TOWARDS USER ACCEPTANCE OF BIOMETRIC TECHNOLOGY IN E-GOVERNMENT: *a survey study in the Kingdom of Saudi Arabia*

Thamer Alhussain[1] and Steve Drew[2]

[1]School of ICT, Griffith University, Parklands Drive, Southport, Qld, Australia, t.alhussain@griffith.edu.au; [2]School of ICT, Griffith University, Parklands Drive, Southport, Qld, Australia, s.drew@Griffith.edu.au

Abstract. The paper discussed an exploratory study of government employees' perceptions of the introduction of biometric authentication at the workplace in the Kingdom of Saudi Arabia. We suggest that studying the factors affecting employees' acceptance of new technology will help ease the adoption of biometric technology in other e-government applications. A combination of survey and interviews was used to collect the required data. Interviews were conducted with managers and questionnaires were given to employees from two different government organisations in the Kingdom of Saudi Arabia to investigate the employees' perceptions of using biometrics. The results of this study indicate a significant digital and cultural gap between the technological awareness of employees and the preferred authentication solutions promoted by management. A lack of trust in technology, its potential for misuse and management motives reflect the managers' need to consider their responsibilities for narrowing these gaps. It was apparent that overcoming employees' resistance is an essential issue facing biometric implementation. Based on the research we recommend that an awareness and orientation process about biometrics should take place before the technology is introduced into the organisation.

Key words: E-government; Biometric technology; Users' perceptions; Kingdom of Saudi Arabia.

1 Introduction

New technologies constantly evolve new dimensions to daily life. They can be used to provide interactions between users and their governments through electronic services. Governments are looking for more efficient and effective uses of technology in order to electronically deliver their services [1, 22]. Electronic government (e-government) has therefore become an important world-wide application area.

With e-government applications, users are required to provide governments with personal information which necessitates an efficient, secure technology to provide reliable methods, particularly for users' identification as well as secure information systems. Thus, the implementation of e-government is facing important issues such as

information security, user authentication and privacy in which biometric authentication is a potential solution to deal with such concerns [13]. It can provide reliable identification of individuals as well as the ability for controlling and protecting the integrity of sensitive data stored in information systems [20]. As a result, several governments have implemented biometric authentication systems in order to efficiently and securely provide their services.

However, the adoption of biometrics in e-government has become a major component of political planning for several governments. In particular, user acceptance can be an essential factor for the successful implementation of biometrics [6, 18, 22]. Moreover, users can have a direct impact on the operational performance of biometric systems, so their concerns need careful consideration, even if their concerns are fairly rough and ill defined [6].

This paper discusses a study conducted in the Kingdom of Saudi Arabia of government employees' perceptions of the introduction of biometric authentication at the workplace in 2008. The aim is gain an understanding of factors affecting the employees' acceptance of biometrics and to advise on how to successfully adopt biometrics in e-government applications. The paper is structured as follows. The relevant literature is reviewed followed by the description of the empirical study that involved a descriptive survey and interviews of the managers and employees in two organisations.

2 Background

To introduce the context in which this study was undertaken it is necessary to consider the concepts of e-government and biometric authentication and how they relate to the technological sophistication of the major users. Saudi Arabia presents a unique set of cultural and technology uptake circumstances that have implications for management of a digital divide. We discuss the background to this enquiry in the following sections.

2.1 E-government

Electronic government involves the citizens of that country in certain government activities in order to help solve problems. E-government provides unparalleled opportunities to streamline and improve internal governmental processes, enhance the interactions between users and government, and enable efficiencies in service delivery [22]. It refers to the use of information technology by government agencies in order to enhance the interaction and service delivery to citizens, businesses, and other government agencies [1, 4]. Thus, there are four categories of e-government applications which are: Government-to-Citizen (G2C); Government-to-Business (G2B); Government-to-Government (G2G); and Government-to-Employee (G2E) [4].

2.2 Saudi Arabia and its Adoption of Technology

The Kingdom of Saudi Arabia is located in the Southern-Eastern part of the Asian continent. It occupies 2,240,000 sq km (about 865,000 sq mi) [25]. The total population reached 26,417,599 in mid-2005, compared with 24.06 million in mid-2004, reflecting an annual growth rate of 2.9 percent; however, 5,576,076 million of the population is non-Saudis [10].

