Proc. 1st International Conference on
Machine Learning and Data Engineering (iCMLDE2017)
20-22 Nov 2017, Sydney, Australia
ISBN: 978-0-6480147-3-7

Biometrics and data security: An investigation on biometric templates in computing environment

Roshan Dhakal[1], Rafiqul Islam[2] and Champake Mendis[3]
[1]Student, School of Computing and Mathematics, Charles Sturt University,Wagga Wagga, NSW, Australia
[2]Lecturer, School of Computing and Mathematics, Charles Sturt University,Wagga Wagga< NSW, Australia
[3] Lecturer, Computing in Mathematics, University of Melbourne, Parkville, VIC, Australia

Email: droshan_2005@yahoo.com;mislam@csu.edu.au;cmendis@csu.edu.au

Abstract

Much research on biometric technology and information system focuses on privacy and security such as access control and information security. Few researches infer issues and challenges in biometrics and how they relate to privacy and security within biometric technology. Thus, this research investigates how issues and challenges in biometric are correlated with privacy and security of data and information in biometric technology and organizational information system network. The outcomes would assist organizational management to determine whether implementing biometric technology invades. A survey that has been conducted on fingerprint and facial recognition (aged in between 20-50) found that there is a substantial relationship between biometric user authentication system and privacy and security of user data and information. Additionally, the implementation of biometric technology for user authentication and access control draw the attention and curiosity and this technology were not apparent to be depraved, abusive and fierce. Biometric technology that contains user information is more efficient in identification and verification purpose and does not need to remember like password but once stolen could not be replaced. The outcomes further point out that biometric data and information are irreplaceable and once compromised, then cannot be replaced or changed like passwords. Biometrics technology is apposite and user friendly even though the contentious stratagem of data uniqueness and its cost of stolen. Organization management should therefore carefully understand the need of organization and the feature and risk factor of biometric technology should be considered while implementing it.

***Keywords**:* Biometric technology, privacy and security, identification and verification, user authentication, access control

1. Introduction

Different biometrics technology ultimately differs in its primary technologies, complications and presentations. Every biometric technology has its own benefits and drawbacks and it is very hard to determine such biometric technology which fulfils all the technological needs. Therefore an in depth investigation on analysis of security and privacy issues on each biometric technology and potential solution is vital in organizational information security policy and decision making before and all the way through the implementation of biometric technology. From time to time, possible settings have been worked out and distinct way out is accessible in border security and business purpose. On one hand, the curiosity of biometrics technology has been widespread for its benefit, but on the other hand the possible threats on the user's privacy that arises from the misuse of biometrics information often thwart the implementation of biometric technology in wide ranging. In reality, people are not passionate to hand out biometrics actions with self reliance that biometric data and information cannot be lost and manipulate without user's permission. This is the main reason that people are more concerned with implementing the biometrics technology in reality and also the cost of recovering the lost or stolen data and information and compensation for the breaching the privacy of the user is another factor. Currently, more research has been committed to building the method for securing the biometric data. Like this, user authentication in biometric technology can be worked out and fulfilling the user's concern in relation to security and privacy of biometric data. This kind of procedure generally allows modification of entered biometric characteristics into secure identifiers and turning out to be impracticable to retrieve the original biometric characteristics. Numerous suggestions have been put together linking encryption technology and biometric technology to improve the certainty while biometric data are collected and stored for verification purpose (Cimato, Gamassi, Piuri, Sassi, & Scotti).

The main purpose of this paper is to recognize the organizational needs in relation to access control applications and also assisting in finding the proper biometric technology which satisfied the organizational requirements. Alternatively, this paper also assists in discovering the further and other security control for efficient information security, sovereignty that arises by assessing the risk factor from methodological design and procedural issues (Cimato, Gamassi, Piuri, Sassi, & Scotti). Many literatures have been detailed, documented and focused on the benefits of biometric technology implementations such as its user friendliness, easy to use, security, legal and ethical aspects, etc. An analysis on technical factors of biometric technology has been testified in smaller number and furthermore which are presented is based on technological factors and purposeful matter and still not inclusive (Cimato, Gamassi, Piuri, Sassi, & Scotti). This paper presents the well throughout up to date analysis on privacy and security issues of biometric technology, which covers technological factors that are connected to biometric functioning influenced by various mechanisms that develop the system.

