Journal of Information Security, 2015, 6, 93-100
Published Online April 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.62010

Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities

Eugen Harinda, Etienne Ntagwirumugara

Department of Electrical and Electronic Engineering, College of Science and Technology, University of Rwanda, Kigali, Rwanda
Email: harindaeugen@yahoo.com

Received 14 January 2015; accepted 27 March 2015; published 31 March 2015

Abstract

Biometric authentication systems are believed to be effective compared to traditional authentication systems. The introduction of biometrics into smart cards is said to result into biometric-based smart ID card with enhanced security. This paper discusses the biometric-based smart ID card with a particular emphasis on security and privacy implications in Rwanda universities environment. It highlights the security and implementation issues. The analysis shows that despite the necessity to implement biometric technology, absence of legal and regulatory requirements becomes a challenge to implementation of the proposed biometric solution. The paper is intended to engage a broad audience from Rwanda universities planning to introduce the biometric-based smart ID cards to verify students and staff for authentication purpose.

Keywords

Biometrics, Security, Privacy, Smart ID Card

1. Introduction

Authentication mechanisms to identify or verify the validity of an individual requesting access to secure locations may be knowledge-based, possession-based, physiological-based or behavior-based [1]. Knowledge-based and possession-based authentication systems may be easily fooled as no link between the individual and the authenticator. Biometric-based authentication systems employ advanced security capability in that individual authentication depends on who you are or what you do rather than what you have or know. Biometric system is effective; however, people are more concerned with significant breach of privacy. To combat the identity fraud

How to cite this paper: Harinda, E. and Ntagwirumugara, E. (2015) Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities. *Journal of Information Security*, **6**, 93-100.
http://dx.doi.org/10.4236/jis.2015.62010

in identity documentations, the unbeatable approach is the use of biometric technology depending on the application [1]. This would limit access to specific areas where information and other important activities are being done. Individual biometrics features have different strengths and weaknesses and there is no single biometric method that can serve all applications required [2]. The choice of the biometric technology depends on the type of applications and its complexity of implementation otherwise all the biometric technologies are capable of providing the required security [2].

In this paper, biometric methods are discussed with comparison of strength and weakness. Various biometrics have various working characteristics and the accuracy differs according to the design of operation of each biometric. Biometrics level of security is also different and they exhibit different kinds of errors which may be subject to denial of access to the biometric sample holders owing to various factors such as physical damages, aging, cold, weather etc. [3]. The long-term stability is very important while choosing biometric methods due to market availability of devices and system operations know-how (**Table 1**). The paper discusses the biometric security effectiveness and application scenario of biometric-based smart ID card. However, the effectiveness of the biometric security cannot guarantee the required security. It is important that the universities consider the implementation of biometrics while considering the human force to closely monitor the operations of the system as system error might happen or internally staff might interfere and leak students and staff biometric information. All biometric existing systems experience false acceptance, false rejection and fraud issues caused by various conditions common to the human-machine interface [4]. The paper provides recommendations to the Rwanda universities regarding the implementation of biometric-based smart ID card for security enforcement and privacy mitigation. This involves the choice of the biometric technology for use in the universities environment considering the class of people to deal with and the ease of biometric technology use in universities while of course considering security and privacy of people's information. The application scenario of biometrics is also important. After understanding why to use biometrics, it's important to understand and identify where to use the technology and how to implement it while considering the cost of implementation and operational maintenance.

2. Biometrics Methods

Biometric is a method used to identify an individual or verify an individual who claim an identity based on behavioral characteristics or physiological features. A biometric system operation is based on pattern recognition that operates by capturing data from an individual and comparing the features contained in a captured data with the features of the stored data in the system's data base [5]. Below is a brief description of biometric methods.

2.1. Fingerprint

Fingerprint is a pattern of ridges and valleys on the surface of a fingertip. The fingerprint recognition system extracts the features from marks made by ridges and valleys for comparison with the stored template. The system has competitive accuracy in that even fingerprints of identical twins are different and so each person's figure tip has a unique surface finger print [5].

Table 1. Comparison of some most used biometrics [10].

Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of use	High	High	low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long term stability	High	Medium	High	High	Medium	Medium	Medium

2.2. Facial Recognition

Make individual identification by analyzing face features that cannot be easily changed. The approach to differentiate and identify faces is based on location, size, and shape of facial features such as eyebrows, eyes, nose, lips, cheekbones, chin and jaw. Facial recognition is a non-intrusive method and can be taken by using digital camera or CCTV for remote video surveillance camera. It has difficulties on how to obtain facial images from different viewing angles, under poor light conditions, or if hair, sunglasses, or hats cover an individual's face [6].

