part on what the system is protecting and what it is trying to protect against. [3]

Identification: In this approach no identity is claimed from the user. The automatic system must determine who the user is. [1]

Verification: In this approach the goal of the system is to determine whether the person is the one he/she claims to be. This implies that the user must provide an identity and the system just accepts or rejects the user according to successful or unsuccessful verification. [1]

Jain, A.K., Ross, A. and Prabhakar, S examined that any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

Universality: each characteristic. Person should have the characteristic.
Distinctiveness: any two persons should be sufficiently different in terms of the characteristic.
Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
Collectability: the characteristic can be measured quantitatively. [4]

Regarding the related research work, it is determined that there are four influencing key factors as cost, privacy, user acceptance & security that we should emphasis on. These factors have been discussed by various researchers and analyzed with the help of different features and surveys by different Biometrics companies.

The feature “Biometrics Enter Europe’s access control markets” by Biometrics Technology Today in 2002, the cost factor is identified as, after September 11th, the prices and growth have stretched and therefore the prices have been brought down. In 2001 biometric only had 2,5% of the sales of control readers. The technologies competing with biometrics are old established technologies such as digital key pads and magnetic swipe and bar codes. [5]

According to the survey conducted on the cost factor by Europemedia on 200 companies, 74% of the investigated companies use some kind of authentication technique. There is not much investment in smart card, tokens, biometrics and digital certificate technologies because it is often considered to be expensive. Further the article says that although the old password technique has a low initial cost, it will most likely be a large cost because of the resetting and administrating of users. [6]

Roberts &Ohlhorst, explored through a poll carried out by CRN that almost 90% of the customers of security solutions providers have not implemented biometrics solutions. According to Roberts and Ohlhorst biometric security solutions can offer a higher level of security and ease of use than no other method can. But the providers struggle with the fact that it is difficult to demonstrate the ROI (return of investment) of biometric solutions [7]. Further the research by Roberts and Ohlhorst (2005) shows that the security service providers believe that uncertainty about ROI (Return on Investment) from biometrics is the foremost reason why their customers stay away. Complexity comes as the second reason why customers do not invest, finally in third place it is the actual cost of the investment. [6]
According to Forte, D, there is clearly a high privacy risk concerning biometric solutions [8]. The researchers Donos, P. &Zorkadis, V identify that since biometrics works with personal data, there are concerns regarding the legal point of view of privacy and personal data protection. With biometric systems there might become a privacy protection problem if a third party get their hands on the databases holding the biometric data. For example, if government authorities

would use a fingerprint database for their own processing desires. [9]

Further, Donos&Zorkadis says that one way of minimizing these problems are to keep the data in an object that remains with the person, such as a smart card or mobile phone. The authors also suggest that the data should be encrypted.

Davis, F.D. exposed that a system needs to be both perceived as useful and easy to use by the users. A system might be considered to be very useful but also very difficult to handle, and thereby it will not be accepted and used. [10]

In computer security, biometrics refers to the authentication techniques that rely on measuring physical and behavioral characteristics [1]. This thesis addresses issues of adoption and deployment of biometrics for security. Biometrics technology is a rapidly growing area of research within computer science.

User's beliefs and perceptions about the biometric system may influence the successful implementation and effectiveness of the biometric system. There may be other factors in the operating environment that influence the effectiveness and acceptability of biometric system, e.g. facial camouflaged with cosmetics. [3]

The decision making process can be complicated for organizations by different influencing factors such as cost, privacy, user acceptance, ease of use, security, communication, size and type of organizations when considering the adoption of a new technology. Biometric security technology has features and challenges that increase the difficulty of decision making to recommend the technology.

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.