Regarding Information Technology in the Kingdom of Saudi Arabia, national e-government program has been launched, early 2005, under the name Yesser, an Arabic word meaning "simplify" or "make easy". It plays the role of the enabler / facilitator of the implementation of e-government in the public sector. Its objectives include raising the public sector's efficiency and effectiveness; providing better and faster government services, and ensuring availability of the required information in a timely and accurate fashion. Yesser vision is that by the end of 2010, everyone in the Kingdom will be able to enjoy world class government services offered in a seamless, user friendly and secure way by utilizing a variety of electronic means [14].

2.3 Digital and Cultural Gap

Digital divide refers to the gap between the group of people that are very familiar and have good access to high technology and those who do not [7]. It can be a result of several reasons such as a lack of financial resources, great education, and computer literacy. However, the digital divide makes the successful of e-government applications challenging [3].

In the case of Saudi Arabia, a digital divide can be caused by the lack of knowledge and experience with technology, for instance, people in rural areas and inner city neighbourhoods may have less internet access than others, while those who have never used computers may simply be reluctant to use the new technology [1]. Moreover, Al-Shehry and others [3] indicated that there is a significant risk of a digital divide in Saudi society and even among employees in public sector since there are a large number of people and employees that are still not computer-literate. Evidence of digital and cultural gap between the technological awareness of government employees and increasing need to deal with new technology can be realized in the result section.

2.4 Biometric Authentication Technology

Biometric technology provides a range of automated methods which can used to measure and analyze a person's physiological and behavioral characteristics [27]. Physiological biometrics includes fingerprint recognition, iris recognition, facial recognition, and hand recognition. Behavioral biometrics contains voice patterns and signatures, which are usually taken for identification and verification purposes. Basic authentication is usually based on something somebody knows, like a pin or a password, or something somebody has, like a key, passport or driver's license. The limitations of these authentication measures in some application areas have led to the

development and adoption of biometric technology which is now used to identify individual behaviors and characteristics [27].

Biometric technology usually involves a scanning device and related software which can be used to gather information that has been recorded in digital form [8]. Having digitally collected the information, a database is used to store this information for comparison with the previous records. When converting the biometric input, namely the already collected data in digital form, this software can now be used to identify the specific inputs into a value that can be used to match any data previously collected. By using an algorithm, the data points are then processed into a value that can be compared with biometric data in the database [8].

2.5 Examples of Biometric Technology in E-government Applications

By using biometric technology, e-government aims to give its citizens improved services with efficient and secure access to information by providing reliable identification of individuals as well as the ability for controlling and protecting the integrity of sensitive data stored in information systems. Most researchers such as Ashbourn [6], Bonsor and Johnson [9], Scott [22], and Wayman et al. [27] argue that a wider use of biometric technology can be applied to e-government projects. Currently biometric technology is used for applications like e-voting to ensure that voters do not vote twice. With biometric technology, governments are better able to prevent fraud during elections and other transaction types. Moreover, biometric technology has most recently been used to ensure correct working times are recorded and that only authorized personnel have access to government property and resources.

Biometric technology can also be used by e-governments for business. For instance, banks frequently adopt a facial feature recognition system to ensure that there is a reduced potential for theft. For example, photos are taken on the bank slips which are stored on computer software. As a result, this has avoided the issue of fraudulent bank slips when withdrawing money at ATMs. These technological advances in authenticating dealings with business have helped the government to conduct its activities more effectively and more securely [9].

In business transactions there is frequently the need for full authentication of employees to ensure that, in case of any problem, management is in a position to identify the person responsible for that act. Commercial applications may also require full identification capability, digital certificates, human interface, and one or more authentication devices to ensure that the business can run safely and effectively. People are also in a position to do their business with increased trust. Digital trust through public key cryptography, strong authentication and certification allows greater transaction confidence as long as that organisation has a certified identity as an effective and trustworthy company [6].

Biometric technology is also used in the identification of citizens by e-government applications. Every nation could ethically be able to identify its citizens and differentiate non-citizens by using variations of national identification cards, visas, and passports with biometric data encoded within. Prior to the use of biometric data with such documents they were too easily forged or altered to allow unauthorized

access to resources and facilities. As a result many nations have avoided the use of mechanisms such as a national identity card in the past.