2.3. Iris Recognition

The iris recognition system uses iris which is the region of the eye bounded by the pupil and sclera. The biometric technology put landmark features, such as the outer iris boundaries and the pupil in the center of an eye to aid marking the iris' borders, high quality cameras are then used to illuminate the eye and take the iris features without causing damage or embarrassment because the cameras are said to emit infrared light. The iris recognition system extracts, examines the iris patterns, keep the template. It is almost impossible to change the surface or quality of iris [6].

2.4. Speaker Recognition

Speaker recognition uses a combination of physiological features and individual behavioral [7]. The system uses voice prints of speakers and other measurable characteristics of human voice to identify speakers'. Individual's voice features are based on vocal tracts, mouth, nasal cavities and lips. A person is requested to speak a word or phrase a number of times, speaker recognition system captures the sample [8]. A template is generated and stored for comparison in the future. Speakers are used in telephone based applications.

2.5. Signature Recognition

In signature recognition system, signature data is captured using pens that have sensors or through touch-sensitive surfaces which senses an individual unique signature characteristics such as stroke order, velocity and acceleration, the applied pressure, the pen-up movements and the angle which the pen is held. The dynamics information is captured and stored as a template [9]. The system can be used in banking applications and access control to confidential documents, contracts etc.

2.6. Hand Geometry

The system examines and evaluates the shape of the hand. It has shown good performance and it is comparatively simple to utilize. Hand geometry has been used and it is widely appreciated [9].

3. Security and Privacy Implications in the Deployment of Biometric-Based ID Card

The main worry is that biometric is exceptionally efficient authentication machinery**,** but when used in a bad way the technology can guide to unwanted privacy concern [10]. Some professionals and activists alarm that the biometric smart ID card could show the way to breach of the basic rights and freedoms of persons. The collections of biometric information about persons have increased obvious and significant concerns. It employs physical and an informational prospect of privacy since it does not simply gather information about individual but somewhat, individual information [11]. Privacy is the ability to lead your life free of intrusions, to remain autonomous, and to control access to your personal information. Numerous privacy fears contain the utilization of biometrics for individual recognition. Biometric system raised concerns three orderly privacy concerns [12].

3.1. Unintended Functional Scope

Since biometric identifiers are in origin biologically, collection agent might reap extra individual information from scanned biometric criterions [13]. Human fast advancements in genetic research have developed fears that deducing additional information from living criterions may as well be done leading to orderly favoritism resulting from natural information being used against section of population seeming as risky.

3.2. Unintended Application Scope

Biometric identifiers permit the feasibility of undesired identifications [13]. For instance, individuals who possess aliases legally, let say for security grounds might be identified by their biometric data. Additionally, biometric identifiers can connect bit and pieces of behavioral information regarding persons registered in a broadly various practices. An enemy can regularly read this potentiality in the same way for organizations, government or corporate to build up power over persons and their financial system.

3.3. Covert Recognition

Biometric features are not top secrets. Even without awareness of individual's knowledge, it is normally possible to get individual's biometric sample such as individual's face which allow secret recognition of formerly registered people [13]. Accordingly, persons who wish to stay unidentified in any specific circumstances could be disallowed their privacy by biometric recognition.

The biometric security design system gives a level of elasticity in the way the actions of enrollment, authentication, identification, and arrangement for the long-term storage space [10]. Only some systems involve the requirement to store data locally within a biometric device while other systems have need of a distributed database that embraces numerous individuals' biometric templates. The private and exceptionally sensitive nature of a biometric data means that there are major privacy and security threat linked with capture, storage and use of biometric security system's data [13] [14]. Theft of individual's identifiers such as address, social security number, name, religion, sexual preferences, medical history, and photography are implicated.

To deal with likely mistreatment of biometric information and related responsibility procedures, particular rules are necessary to make sure that data cannot be utilized outside the intention it was formerly collected for [15], but this cannot always be assured. It is paramount to apply national laws in relation to data protection appropriate to requirement like responsibility to hold data suitably and securely, and make use of personal data with lawful and for clear purposes. Tough regulations functional to sensitive data related to races, origin, ideology, health, religion, or sexual life. The important aspect is that people must understand that the purpose of biometric system technology is not intended to breach privacy rather how it is used and that a biometric system store up a tiny file resulting from the individual features of individual's biometric data called template [16]. There is no biometric system that does not involve some privacy loss whenever personal information is stored somewhere the owner has no control for authentication [11]. Trade-off of privacy against the required security has to be done. There is need for appropriate use of the biometric data that is founded in law, legitimate public policy which also relates to the purpose of biometric data collection and storage. It is important to refrain to areas of heightened privacy protection concern such as medical and financial status of persons. Limited information collection is adequate for universities biometric system.