In a poll carried out by CRN almost 90% of the customers of security solutions providers have not implemented biometrics solutions. According to Roberts and Ohlhorst biometric security solutions can offer a higher level of security and ease of use than no other method can. But the providers struggle with the fact that it is difficult to demonstrate the ROI (return of investment) of biometric solutions. [7]

Further the research by Roberts and Ohlhorst shows that the security service providers believe that uncertainty about ROI from biometrics is the foremost reason why their customers stay away. Complexity comes as the second reason why customers do not invest, finally in third place it is the actual cost of the investment. [7]

According to Forte, D, there is clearly a high privacy risk concerning biometric solutions [8]. Since biometrics works with personal data, there are concerns regarding the legal point of view of privacy and personal data protection [9]. With biometric systems there might become a privacy protection problem if a third party get their hands on the databases holding the biometric data [9]. For example, if government authorities would use a fingerprint database for their own processing desires [9].

Davis, F.D. found that a system needs to be both perceived as useful and easy to use by the users. A system might be considered to be very useful but also very difficult to handle, and thereby it will not be accepted and used. [10]
Faith-Michael E. Uzoka, TshepoNdzinge analyzed the adoption of biometric technology in a developing country from an institutional point of view. Their findings show that job positions (managerial and operational) could influence perceptions of innovation characteristics (especially ease of use and usefulness) in the decision to adopt biometrics. [19]
Although a large amount of work has been done to maintain and strengthen the security of biometric identification but it has not been widely recognized and completely resolved. In identification approach no identity is claimed from the user. The automatic system must determine who the user is [1].

After a literature review on adoption of biometric technologies in organizations, we discovered a gap in research regarding the factors influencing the decision to implement biometric technologies. Research in this area could help to discover and clarify why organizations are unwilling to deploy biometric authentication techniques. It could also help IT responsible, most probably security managers and security analysts to determine what aspects of biometric security technologies are of concern to them and accordingly recommend appropriate security solutions. Companies that have some similar work on security can also gain benefits from this research for suggesting IT security solution/products.

Bill Gates predicted that in the next few years, biometric technology will become an important reform in the IT industry [11]. Nowadays, biometrics has not really entered the lives of the most people, but it also couldn't meet the requirements for some of the strong security applications areas (such as banking, e-passport, healthcare etc.).

B. *AREA OF RELEVANCE*

With the passage of time, the demands on security systems and technologies are increasing and organizations and authorities want simpler but precise information systems that are cost efficient, maintain privacy and User acceptable. Because of its authentication techniques, its emergence and development is exciting and it owns considerable application potential. Bill gates predicted that in the next years, biometric technology will become an important reform in the IT industry. [11].

There are different forms of applications and markets for biometric systems in security issues.
Biometrics and e-passports initiate the use of biometrics in order to fight against look-alike fraud that may happen after 9/11 attacks. Now modern passports hold many protection mechanisms that are really hard to forge. A passport traditionally has three security requirements, (1) authenticity and integrity of the document (and its data), (2) match with the holder, and (3) authorization, depending on the situation of use. [12]

Biometrics is being incorporated in a wide range of health care applications. By initiating the use of biometrics to safe protect records, in 1996, the US congress passed Health Insurance Portability and Accountability Act (HIPAA) to "improve the portability and continuity of health insurance coverage in the group and individual markets, .. . (and) to combat waste, fraud, and abuse in health insurance and health care delivery." Biometrics can protect the confidentiality of medical records through health care provide authentication. [13]

Biometrics at the border was considered important when the European Commission (EC) planned to strengthen Schengen zone border security, while making smooth travel for citizens, tourists and legal migrants. The idea includes proposals for the introduction of biometric base entry/exit system, the implementation of automated border crossing facilities for bona fide travelers. UK border agency also announced plans for automated border gates with facial recognition technology where the comparison is made between the image in e-passport chip and live image. [14]

Biometric-based smart ID card implementation in Rwanda Universities have some security and privacy issues that further effects its implementation. The purpose was to introduce biometric solution by engaging the audience and then to implement by meeting present challenges. [20]

Although there is a lot of big-name in the government sector and a number of private enterprises also took steps to implement the technology. For example, one of China's largest banks, China Merchants Bank (CMB), deployed PerSay'sFreeSpeech voice biometrics system to make phone-based transactions more secure. [14]

III. CHALLENGES AND PROBLEM FOCUS

A. *RESEARCH QUESTIONS*

Users 'beliefs and perceptions about the biometric system may influence the successful implementation and effectiveness of the biometric system. There may be another factors in the operating environment that can influence the effectiveness and acceptability of biometric system, e.g. facial compromised with some changes [15].