Effective e-government biometric applications to authenticate and identify citizens have effectively been used in reducing the issues of illegal immigration, access bottlenecks in busy facilities and high costs of employing security personnel. A good example is the United States whereby, since "September 11", it has widely adopted biometric technology. Two laws were made in the United States as a first mass deployment of biometrics. Seven million transportation employees in the United States incorporate biometrics in their ID cards. Moreover, in order to closely control visitors who enter and leave the country, all foreign visitors are required to present valid passports with biometric data; consequently, over 500 million U.S. visitors have to carry border-crossing documents which incorporate biometrics [6].

Several European governments have also started to implement the use of biometrics. The U.K. government has established issuing asylum seekers with identification smart cards storing two fingerprints. General plans have also been made to extend the use of biometrics throughout the visa system in the U.K. as well as in France, Germany and Italy [22].

The Australian Customs established an automated passenger processing system, that is, the e-passport SmartGate at Sydney and Melbourne airports, and it aims to introduce self-processing by employing facial recognition systems to confirm identities and streamline the travelers'' facilitation procedures [24].

E-government facilities use the various types of biometric identification in order to control certain illegal behavior. For example, the Japanese government plans to use biometric technology in passports to tackle illegal immigration and to enable tighter controls on terrorists. This will be applied within a computer chip which can store biometric features like fingerprints and facial recognition [22].

Other e-government applications are using the biometrics for certain defense bases for secure areas. For instance, hand recognition has been used at the Scott Air Force Base to save more than $400,000 in manpower costs through their metro-link biometric access gate [17].

2.6 Concerns about the Use of Biometric Technology

While biometrics can provide a high level of authentication through identifying people by their physiological and behavioural characteristics, there are also several negative aspects. Biometrics can sometimes be ineffective when using the various styles of identification. For instance, fingerprints can be saturated, faint, or hard to be processed with some of devices, particularly if the skin is wet or dry. Hand recognition can sometimes be ineffective when the hand is damaged, thereby no results will be obtained to match with the images already in the database. Few facilities have databases or hardware to employ iris recognition, which makes the upfront investment too high to initiate a worldwide iris ID system. Biometric technology has also been criticized for its potential harm to civil liberties. This is because people have been denied access to the various regions and countries simply because they do not have the correct identities for those places. Moreover, there is potential for people's privacy to be violated with this new technology [8].

3 Methodology

The review of the current literature on biometric applications guided our research and the literature on methods available for an exploratory study. Given the exploratory nature of the study the two research questions were aimed at providing descriptive information on the perceptions of current and potential users of biometric application. The research was designed to answer the following questions.

1. What are the managers' perceptions regarding the use of biometric authentication in e-government applications?
2. What are the employees' perceptions regarding the use of biometric authentication in e-government applications?

Given the two distinctive groups of people – managers and employees - involved the research was carried out in two distinct stages.

Method of sampling was purposive. This method of sampling [19] is a strategy in which "particular settings, persons, or activities are selected deliberately in order to provide information that can't be gotten as well from other choices" (p.88). A selection of knowledgeable interviewees was approached.

The literature on user acceptance of new technology was used to design the questionnaire. The interviews were to discuss the questions in more detail and to gain further understanding on the factors that influence the use of biometric application, such as authentication.

Two distinct stages were designed in this research, each using a different method and each with a particular focus. A mix of qualitative methods and user groups provides rigor through triangulation and quantitative techniques provide useful trend analysis. Thus the use of the multiple or mixed methodology with both qualitative and quantitative aspects compensates for the weakness of one method via the strengths of the other method [21]. A combination of qualitative and quantitative methods in the research "may provide complementary data sets which together give a more complete picture than can be obtained using either method singly" [26, p.197]. Additionally, the use of multiple qualitative methods enhances the richness and validity of the research [21]. In particular, interviews were conducted with managers and questionnaires were given to employees in order to investigate their perceptions regarding the use of biometrics.

3.1 Interviews

Interviews with knowledgeable individuals are recommended as an appropriate method to narrow down the scope of the research and investigate the range of issues [23]. In this research, face-to-face interviews were conducted in the Kingdom of Saudi Arabia with eleven managers of the General Organisation for Technical Education and Vocational Training and the Royal Commission for Jubail and Yanbu. However, the participants were selected at different management levels. In order to obtain personally meaningful information from the participants, open-ended questions were used for the interviews [21].