4. Security Effectiveness of a Biometric System

The biometric system performance depends on technical, set-up and operational analysis [12] Biometric identifiers such as hand, iris and face have limitations that greatly affect the performance biometric systems. The performance of a biometric system can be affected by any user in any system's application and environment. The evaluation of biometric system effectiveness is done based on performance of its recognition system [13]. During the placement of biometric systems in the universities, the quality and roughness of biometrics sensors, the quality of communication interfaces, the ease of use, acquisition and processing speed are important consideration parameters. The stored characteristic of a person greatly affect the performance of a biometric system [14]. The biometric matching system is naturally a matching score which compute the resemblance involving the input as well as the stored template depiction [12]. However, if biometric system's sensor is of poor quality, the performance of recognition algorithm is affected leading to errors in resemblance. As various sensors are used during enrolment, the evaluation of biometric system effectiveness can be done based on the resistance of recognition algorithm against the use of various sensor types. Primarily, the rate of correct verification of legitimate users and the percentage rate that a biometric presents a false acceptance measure the system verification effectiveness [13] [14]. In a verification system, factors like aging and nature conditions can modify user's physiological or behavioral personality thereby causing two error rates namely false rejection rate (FRR), that is, rejection of a legitimate user and false acceptance rate (FAR), that is, impostor acceptance [15]. The system takes a decision to reject or accept a user by comparing the system's answer to the system set threshold [17]. The FAR and FRR are thus dependent on this set threshold which can be adjusted to reduce the system's error rates. The biometric system set a threshold value which is a number to control the biometric system judgment. The biometric system conclude that pairs of biometric samples are mate pairs or non-mate pairs if matching score is higher/equal to the set threshold value or lower than the set matching threshold value. A functional biometric system performs a trade-off between the FAR and FRR [18]. In other words, the Biometric system checks for a probability of a user being a legitimate user or an impostor. It results into a test of a system usability and security. This means that both FAR and FRR are a function of a set threshold value. The decision threshold should be adjustable to desired security characteristics of the application. In some applications, high FRR rate is a vital system design requirement while in other applications FAR rate is a fundamental system design requirement [15]. Applications requiring high security level need low FAR, a fact that sees FRR increasing while applications demanding low security level careless in terms of FAR, **Figure 1**. The Biometric performance level introduces many issues when using biometric technology and systems [17]. Rwanda Universities have to consider that there exist variations in the biometric system's ability to access authorization adjustment based on the system's sensitivity to the threshold value. Biometric systems manufacturer's system specification is important. The adjustments to reduce system threshold value to deal with tolerance to input variations in students environment might be necessary and will increase FAR meaning that the system can easily grant access to unauthorized students or staff while the increase in system threshold value to make the system more secure increase FRR which implies the system might deny access to even authorized students or staff. Great care should be taken so that inaccuracy of the systems to grant access does not make severe academic concerns such as delay in examination rooms or access to Universities resources, offices etc.

5. Application Scenarios of Biometric-Based ID Card in Rwanda Universities

The combination of biometrics with the smart card is a practical application for biometrics in the Rwanda Universities. This means that the system will be operating in verification mode. Biometric smart ID card is furnished with microprocessor and memory. It is portable and smart tool able to maneuver and store data [19]. Importantly, places where biometric template is stored and system configuration will result into diverse security and protection capabilities. Biometric template can be stored on smart ID card and match takes on place similar smart ID card allowing students and stuff to hold their biometric information [20]. Fingerprints are easy to implement in Universities environment and widely used, making it the preferred biometric template. The biometric readers can be placed at all locations that the Universities wish to secure as the system does not require the cen-

