Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 6; October, 2014 pp. 51-55
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Biometrics Technologies for Interactive Access of Data: A Case of Patient Identification in Emergency Scenarios in Botswana

Gofaone Kgosietsile Kebualemang

Botho University, Botswana, P O Box 501564
Gaborone, Botswana, Botho Education Park

Abstract: **Modern Societies are now filled with an increasing number of Information Communication Technologies (ICTs) for interactive access to data that require a lot of security measures to be integrated within them. In the case of Botswana, a predominant number of these interactive access devices are still primitive and often use the old traditional way of keying in security details for authentication. This paper is an attempt in exploring various technologies surrounding the implementation of Biometric systems while putting emphasis on security as the main driving factor. The author intently adopts a purpose driven approach by contrasting the benefits brought by these Biometric technologies in emergency scenarios within the context of Botswana based emergency services.**

Keywords: **Behavioral intention, Perceived credibility, Applications, Biometric Technologies, Security, Emergency, Processing, Retrieval.**

1. INTRODUCTION

Security has come a long way as one of the factors needed in order to maintain data integrity and authentication. It is the security of data and its accessibility which has called for so many various security measures to be put in place and yet many have done little or are still taunted with loopholes in ensuring data protection. It is the accessibility at personal level which has made data more vulnerable to stealing and this paper tries to implore the utilization of Biometrics technology in the security of data. Biometric technologies have become the best option available into securing data accessed through individuals as they easily secure personal identification which is the key component to valuable information accession.

These technologies utilize human biology features to authenticate personal identity of individuals. They come as automated methods which are used to identify or verify the veracity of an individual based on their human biology features such as fingers, hands, iris, voice and or face. They also extend to behavioral characteristics such as dynamics of keystrokes and signatures. These systems compare the recorded scans of such characteristics versus the live captured scans. These systems have come about as the most reliable, practical and cost effective forms of security which are acceptable to users, yet in Botswana they have remain largely unutilized. Their low utilization has prompted the undertaking of this research. Currently in Botswana, the predominant form of security to data accession is keying in security detail for authentication. This form of security identification has many flaws amongst which includes theft of security identification keys or their compromization in a manner which will give the compromiser the abilities to have access to confidential and secretive data. Therefore, this research focuses on utilization of Biometrics technologies for interactive access of data.

2. PROBLEM STATEMENT

With the rapid growth of Information Communication Technologies such as the internet, e-commerce has gained huge acceptance with more individuals search for information, communicating, purchasing and bank electronically. Yet such developments pose a significant threat to most of the organizations in Botswana. The organizations are relying on the Internet and online systems more heavily today than ever before to reach both their customers and partners. In Botswana, organizations which process sensitive data in most cases are using the keying in authentications that can be easily tampered with in the process of authentications. There are numerous cases that are reported in Botswana which relate to the authentications theft and hacking in Botswana particularly the banking and data theft access.

3. RESEARCH AIM

In relation to the questions posed in the previous section it is possible to construct five key aspects for the investigation of various Biometrics technologies surrounding the implementation of Biometric systems while putting emphasis on security as the main driving factor in Botswana are as follows:

3.1 Procedural Development

To identify various biometric technologies that can be implemented in various organizations in Botswana.

3.2 Function domain

To identify the procedures and possible application architecture and standards will support biometric technologies.

3.3 Communal Impact

The examination of the human perspective and their degree of acceptance, privacy and ethical issues the use of Biometrics in access of data.

3.4 Environmental Influence

Feasibility study in the implementation of the Biometrics systems mainly in the emergency scenarios such as the patient identifications in the rescue missions where the patients are not recognized

3.5 Performance

This is to identify and examine the expenses and cost metrics in the use of Biometrics, their safety and security in the modern technologies and Human rights.

The main aim of this project will focus on the above mentioned aspects from the literature review through to the recommendations and the development of the Biometric application for the interactive data access in Botswana in case of Emergency scenarios. Yet in overall, provides an opportunity to research an emergent technology with a compelling application in many, future systems, commercial and e-governmental security systems. In addition to Investigate key biometric technologies in the market today, in terms of improvement standards, realization, performance issues and communal impact.

4. RESEARCH OBJECTIVES

This research attempts to identify the factors that influence the intention to use biometric technology in an interactive data access, e-government , online interactive data access applications generally and also based on major emergency application that are used in Botswana. The application types are patient identification, Internet banking; online purchase, e-government services as well as public service delivery. This research in biometric technology will achieve its goal by using an adaptation of the technology acceptance model for interactive data access applications systems and context. Finally, this research seeks to understand the role of usage experience as moderator on the relationship between those factors and intention to use biometric technology in emergency scenarios.