This paper further exposes that challenges on the strength of the system difference in the real time working environment and the security vulnerabilities of spoofing and repeated attacks remain the main problem on top of the biometric technology application. This paper also highlights on the necessity for consistency biometric system analysis, reporting and guarantee of biometric device compatibility. The research paper is structured as follows: Section 2 represents Biometrics performance methods; Section 3 represents Experimental study and measurement; Section 4 represents Results and Analysis; Section 5 represents Discussion and future direction; Section 6 represents the conclusion.

2. Biometrics performance methods

The primary purpose of biometrics technologies are identification and authentication and both needs the subsistence of user's reference data which will be equated to reference template or odd data. Before discussing the identification and authentication phase, enrolment process needs to be defined. Enrollment phase in biometric system inputs the user's biometric data and characteristics into the database of biometric system. In enrollment stage, the user places his finger, face or hand or retina over a biometric device or reader, which scans the user's biometric features and creates a digital symbol or icon. The biometric system normally does a quality assessment to make sure that consecutive stage could develop the acquired sample consistency. For easy matching, a feature which is named as extractor processes the entered sample to create a compress other than meaningful image known as a template. Biometric system could store these templates on the smart card that has been assigned to user or register these templates into a central database which relies upon the biometric applications (Sharifah Mumtazah Syed Ahmad, 2012).

Biometric identification means the capability of the computer information system to exclusively differentiate the user from stored biometric templates in the database. For example, the government of any country implements the national biometric identification system which admits the residents to confirm his/her identity without presenting any document and believing that residents are previously recorded in the national biometric identification system. In other hand biometric data will be compared with all other templates that are stored in a database on a national biometric identification system and when a successful match is found with the corresponding resident's identity then data would be obtained from the database. This process is also called as "one to many "match and usually employed by police and forensic department to identify the criminals (Cavoukian & Stoianov, 2007). Whereas biometric verification means "one to one" match where real time biometric data presented by the user is matched with the stored biometric templates that has been previously provided by the user and the match is established. Here biometric devices could match the real time biometric data and there is not necessary to search the biometric templates in the database even though database could be used. This kind of comparing the real time biometric data to the recorded biometric template is all the essential requirements to authenticate the user is correct user (Cavoukian & Stoianov, 2007). Verification need not insist identification all the time when the appropriate user uses the facility.

Biometric performance is based on the two results known as "false accept" and "false reject" and these are two common mistakes that happen throughout the identification and verification process. The degree which measure these ensue is called as "False Accept Rate" and "False Reject Rate" which is used to calculate the level of correctness and consistency of biometric systems. While measuring the user's biometric data, the biometric data is matched to the enrolled biometric templates and if the biometric system fails to match, for instance, user data have been stored in biometric template and still biometric system fails to recognize then it is called "False Reject Rate". For a particular biometric system, the False Reject Rate would be the similar process for verification and identification. External factors such as the user's wet or dirty hand, poor lighting for Irish recognization, etc. could affect the False Reject Rate (Navaz, Sri, & Mazumder, 2013). On the other hand, when user's characteristic is satisfactorily identical to the stored template and the result match is false stated then it is known as "False Accept Rate". The False Accept Rate of the given biometric device precisely manifest to the consistency and the influence of the equipment. To receive the low False Accept Rate user's data must be totally distinctive and the algorithm employed should summarize record and seek and return user's distinctiveness in an efficient manner (Navaz, Sri, & Mazumder, 2013).

Additionally, the term "collectability" also needs to be addressed which is another significant feature of biometric systems. While all biometric technologies rely on the input devices that focuses on active command, in some cases where the devices itself fails to acquire or capture the required entered samples in satisfactory circumstances. In that case, it might require the collectability necessity which in return delays the recognition and this process is known as "Failure To Acquire" or "Failure To Capture". For instance, application of residents for biometric smart card needs high output, demand for low Failure To Acquire. Beside these facts, a real biometrics technology should comply with the comprehensive prerequisite which basically means that it is should be user friendly and practical for all users (Cimato, Gamassi, Piuri, Sassi, & Scotti).