The decision making process can be complicated for organizational when considering the adoption of a new technology. Biometric security technology has capabilities, features, and challenges that increase the difficulty of decision making to recommend the technology.

RQ#1. What are the reasons to why the biometric technology has had difficulties to breakthrough?
RQ#2. What are the attitudes towards biometrics among company leaders and ordinary individuals?
RQ#3. Analyze the Factors influencing the adoption of Biometric security technologies by decision making when trying to adopt biometric security technology solutions.

B. *FOCUSED AREA*

Although a huge work has been done to maintain and strengthen the security of biometric identification, but it has not been widely recognized and completely resolved by the people.

After a literature review on adoption of biometric technologies in organizations, it is discovered that a limited research regarding the factors influencing the decision to implement biometric technologies. Research in this area could help about why organizations are unwilling to deploy biometric authentication techniques. It could also help IT persons, most probably security managers that may also security analysts to determine what aspects of biometric security technologies are of concern to them and accordingly recommend appropriate security solutions. Companies that have some similar work on security can also take benefits from this research while suggesting IT security solution/products.

IV. METHOD/APPROACH

A. *PROPOSED RESEARCH METHODOLOGY*

To reach conclusion and proper answers of research questions, it is required to have a suitable research approach for the research work. There are different research methodologies in literature that can be used for the research work. Qualitative [16, 17], quantitative and mixed methodologies [18] 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 involves certain phenomenon that involves humans and that's why qualitative research methodology is best fit for it [18]. We started from literature study to get information about the subjected area. Later on, Interviews will be conducted for collecting data from companies. Interview questions will be based on the strategy to have a deep understanding about company's point of view about biometrics and to identify, why they are not ready to invest in biometrics technology. According to our research questions interviews could be a better research approach to answer our research questions. On the other hand, to explore individual's opinions about biometrics, questionnaire could be an appropriate way. In questionnaire, we can judge the factors like 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. We will use a questionnaire with open ended questions. The purpose is to record the related things like attitudes and create a relationship with the respondent so that we will help them to clear their ideas. This will help to gather more appropriate material for further analysis. Interviews will be conducted with three different ways. One is e-mail interview, one is telephonic interview and the last one is live interview.

B. *EXPECTED OUTCOME*

Expected outcome of our study will be a report which will reflect the results of the study in the form of analysis of questionnaire, analysis of interviews, suggestions and arguments. These methods are suitable because nature of the outcomes is observed to be theoretical.

Through this study, the mentioned factors (Cost, Privacy, User acceptance and Security) are proved to be the key factors in recent security trends in potential organizations/institutes.

It will forecast its impact on future security concerns in perspective of these key factors. It may help for strong recommendations before development and deployment after a detailed feedback.

This analysis will help further to publish a guide with detailed facts about mentioned factors to boom its presence as emerging technology.

V. POTENTIAL CONTRIBUTION

Specifically, the research can help information technology professionals to determine if the security effectiveness, organizational need, reliability, and cost/value aspects of biometric security technologies are generally acceptable to IT/IA decision makers. The study can also provide security technology companies with information that will assist in the determination of what is important to their customer base when considering the introduction of new IT security products.

VI. CONCLUSION

This paper describes the stages for introducing, comparing and then suggesting biometric technology as emerging security measure than other conventional identification methods. The area of concern that was particularly discussed mainly based on some factors like Cost, Privacy, User acceptance and Security to meet the needs of recent security trends in potential organizations/institutions. These factors also help to assess the future security concerns for further enhancing this technology as a pure and trustable solution.

ACKNOWLEDGEMENT

My thanks and sincere appreciation goes to Professor *Dr. Jobair bin SulemanAlharbi* , the finest teacher and mentor we could possibly want. *Dr. Jobair* provided continuous encouragement, strategic thinking and goal focus throughout my research work.