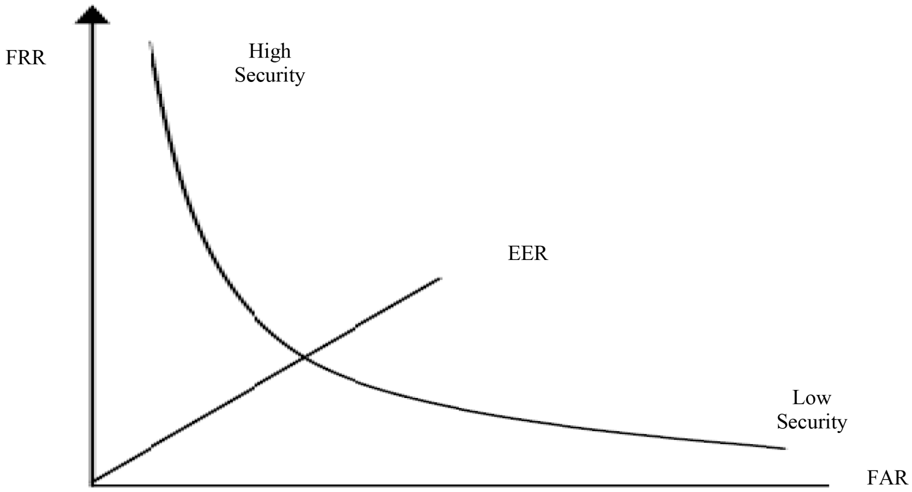

Figure 1. Biometric receiver operating characteristic curve [16].

tral servers. When a student/staff places his/her biometric smart ID card on the smart card reader, he/she is required to issue a fingerprint which in turn trigger the card to match the own stored template against the presented template and then send the matching decision to the card reader [19]. The biometric smart ID card can be used to control access to universities most important locations such as examination and server rooms to ensure authorized access. Libraries can use smart card ID to control access and manage the use of available resources thereby replacing the barcode cards (if any) which can be exchanged. Biometric smart ID card can be used to record and provide administration with certain evidence of students and staff attendance for accuracy and analysis reporting. Students will be required to be present to class rooms and examination rooms according to the timetable. This will phase out manual attendance where all university students are required to sign attendance lists to justify the presence. The application of biometric smart ID card in halls of residence will be guarantee enhanced security.

Similar to other technologies, biometric smart ID cards are susceptible to hardware and software assaults [20]. Given that a contactless smart ID card is a wireless device, it is susceptible to assault at the far distance. Security violation can happen at level of the card, in the supporting communication network or in the backed system. The biometric smart ID card security and privacy can be threatened by the attacks such as reverse engineering of the biometric template which might result to a transformation of the image of the physical feature, power analysis attack which intends to take back information by examining adjustments in the power utilization of a device [20]. Other possible security attacks include Clandestine scanning which is a secretly reading of the electronic information of an electronic ID card with no permission and perhaps the awareness of the card owner, Clandestine tracking which is a straight menace at persons since it is able to disclose the biometric ID card owners activities to expose venue privacy, card cloning which is a type of spoofing that capture information from a lawful ID card and afterward makes an official copy of the captured sample in a fresh chip, Skimming of biometric ID card's chip and even when the ID card is in pockets and eavesdropping during transmission between biometric ID card chip and biometric ID card-reading system [21]. The application of this biometric-based smart ID card is based on verification. It is privacy-friendly as a person makes claim about the identity by presenting the smart ID card and the claim is verified with the biometric characteristic stored on a smart ID card.

6. Challenges to Implementation of Biometric-Based ID Card in Rwanda Universities

6.1. Legislation and Regulatory Requirements

Without legislation and regulations relevant to the use of biometric technology, the implementation and operation of a biometric-based smart ID card technology to improve identification services in the University environment without compromise of privacy is a challenge. This could be an issue during the system design and deployment. It is necessary that all biometric systems exist within a legal jurisdiction [22]. Rwanda has no biometrics privacy protection laws, a fact that poses a challenge to privacy protection. There is need for specification of the kind of biometric information to be collected and use within the system and any other system that may share this data.

6.2. Human Resource

Though the biometric is a mature technology [23], it is still new to parts of the developing world. Rwanda like any other developing country lacks skilled human resource. There is training need for university technical staff to acquire knowledge and skills for the implementation and maintenance of the biometric technology. Prior to implementation the universities need to look for specialist assistance to develop the implementation strategy and well established clarity of universities' biometric system purpose. Without maintenance staff, sustainability will not be possible. It also involves examination and assessment of security requirements in accordance to the universities requirements. Also, this includes the determination of physical and technical specifications of the biometric equipments and necessary systems to be installed.

6.3. Biometric Technology User Acceptance

The system must be resilient. As researches found [24] [25], user acceptance is an important factor in the implementation of biometric systems. As users have impact on biometric systems operational performance, it is essential to address user concerns even if not felt necessary by the universities administrators to attain user confidence during the biometric system registration.