5. RESEARCH QUESTIONS

To achieve the objectives of this research, the following questions are addressed:

1. What are the factors that influence the intention to use biometric technology in emergency and other online applications by users in Botswana?

2. Are there any differences in the levels of intention to use biometric technology based on types of online applications (emergency rescues, banking, online purchase and online income tax filing)?

3. Does usage experience in online applications and biometric technology moderate the relationship between those factors and intention to use?

6. RESEARCH SCOPE

With the growing popularity of Information Communication Technologies such as the Internet, e-commerce has gain huge acceptance with more individuals search for information, communicate, purchase and bank electronically online and live interaction with the data in the cases of emergency scenarios in Botswana. The Internet enables all of us to do so much more efficiently at anytime and anywhere. Organizations are relying on the Internet more heavily today than ever before to reach both their customers and partners. For the Internet confidence customer, it provides a more convenient way of accessing services and performing transactions. For the organization, it can translate into a competitive advantage as well as delivering significant cost savings versus traditional phone-based and brick and mortar transaction methods. Further, in a multi-channel environment, online services can help increase customer retention by being an effective way of delivering new products and services (Voice, 2005).

7. DEFINITIONS OF KEY TERMS

- **Behavioral intention:** according to the results of the research by T. Mansfield et al (2009) as the degree in which a person or an individual can be determined to perform a specific behavior

- **Perceived credibility**: defined as the degree to which a person believe that using a particular system would be free from privacy and security threats (Ong et al., 2004)

- **Biometric Technologies**: according to the results of the research Davis et al.(1989) defined the biometrics technologies as

- **Perceived ease of use**: defined as the degree to which a person believes that using a particular system would be free of effort (Davis, 1989a)

- **Perceived risk**: perception of an individual of the adverse effect, consequences and the uncertainty that may occur by engaging in a particular behavior or activity (Dowling and Staelin, 1994)
- **Perceived usefulness**: defined as the degree to which a person believes that using a particular system would enhance his or her job performance (Davis, 1989b)

8. RESEARCH METHODOLOGY

The dependent variable for this research is the intention to use biometric technology in interactive data access in case of emergency scenarios or online applications. The actual usage is not used as the dependent variable since there is little of this technology that is in use in Botswana. Similar in many other studies of Technology Acceptance Model (TAM) with the extended model (e.g., Adams et al., 1992; Wang et al., 2003; Fusilier and Durlabhji, 2005; Luarn and Lin, 2005), the attitudes construct has been removed to simplify the model. Based on the literature review, TAM is able to explain and offer a better prediction on the users' intention to use a new technology. As such, this research uses selected constructs from TAM (Davis et al., 1989) which are perceived ease of use (PEOU) and perceived usefulness (PU) as the independent variables.

A questionnaire was used to gather the information required for the study. The questionnaire elicited information about demographic, perceived usefulness, perceived ease of use and intention to use.

The questionnaire was developed based on researches conducted by Tampa (2013), Florida (2012) Davis, Bagozzi and Warshaw (1989), Basyir (2000), Ndubisi et al. (2001) and Polatoglu et al. (2001). The Cronbach alpha obtained for the two measures were 0.70 for perceived usefulness and 0.69 for perceived ease of use. The intention to use measure was adopted from Davis et al. (1989).

9. LITERATURE REVIEW

In this research study a literature search on the topic of the use of Biometrics in interactive access of data and management systems discovered few preceding research studies and surveys, four of which are investigative in nature: Cory Janssen (2002) study on how the Biometrics technologies work in Security and Patrick Grother, Elham Tabassi (2007) study on Performance of Biometric Quality Measures on the IEEE transactions on pattern analysis and machine intelligence sought to determine whether use of Biometrics can used as the full authentication for easy access of interactive data and other public services.

However, in their findings it provided an analysis and gave the justifications as to how the project would fit into the already existing body of knowledge in case of Botswana. Furthermore, it gave a clear view of how the implementation of the automated system can be concluded to suite well with the current environment of work in Botswana government and other emergency scenarios.

9.1 Biometrics Overview

9.1.1 Defining the Biometrics

The term biometrics is derived from the Greek words bio (life) and metric (to measure) (Scherer, 2005). Biometric identification exploits the universally recognized fact that certain physiological or behavioral characteristics reliably distinguish one person from another (Scherer, 2005; Ahmed and Siyal, 2005). In short, biometric is the process of automatically recognizing a person using distinguishing traits not shared by any other individuals (Harris and Yen, 2002; Scherer, 2005).

Physical characteristics include fingerprints, hand geometry, retina, iris and facial characteristics, DNA, ear and lip motion recognition (Ahmed and Siyal, 2005; Jain et al., 1999; Scherer, 2005; Langenderfer and Linnhoff, 2005). Behavioral characteristics include signature, voice, keystroke patterns and gait (Jain et al., 1999; Scherer, 2005).