3.2 Questionnaire

The questionnaire was used for data collection for this research as it is an efficient means to gain data from a large participant group, it is an appropriate method to answer the research questions, and it is an effective method to investigate people's attitudes and opinions regarding particular issues [16]. In this research, a total 101 participants completed the questionnaire, and they are all employees in one of these two organisations: the General Organisation for Technical Education and Vocational Training and the Royal Commission for Jubail and Yanbu.

3.3 Data Collection and Analysis

As mentioned, the data of this research were collected through face-to-face interviews and questionnaires as well as the literature review. The justification for using different techniques for collecting the data is triangulation to provide verification. Triangulation refers to the use of several different methods or sources in the same study in order to confirm and verify the data gathered [21].

In the interview, all participants were asked if the interview could be recorded, and none of them objected. The expected maximum time for each interview was 60 minutes; however, the actual time for each recording was about 25 to 40 minutes. Notes were taken during each interview as a safeguard against recording failure. Afterwards, all interviewees' answers were categorized according to each question of the interview and they are presented in the results section.

In the questionnaire, permission from the surveyed organisations as well as all the managers of the participating employees is gained to distribute the questionnaire to the employees. However, all responses were stored in the SPSS (Statistical Package for the Social Science) software which was used for the analyses. Statistical analysis includes the frequency and the percentage of each category of the responses for each answer, the Chi square value and its level of significance.

4 Results

It is noteworthy that the two investigated organisations implemented fingerprint scanners for proving employees' attendance. Previously, manual signature recording was the official process for proving employees' attendance in most agencies in the Kingdom of Saudi Arabia. In this process, the employee has to sign and record attendance twice a day, at the beginning of the work day and at the end as well. This process has several negatives, because the employees may sign for others and may not write the correct time of signing. Therefore, this was not an effective or efficient process for recording attendance, and was considered a good reason for implementing biometric technology.

However, in this section we will present just a number of our survey questions which are relevant to detecting problems in this context and seeking solutions to reducing the digital and cultural gap.

4.1 Interview Results of Managers

A question by question analysis is presented as follows:

4.1.1 What cultural gap do you perceive between the employees' level of technological experience and the level of biometric technology that is being deployed?

This question investigates the cultural gap between the employees' level of technological experience and the level of biometric technology that is being deployed in their organisation. Nine of the respondents to this study agreed that there is a cultural gap between the employees' technical cultural levels and the level of technology being used, but they attributed this gap to different reasons, as follows:

- Four respondents attributed the technical cultural gap of the staff to their levels of technological literacy.
- Two respondents attributed the technical cultural gap to the employees' age; that is, the older the employee, the wider the gap.
- One respondent attributed the cultural gap to a perception that use of this technology indicates a level of mistrust of employees by management causing them not to want to use the technology
- Two respondents did not attribute the cultural gap to a particular reason.
- Two other respondents did not agree that there is a cultural gap at all.

4.1.2 Do you accept a level of responsibility for narrowing this cultural gap?

This question investigates the managers' perceived responsibility for narrowing the cultural gap between their employees' level of technological experience and the level of biometric technology.

- Five of the interviewed managers felt that they are responsible for narrowing the cultural gap; they proposed procedures concentrating on enhancing employee awareness of technology and its utilities.
- Four respondents did not consider that it was their responsibility to narrow the cultural gap.

4.1.3 Have you experienced any difficulties in dealing with this technology? If so, what were they?

This question investigates the managers' points of view regarding the difficulties in dealing with biometric technology in their workplace. Regarding the difficulties being experienced, 11 responses were presented by the interviewees, distributed among the following categories:

- Employee resistance (11 respondents);
- Disabling and breaking the fingerprint device by some employees (4 respondents);
- System failures (5 respondents); and,
- System unable to take fingerprints from some users (7 respondents).

4.1.4 What are the main barriers (inconveniences) of applying biometric technology in your organisation?

This question investigates the managers' point of view regarding the main barriers of applying biometric technology in their organisations.

- All responses to this issue were related to digital and technological culture as well as resistance to change that was evidenced by the employees at the beginning of the deployment.

4.1.5 How do you think the use of biometric technology affects self perceived social level of your employees?

This question investigates the social impact of the use of biometric technology on the employees themselves and among their society. A wide range of responses were provided regarding the social impact of the fingerprint technology; these responses showed contradictions regarding the effects on hardworking employees.