7. Recommendations

Rwanda Universities are recommended to use fingerprint biometric technology. Fingerprint is one of the top known and widely used biometric technologies [26]. There are many vendors of fingerprint biometric system, standards and has the highest market share which make fingerprint biometric devices affordable. Fingerprint standardization and advancement would make the biometric security implementation cost effective for Universities due to interoperability and easy of choice of equipments availability from suppliers and would offer cheap running and maintenance cost. It is easy to use fingerprint biometrics as it has high public acceptance record and hence suitable for use in the student and staff environment. The availability of alternative system vendors would help to obtain the system with reasonable threshold value specification which achieve security requirement while making trade-off between false match rate and false non-match rate which be rise due to error incidences due to dry and dirt fingers. Rwanda Universities are recommended to adopt Biometric template-on-card and matching-on-card (**Figure 2**) as it guarantee security and overcome privacy concern since students and staff keep their own biometric information. In order to address the privacy concerns, the universities are also recommended to strengthen legal and regulatory mechanism, to develop and implement policies which are clear to data usage and to improve efforts for the education awareness for concerned stakeholders. Universities are recommended to make sure that students and staffs understand the usefulness of the required biometric information and should train all persons involved in the implementation of biometric-based ID card.

8. Conclusion

Biometric-based smart ID card is by far a secure access control mechanism compared to the traditional mechanisms. Biometrics cannot be lost or forgotten and access grant requires a person requesting access permission to be physically present. It is hard for attacker to be successful and deal with repudiation. Regardless of biometrics advanced capabilities to security provisioning, concerns about the compromise of students and staffs biometric information whether on smart ID card or not are reasonable. Biometric security and privacy concern remains the point of discussion since its flaws exhibition does not guarantee privacy of biometric information. Universities should make correlation between the cost of biometric system implementation and the required security; the cost of implementation system should not out-compete the required security and privacy. The use of Biometric template-on-card and matching-on-card in conjunction with the requirement to request basic information for biometric identifiers, national laws for information security and privacy, biometric education to students and staff would

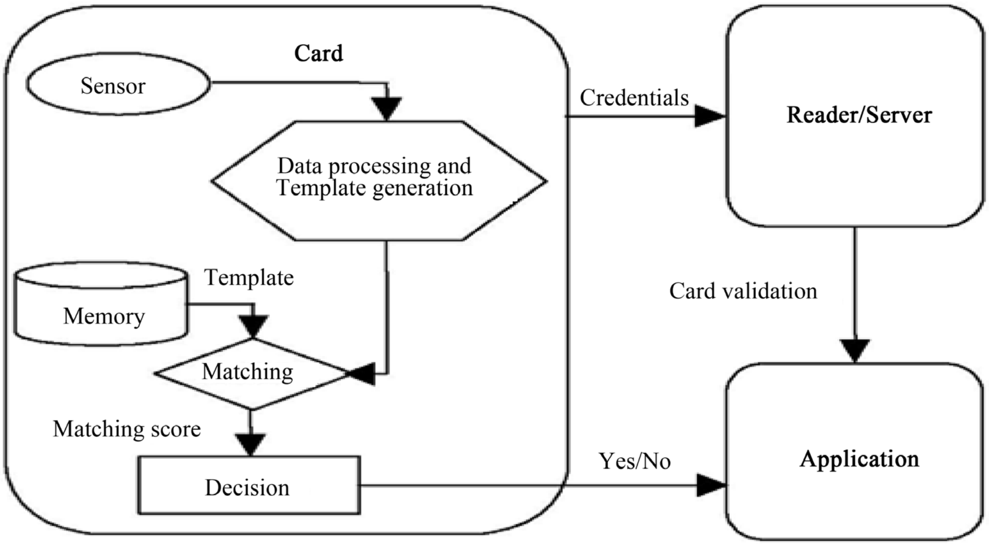

Figure 2. Biometric template-on-card and matching-on-card [19].

make the system more efficient and trusted.

References

[1] ITU-T Newslog (2009) Technology Watch Report: Biometrics and Standards.

[2] Liu, S. and Silverman, M. (2002) A Practical Guide to Biometric Technology. *IT Professional*, **3**, 27-32. http://dx.doi.org/10.1109/6294.899930

[3] Pato, J.N. and Millett, L.I. (2010) Biometric Recognition: Challenges and Opportunities. Whither Biometric Board. http://dataprivacylab.org/TIP/2011sept/Biometric.pdf

[4] Jain, A., Bolle, R. and Pankanti, S. (2002) Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, Forth Printing.