9.1.2 Brief History

Biometric has been used throughout history. Biometrics has been applied in a variety of ways since the time of Egyptian Pharaohs who used height measurement (Davies, 1994). Babylonian kings used handprints to identify different things such as engraving (Harris and Yen, 2002). The Chinese merchants stamped children's palm prints and footprints on paper with ink to distinguish the young children from one another (Scherer, 2005).

In the early nineteenth century, criminology was the main driver of biometrics, when researchers studied the relationship between physical features and criminal tendencies. A method called anthropometrical signalmen involved taking measurements of people's skulls to identify criminals and catch repeat offenders. Although no definitive conclusions were reached on the link between cranial features and a life of crime, this work did lead to the use of the most well known biometric, the fingerprint, as the international standard for identification.

9.1.3 Current practices

Although at present biometrics have limited mainstream usage, they have found a home in popular culture, specifically the movies. Movies have used biometrics in sci-fi or adventure films, including such movies as Total Recall and Charlie's Angels. Examples of biometrics in movies include forged identities through high tech facemasks, voice disguise, forged hands or fingerprints, even false retinal images through the use of contact lenses. Whether the movies are prophetic in depicting how easily biometrics can be circumnavigated remains to be seen. Without question, as with all security measures, there will always be those who seek to evade detection.

Currently, biometric techniques are used mainly in security operations. For example, they are used in prison visitor systems, state benefit payment systems, border control, gold and diamond mines and bank vaults. Clearly these are areas where security is an issue and fraud is a threat. Recent world events have led to an increased interest in security that will propel biometrics into mainstream use. Areas of future use include workstation and network access, Internet transactions, telephone transactions and in travel and tourism.

There are a number of different types of biometrics: Some are ages old; others are more recent and employ the latest technology. Technological advances will surely refine existing methods and lead to the development of new ones. The most well known biometric technologies include fingerprinting, hand geometry, signature verification, voice verification, retinal scanning, iris scanning and facial recognition:

Fingerprinting: This is the most well known non-invasive biometric technique. There are several sub-methods within fingerprinting, with varying degrees of accuracy and precision. Some can even detect when a live finger is present. This method has been refined over the years. Training is an issue with this technique.

Hand geometry: This method measures the physical aspects of the hand and fingers. It is easy to use.

Voice Verification: A number of such products exist, although flaws exist with regards to local acoustics. This method is still developing and will undoubtedly improve over time.

Signature verification: widely accepted as a means of identification, which is promising in its use as a biometric measure

Retinal scanning: An accurate method, it does require the subject to look into a device and focus on a specific location. This will likely limit consumer acceptance. It is currently considered a marginal biometric technology.

Iris scanning: Less intrusive than retinal scanning, this method is easier to use, and has great potential as an identification device.

Facial recognition: Unobtrusive detection and verification are the strong points of this technology

9.2 The Technology: How does it work?

Facial recognition, like any other biometric device, has three basic steps: observation, normalization, and matching.

9.2.1 Observation

In the observation phase, a sensor takes some sort of reading of the biometric. The sensor type depends on the type of biometric. In the case of facial recognition, a picture is taken. This captured biometric observation is then turned into a "biometric signature" for the individual observed.

9.2.2 Normalization

In this phase, a computer uses an algorithm to "normalize" the captured biometric signature. The algorithm makes sure that this signature is saved in the same format (size, resolution, etc.) as the signatures in the database it holds. This "normalized signature" is saved for the individual.

9.2.3 Matching

A computerized matcher compares the normalized signature to the set of pre-existing signatures stored in the system's database. The matcher provides a score to indicate how the normalized signature compared against each of the signatures in the database. What is then done with this information and the score depends upon the purpose of the overall application.

For any biometric application, two possible matching processes exist: verification and identification. In a verification application, the system must only answer a simple yes/no question – does this individual match who they say they are? This type of application could be used to verify employee identification to restricted areas, for example, by confirming that the employee presenting himself was who he claimed to be.

In an identification application, however, the system must compare the captured signature against all signatures in its database and provide a ranked list for the success of the matches. The process is no longer a one-to-one process, as verification is, but is instead a one-to-many process that is much more complex. Additionally, in an identification application, the subject need not be aware that the system is capturing his or her image.

9.3 Existing Emergency or Medical related applications

Telemedicine can be defined as the use of audio, video, and other telecommunications and electronic information processing technologies to provide health services or assist health care personnel at distant sites. Nowadays the evolution of wireless communication means enables telemedicine systems to operate across the world, increasing telemedicine benefits, applications, and services. The following are sample of projects that have been developed in the field of telemedicine and communication:

According to the results of the research by Shihab A. (2010) Mobile Medical Data called MOMEDA is a demonstrator that can be used from a PDA (Personal Digital Assistant) to access electronic patient record data and provide it to the consulting physician. Diagnostic information such as radiological images as well as text and laboratory data is transmitted to a wireless pocket-size access customized disease-specific information material that enables them to fully understand in a simple and constructive form what their medical problem is, what the planned procedures are, what lifestyle they should follow during and after their hospitalization, thus becoming more qualified partners in the recovery process.