- Six respondents said that there were positive effects as regulation became stricter.
- Five respondents highlighted the negative effects of using this technology. However, they attributed the positive and negative effects to the following:
- Three respondents raised the issue of mistrust concerns that the employees may feel. They feel the perception that their managers do not trust them and that this may reflect badly on them in their society as other people may mistrust them as well.
- Four respondents commented that this type of regulative technology has reported positive effects on all types of employees, especially when comparing with other employees who do not use this technology. For example, one response said that I feel proud with my friends that I use this new technology while they do not.

To sum up, managers' responses to all questions indicated that there is a digital and cultural gap evidenced by the technological awareness of employees and the preferred authentication solutions promoted by management. This digital and cultural gap creates a resistance to change by the employees which reflects on the acceptance and adoption of new technologies such as these.

4.2 Questionnaire Results of Government Employees

As mentioned before the questionnaire was distributed to 101 government employees and a question by question analysis is presented in this section. Questions were presented as a five point Likert scale (1 to 5) where 1 is the lowest level of importance and five is the highest. There was an "opt out" option if the respondent did not know the importance or relevance of the question's concept. Likert responses have been generalised to provide a preliminary analysis view.

4.2.1 How important do you think the use of biometric technology is to the organisation?

Responses to this question examine the users' points of view regarding the level of importance that the employees think the organisation places on the use of biometric technology. The responses were as the following:

- No one of the respondents think that it is not important.
- 23.8% feel that it is important.
- 13.9% feel that it is very important.
- A minority (45.5%) of the respondents have no idea of the importance of using fingerprint technology in their workplace.

4.2.2 How important do you think it is that there should be an awareness of this technology before its implementation?

Responses to this question examine the users' points of view regarding the importance of awareness before implementation of the used biometric technology. The concept of awareness includes aspects of notification, information and education of employees. All respondents classified the level of importance as follows.

- Only 5% of the respondents feel that it is not necessary to promote employee awareness of the technology before the implementation.
- 15.8% think that it is important.
- A majority (52.56%) of the respondents perceived that it is very important to have awareness before using fingerprint technology.

4.2.3 Do you think that the use of this technology in your workplace means that employers mistrust employees?

Responses to this question examine the users' points of view regarding the perception of employer mistrust created by introducing and using biometric technology. There is a significant difference among employees' responses as follows.

- 33.7% of the respondents state that it does not mean mistrust.
- 11.9% think that it means mistrust.
- 22.8% think that it certainly means mistrust.
- 33.7% of the respondents are unsure if it means mistrust or not.

5 Discussion

The results indicate that nine of the interview respondents agreed that there is a digital/cultural gap created by the employees' low familiarity with technology and the organisation's adoption of biometrics. This has been supported by several studies; for instance, Ashbourn [6] stated that education is an essential phase that users need. The organisation that is going to implement such biometric technology has to communicate with users in order to provide them with a good understanding and overview about biometrics, how this technology works, and the reasons for its implementation. Moreover, if this information is presented in an attractive and truly informative manner, the organisation will achieve much in warming users towards the project and raising their confidence regarding the implementation of this technology.

In addition, this result reflects some of the literature findings regarding the challenges in the implementation of e-government in the Kingdom of Saudi Arabia. These might be summarized as the weakness due to the lack of social and cultural awareness of the concepts and applications of e-government, the extent of computer

illiteracy, as well as the deficiency of the official education curricula in addressing the information age. However, the result of this study supports the finding which reveals that there is a need programs related to the application of e-government [2, 5].

Only five of the interviewed managers felt that they are responsible for narrowing the technological cultural gap. This result concurs with Ashbourn's [6] finding that managers need some in-depth training in order to understand the various issues regarding the introduction and use of such technology. In particular there is a need to be able to fulfill their roles regarding the ongoing running of the application and user acceptance and understanding. Therefore, such training may lead managers to narrow the technical cultural gap.