[5] Bosworth, S. and Kabay, M.E. (2009) Computer Security Handbook. 4th Edition, John Wiley & Sons Inc., Hoboken.

[6] Robinson, S. and Stonecypher, L. (2011) Using Biometry for Security and Identification. Bright Hub. http://www.brighthub.com/computing/smb-security/articles/63325.aspx

[7] Sanderson, C. (2008) Biometric Person Recogntion: Face, Speech and Fussion. Chapter 3. VDM Verlag, Saarbrücken.

[8] Nalwa, V. (1997) Automatic On-Line Signature Verification. *Proceedings of the IEEE*, **85**, 213-239. http://dx.doi.org/10.1109/5.554220

[9] Boreki, G. and Zimmer, A. (2004) Hand Geometry Feature Extraction through Curvature Profile Analysis. UNICENP, Computer Engineering Department.

[10] Prabhakar, S., Pankat, S. and Jain, A.K. (2003) Biometric Recognition: Security and Privacy Concern. *IEEE Transactions on Security & Privacy*, **1**, 33-42.

[11] Cavoukian, S. (2008) Access and Privacy Excellence…20 Years in the Making. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/images/Resources/20-20book_374675128750.pdf

[12] Sanger, D.E. (2015) Report Find No Substitution for Mass Data Collection. http://www.nytimes.com/2015/01/16/us/politics/report-finds-no-alternative-to-bulk-collection-of-phone-data.html?_r=2

[13] Maltoni, D., Maio, D., Ain, A.K. and Prabhakar, S. (2009) Handbook of Finger Print Recognition. 2nd Edition, Springer-Verlag, London, 51-57.

[14] Wadhwa, K.R. and Meister, M. (2004) Biometrics and Privacy. Faulkner Information Services. http://www.biometricgroup.com/in_the_news/biopri3.pdf

[15] Gregory, P. and Simon, M.A. (2008) Biometrics for Dummies. Wiley Publishing, Inc., Indianapolis, 271-277.

[16] Dorizzi, B. (2005) Biometrics at Frontiers, Assessing the Impact on Society Technical Impact of Biometrics. http://researchweb.iiit.ac.in/~vandana/PAPERS/BASIC/biometric_challenges.pdf

[17] Ashbourn, J. (2014) Biometrics in the World: The Cloud, Mobile Technology and Pervasive Identity. Springer International Publishing, Berlin, 62-72.

[18] Bidgoli, H. (2006) Handbook of Information Security, Threats, Vulnerabilities, Prevention and Management. Volume 3, John Wiley & Sons, Inc, Hoboken, 473-478.

[19] Xiao, Q. and Savastano, M. (2007) An Exploration on Security and Privacy Issues of Biometric Smart ID Cards. *Proceedings of the IEEE SMC Information Assurance and Security Workshop*, West Point, 20-22 June 2007, 228-233.

[20] Vielhauer, C., Dittmann, J., Drygajlo, A., Juul, N.C. and Fairhurt, M. (2011) Biometrics and ID Management. *Proceedings of the COST*2101 *European Workshop*, Brandenburg (Havel), 8-10 March 2011, 1-3. http://www.springer.com/gp/book/9783642195297

[21] Kolan, H. and Thapaliya, T. (2011) Biometric Passport: Security and Privacy Aspects of Machine Readable Travel Document. https://diuf.unifr.ch/main/is/sites/diuf.unifr.ch.main.is/files/documents/student-projects/eGov_2011_Hesam_Kolahan_&_Tejendra_Thapaliya.pdf

[22] United States General Accounting Office (2002) Technology Assessment: Using Biometrics for Border Security. http://www.gao.gov/new.items/d03174.pdf

[23] Ashbourn, J. (2000) Biometrics: Advanced Identity Verification: The Complete Guide. Springer-Verlag, London, 1-6.

[24] El-Abed, M., Giot, R., Hemery, B. and Rosenberger, C. (2010) A Study of Users' Acceptance and Satisfaction of Biometric Systems. http://www.pchocolaad.com/research/Biometrie%20-%20User%20Acceptance.pdf

[25] Patrick, A.S. (2008) Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems. http://www.andrewpatrick.ca/essays/fingerprint-concerns-performance-usability-and-acceptance-of-fingerprint-biometric-systems

[26] Du, Y. (2013) Biometrics: From Fiction to Practice. Pan Stanford Publishing Pte Ltd., Singapore, 11.