10. CONCLUSION

In recent years biometrics has become a commercially viable technology and will certainly bring about profound changes in our everyday lives as it continues to develop. However, misconceptions of the technical and performance side as well as the social impact of biometric systems, has lead to a distortion of the facts. As Ashbourn points out in [A][2], “there is really no such thing as a biometric system”, that in reality, biometric recognition is incorporated as part of the system and as such, careful consideration has to be given to the architectural design and implementation of a particular solution. Clearly, system integration and infrastructural issues such as template and interface standards, operational conditions and user interaction are vitally important to effective deployment. Additionally, selection of biometric methodology based on the above must also be carefully considered, particularly from the user point of view.

Understanding the difference between general and operational conditions when testing goes a long way to understanding what a feasible and reasonable expectation is when it comes to evaluating biometric performance. This also highlights the often over-estimation of performance, security and reliability that some commercial vendors claim for their products. So crucially, it is important to understand the conditions under which performance-metrics for a given product are achieved i.e. are they verifiable independently or can test conditions be recreated easily by customers. Different implementations have different requirements, personal security i.e. PIN, secure physical access or open/closed systems. These deployments vary in required functionality and operational environment, therefore best practices in software development must be followed including thorough end-to-end testing prior to deployment.

Individual governments or organizations may also have a vested interest in distorting the facts about the capabilities of biometric technology. For example, the relentless promotion of biometrics as a global panacea for all security issues. It is important that the general public is properly informed as to the biometric technology can and cannot do. It is true that a person’s biometric data can be used to abuse their civil rights but only in as much as the political will to abuse the civil rights of the citizenry prevail. Government has a social obligation to protect individuals against biometric identity theft and to protect individual rights, freedom and privacy via new legislation if necessary.

As biometric technology continues to evolve, the need to provide comprehensive information for IT industry professionals, researchers and students has become an imperative. Many experts in the field have provided such information in the form of various generally available texts intended to fill that knowledge gap. Maltoni et al, [A][1], and Bolle et. al., [A][3], are the core technical research sources for this project because they proved the most relevant. Maltoni et al, provides the specifics relating to fingerprint recognition whereas Bolle et al, provides a more general overview of all the major technologies.

As a technologist Ashbourn, [A][2], [A][8], is primarily concerned with the issues facing commercial industry and government in the deployment of biometric applications. His view includes the pragmatic and sometimes controversial considerations largely ignored by the ostensibly technical viewpoint of the pure researcher.

REFERENCE

[1] A. A. Ross, K. Nandakumar, A. K. Jain. (2011) Handbook of Multi-biometrics: Discussing obstacles and Positive Aspects in Biometrics', *Journal of Security in Biometrics*, 30 (5), pp.49-95, [Online]. Available from: http://www.uidai.gov.in/UID_PDF /Biometrics_Report.pdf (Accessed 7 July 2014)

[2] Anil Jain, Patrick Flynn, Arun Ross. (2009) 'Handbook of Biometrics', Proceedings of the International Workshop on Biometrics, 24-27 April, Berlin. Los Alamitos, California: IEEE Computer Society Press, pp.77-98.

[3] T. Mansfield, G. Kelly, D. Chandler, J. Kan (2009). ‘American National Standard for Information Systems’ *Electronic Journal of Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1* [Online] Available from: http://www.globalsecurity.org/security/systems/biometrics-ref.htm (Accessed: 8 July 2014)

[4] Nissan Moradoff (2009). ‘Biometrics: Proliferation and constraints to emerging and new technologies *Electronic Journal of Biometric Information* [Online] Available from: http://www.palgrave-journals.com/sj/journal/v23/n4/abs/sj200821a.html (Accessed: 8 July 2014)

[5] Shahram Orandi (2006). ‘Biometrics is an automated method of recognizing a person based on a physiological or behavioral characteristics’ *Electronic Journal of Biometric Information* [Online] Available from: http://www.creativeworld9.com /2011/03/abstract-on-biometrics-no-more.html#sthash.bBkGj2Eq.dpuf (Accessed: 8 July 2014)

[6] Aarvak T, Lorentsen S-H & Bangjord G (1996): Use of individual differences in belly patches in population monitoring of Lesser White-fronted Goose *Anser erythropus* at a staging ground. Fauna norv. Ser. C, Cinclus 19:69–76.