It is important to note that employee resistance is an essential issue facing organisations, as mentioned by all respondents through their answers to several questions. Several employees have tried to prevent the use of this technology in many ways. Four interviewees clarified that some employees had tried to break down the device which meant that some managers had to install cameras in order to catch the person and prevent this from happening. Furthermore, some employees tried to distort their fingers by injuring them or rubbing them on wood in order to make the system unable to read their fingerprints in an attempt to prove this technology to be ineffective. In addition, this result relates with the literature finding where Alsuwail [5] and Alshareef [2] confirmed resistance by employees to change as one of the challenges of implementing e-government in the Kingdom of Saudi Arabia. This has been supported by Feng [15] who stated that one of the main barriers to implementing e-government is the need for change in individual attitudes and organisational culture. Furthermore, user acceptance and perception problems relating to the implementation of the new technology have been clarified by Giesing [18] as factors that would prevent an organisation from implementing or adopting biometric technology.

Furthermore, the interviews provided a wide range of responses regarding the social impact of the fingerprint technology. Six respondents said that there were positive effects through the regulation of attendance and working hours. On the other hand, five respondents highlighted the negative effects of using this technology, which relate to the literature finding by Coventry [12] who highlighted the weakness of the social and cultural awareness of the concepts and applications of e-government. Coventry continued that the usability and acceptance of biometric services can be affected by the context of use as well as the social issues, such as the perceived benefits to the user and the perceived privacy risks. Application contexts with obvious, apparent benefits and low risks may lead to greater perceptions of usability and higher acceptance opinions of biometrics than contexts where there are little obvious benefits and high risks.

On the other hand, a minority (45.5%) of the employees had no idea of the importance of using fingerprint technology, which may relate to the shortage of any awareness program that the employees could undertake before using such technology. This supports the challenges of implementing e-government in the Kingdom of Saudi Arabia which indicate a scarcity of information programs related to the application of e-government, the deficiency of the official education curricula in addressing the information age, and the lack of computer literacy among citizens [1, 2, 5].

A small majority (52.56%) of the respondents perceived that it is very important to have an awareness of the introduction and implications of the technology through

information and education programs before using fingerprint technology. Change resistance might also be a key factor here. In fingerprint technology contexts in Saudi Arabia, many people raise the issue of radiation risks that they think are associated with using these systems, as well as the disease transfer by every employee touching the same point, which was also illustrated in other responses to the interviews. These concerns will simply be reduced as the levels of awareness increase, and as the usual habits continue after adaptation to this technology takes place. As stated, a weakness of the social and cultural awareness of the concepts and applications of e-government has been noted in the literature by Alshareef [2] and Alsuwail [5] as well as a scarcity of education programs related to the application of e-government. Moreover, Alharbi [1] clarified that society lacks awareness about e-government advantages and benefits. However, a study by Giesing [18] noted that the employees expressed the need for more information about biometric technology in general and for more detailed information on the specific biometrics that will be used, as they only had basic knowledge of biometrics. Giesing's study shows that employees would like to know more regarding biometric technology, such as background information, advantages and disadvantages, user guides on the use of the biometrics, technical specifications, the storage of biometric data, as well as the security and privacy issues. Furthermore, Ashbourn [6] stated that the education phase of implementing technology is very important for users in order to provide them with a good understanding and to make them more confident in its use.

A significant 33.7% of the respondents to the survey section of this study do not know whether introduction of this technology indicates mistrust and 22.8% of them think the use of this technology certainly means employers mistrust employees. This may be attributed to various factors including a lack of awareness through consultation, notification, information, and general levels of computer literacy. The scarcity of programs related to the application of e-government may also explain these some of the results. As 33.7% of respondents do not feel that it signifies mistrust of employees and these may relate to the proportion of the user population with higher levels of the familiarity with technology, its adoption, convenience and usefulness which they may have experienced elsewhere.

6 Conclusion

A study was undertaken to investigate government employees' perceptions of factors relating to the introduction of biometric authentication at the workplace. This was undertaken to determine how best to gain employees' acceptance of biometric in order to successfully adopt biometrics in e-government applications. Results supported a number of findings reported in literature regarding user acceptance and adoption of biometrics and e-government technology. Analysis of results shows that an awareness and orientation process about biometrics should take place before the technology is introduced into the organisation. This is highlighted as all managers expressed employees' resistance to the technology's installation at the beginning of its implementation. The employees should be made aware about the use of the new technology, the purpose of its implementation and the benefits. Since about half of the

managers had not considered their responsibilities for narrowing the digital and cultural gap regarding the fingerprint technology, it is recommended that managers should be made aware of their responsibilities in this issue. They should recognize that digital and cultural gap in technological awareness exists and that they have to act as leaders and role models for their employees. Finally, as the managers have a big part of the responsibility to successfully implement biometric technology in their organisations, they need to gain a detailed understanding of this technology and preferably have a basic background about Information Technology as well.