REFERENCES

[1] Faundez-Zanuy, M."Biometric security technology," Aerospace and Electronic Systems Magazine, IEEE , vol.21, no.6, pp.15-26, June 2006. DOI=http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=166203 8&isnumber=34781

[2] Lawrence, O. It soulutions Series: Information Technology Security: Advice from Experts. Idea Group Publishing. Hershey, PA, USA. p.138-142, 2004

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

[4] Jain, A.K.Ross,A and Prabhakar, S. "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on , vol.14, no.1, pp. 4-20, Jan2004.DOI=http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber= 1262027&isnumber=28212

[5] Biometrics Technology Today. 2002 . Biometrics enter Europe's access control markets .Retrieved 2005-03-16.DOI=http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6W70-47DH7D0- 1B-5&_cdi=6612&_user=646817&_orig=search&_coverDate =09%2F01 %2F200

[6] Europemedia. 2003. 62% of European enterprises have no plan to increase spend on IT security in 2003. Amsterdam. Retrieved2005-03-16. DOI=http://proquest.umi.com/pqdweb?index=0&did=3234 57561 &SrchMode= 1 &sid= 1 &Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1110979468&cl ientId= 17918#fulltext

[7] Roberts, J. &Ohlhorst, F, J.Channel Engagement Key to Boosting Biometrics. CRN. p.32. Feb 28, ABI/INFORM Global, 2005

[8] Forte, D. Biometrics: Future Abuse. Computer Fraud and Security. 03 (10), p.12-14. 2003

[9] Donos, P. &Zorkadis. On biometrics-based authentication and identification from a privacy-protective perspective. Information Management & Computer Security 12 (1) p.125-137.2004

[10] Davis, F.D. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly. 13, (3), 319.

[11] Shan, A. Ren, W. and Tang, S. "Analysis and Reflection on the Security of Biometrics System," Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on , vol., no., pp.1-5, 12-14 Oct.2008. DOI=http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4681014&isnumber=4677909

[12] Schouten,B.Jacobs,B. Biometrics and their use in e-passports, Image and Vision Computing, Volume 27, Issue 3, Special Issue on Multimodal Biometrics - Multimodal Biometrics Special Issue, 2 February 2009, Pages 305-312, ISSN 0262-8856,

DOI=http://www.sciencedirect.com/science/article/B6V09-4SKK206-1/2/5a0b6a79ccc94a506253c004b357c318

[13] Marohn, D. Biometrics in healthcare, Biometric Technology Today, Volume 14, Issue 9. September 2006. DOI=http://www.sciencedirect.com/science/article/B6W70 -4KWCG46-J/2/a4d62fecb8c4ad9efc 1 b 1 d5efc769c43)

[14] Biometrics review: Biometric Technology Today, Volume 17, Issue 1, January 2009, Pages 9-11, ISSN0969-4765,DOI=http://www.sciencedirect.com/science/article/B6W70
-4VND8DS-N/2/0537c8709cd589674a6b84562b05794a

[15] Liu, S. and Silverman, M. A practical guide to biometric security technology. IT Professional3,1(2001)27- 32 .DOI=http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=899930&isnumber=19477

[16] Hazzan, O., Dubinsky, Y., Eidelman, L., Sakhnini, V., &Teif, M., 2006. Qualitative research in computer science education, In Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education. SIGCSE '06. ACM, New York, NY, pp. 408-412.

[17] Seaman,C. Qualitative methods in empirical studies of software engineering, Software Engineering, IEEE Transactions on, vol.25, no.4, pp.557-572.1999

[18] Creswell,J.W.2002. Research Design. Qualitative, Quantitative and Mixed Method Approaches. Second Edition, Sage Publications.

[19] Uzoka F, E., Ndzinge, T. 2009. Empirical analysis of biometric technology adoption and acceptance in Botswana, Journal of Systems and Software, Volume 82, Issue 9, SI: QSIC 2007. September 2009. Pages 1550-1564, ISSN 0164-1212. DOI=http://www.sciencedirect.com/science/article/B6V0N-4W6Y5DT- 2/2/173559a10312e3695cbf882e853c6a01)

[20] Harinda, E. and Ntagwirumugara, E. Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities. Journal of Information Security, 6, 93-100. doi: 10.4236/jis.2015.62010