References

1. Alharbi, S.: Perceptions of Faculty and Students toward the Obstacles of Implementing E-Government in Educational Institutions in Saudi Arabia. West Virginia University (2006)
2. Alshareef, T.: E-Government in the Kingdom of Saudi Arabia, Applicational Study on the governmental mainframes in Riyadh City. King Saud University, Saudi Arabia (2003)
3. Al-shehry, A., Rogerson, S., Fairweather, N., Prior, M.: The Motivations for Change towards E-government Adoption: Saudi Arabia as a case Study, eGovernment Workshop. Brunel University, West London (2006)
4. AlShihi, H.: Critical Factors in the Adoption and Diffusion of E-government Initiatives in Oman. PhD thesis, Victoria University, Australia (2006)
5. Alsuwail, M.: Directions and local experiences, Foundations and Requirements of E-Government. E-Government Conference, Institute of Public Administration, the Kingdom of Saudi Arabia (2001)
6. Ashbourn, J.: Practical biometric from aspiration to implementation. London: Springer (2004)
7. Blau, A.: Access isn't enough: Merely connecting people and computers won't close the digital divide. 33(6), pp. 50-52. American Libraries (2002)
8. Bolle, R., Connell, J., Pankanti, S., Ratha, N., Senior, A.: Guide to Biometrics. New York: Springer (2004)
9. Bonsor, K., Johnson, R.: How Facial Recognition Systems Work, How Stuff Works, viewed on 1st October 2007 at http://computer.howstuffworks.com/facialrecognition.htm.
10. Central Department of Statistics & Information (CDSI), (2009). Available at http://www.cdsi.gov.sa, The Kingdom of Saudi Arabia.
11. Central Intelligence Agency (CIA): The Word Fact Book. (2009). Available at https://www.cia.gov/library/publications/the-world-factbook/
12. Coventry, L.: Usable Biometrics, Security and usability. Chapter 10, pp. 181-204. Human Centred Systems Group, University College London (2005)
13. Dearstyne, B.: E-business, e-government and information proficiency. Information Management Journal, Vol. 34, No. 4 (2001)
14. E-government Program (Yesser). The Ministry of Communications and Information Technology (2009). Available at http://www.yesser.gov.sa.
15. Feng, L.: Implementing E-government Strategy is Scotland: Current Situation and Emerging Issues. Journal of Electronic Commerce in Organizations 1(2), P. 44-65 (2003)
16. Fraenkel, J., Wallen, N.: How to design & evaluate research in education. United States, New York: McGraw-Hill (2000)
17. Frees, R.: Biometric technology improves identification security. U.S. Air Force (2008). Viewed on 3rd March 2008 at http://www.af.mil/news/story.asp?id=123084564.
18. Giesing, I.:, User response to biometric. University of Pretoria. pp. 95-135 (2003)

19. Maxwell, J. A.: Qualitative Research Design: An Interactive Approach (2nd Ed). Thousand Oaks. Sage Publication (2005)
20. McLindin, B.: Improving the Performance of Two Dimensional Facial Recognition Systems. University of South Australia (2005)
21. McMurray, A., Pace, R., Scott, D.: Research: a commonsense approach. Melbourne: Thomson Social Science Press (2004)
22. Scott, M.: An assessment of biometric identities as a standard for e-government services. Services and Standards, Vol. 1, No. 3, 2005, pp. 271-286 (2005)
23. Sekaran, U.: Research Methods for Business: A Skill Building Approach. 4th edn, John Wiley & Sons Inc, New York (2003)
24. The Annual Report of the Australian Customs Service (ACS) (2005). available at http://www.customs.gov.au/webdata/resources/files/ACSannualReport0405.pdf.
25. The Saudi Network, available online at http://www.the-saudi.net/, viewed on 14th of January 2009.
26. Tripp-Reimer, T.: Combining qualitative and quantitative methodologies. In M. M. Leininger (Ed.), Qualitative research methods in nursing, pp. 179-194, Orlando, FL: Grune & Stratton (1985)
27. Wayman, J., Jain, D., Maltoni, H., Maio, D.: Biometric Systems: Technology, Design and Performance Evaluation. New York: Springer (2005)