3. Performance based on literature review

The literature review is involved in the study of previous research and identifying and comparing the difference in previous and current studies. According to Irfan Iqbal (McConnell), most of the researcher believes that biometric technologies provide a high level of security and privacy, but researchers' crusade with the truth that it is hard to show the return on investment of biometrics technology (McConnell). Is the biometrics technology fulfilling the organization's needs? How much will be the ongoing cost for maintenances? Biometrics relate to the personal data and information, so there is concern in relation to privacy and security of this data and information from a legal point of view (McConnell). After collecting the biometric data and information from the users, these data and information as well as biometric devices needs to be protected. The only solution for this is to encrypt the biometric data and store in central database rather than local workstation. Users trust and awareness in relation to biometrics technology could affect the successful execution and competence of the biometric technology (McConnell). Some of the other issues could arise in the working environment that affect on the performance of biometrics technology. For example, wet and dirty hand could affect in reading the finger scan and hand geometry, poor lighting could affect in retina scan and facial recognition, extra makeup could affect in detecting faces recognition, any cuts or wounds in hand or palm could affect in detecting finger scan and hand geometry (Iqbal, 2017). In order to address such issues, alternative way for access control should be provided such as pin number or password. Training and awareness should be provided to users about handling the biometrics technology.

Even though, the extensive research in relation to privacy and security issues in biometric has been done and yet additional research needs to be carried out. As discussed earlier that security and privacy are directly related to the single user and also the effectiveness of biometric system implemented for user authentication. Further, in depth analysis points out that there is some section on biometric system that needs urgent concern. Fingerprint was believed to be one of the best and most secure biometric tools, but due to increase in technology and digital biometric devices finger print scanning could be fooled. And there are some other websites which provide the full step by step information which can generate the duplicate finger print. Facial recognition was also believed to be a secure method of biometric tools, but it also could be deceived with a mask at non attendance circumstances. Now a day, cosmetic make up and plastic surgery are other methods to deceive the facial recognition. Additionally, faces transforms eventually, the recorded templates has an inadequate time period that influences biometric system consistency. Moreover, poor lighting condition and crash in the whole system are other issues related to privacy and security (Zimmerman, 2002). Voice reorganization could be tricked by manipulating the recorded voice with the voice recognition software and matching them with an original voice. Irish cameras are very expensive that require high technology and also are not suitable in every environment. The primary issue is that if other technology provides high speed data and template matching then why there is a necessity if Irish recognization (McConnell)? Biometric data and information once compromised would not be able to change like passwords. How users are convinced that the compromised data would not affect their privacy? None of the biometrics is 100% secure except DNA matching which is highly costly and is not ethical to implement this for user identification and authentication. Biometric system does not provide any security of the user so why an organization should implement it for access control? The cost of employing biometric should and its ongoing cost of maintenance of biometric system and cost for protecting the template data are other issues. Spoofing attacks, the man in the middle attacks, replay and substitution attacks, Trojan horse attacks and masquerade attacks are some of the common attacks in relation to security and privacy of biometric system.

After reviewing literature on implementing the biometrics technology, some of the gaps have been identified in research in relation to factors affecting whether to employ biometrics technology or not. Study and investigation in this field help organization management to know organizations could be beneficial by implementing the biometrics technology. Moreover, it will also helps information technology professionals, information security managers and analysts to decide which area of biometrics technology they are related to and also know which biometrics solution suits best for their organizations. Some of security organizations which work in information security could also gain advantage from this paper for proposing information security solutions (McConnell).

4. Performance based on secured biometrics templates

Biometric templates are generally altered prior to store during the enrollment stage so that biometric user authentication process could be carried out accurately, but illicit access to the stored templates allows the foe with the fewest amount of real data on the biometrics of the confronted user. The usual method for securing the templates is to reproduce the method that is used in a password based authentication method. In this method, passwords are stored in hashing form and hash function never provides any information and in the event of system crash password is not leaked (Zimmerman, 2002). Another criterion for every created biometric template is known as unlikable characteristics which underlines its originality. This is crucial to enhance the security features mostly since the similar biometric characteristics could be exercised to recognize the user in several applications (Cimato, Gamassi, Piuri, Sassi, & Scotti). For instance, suppose biometric application such as a fingerprint is used to gain access to secure building and through the biometric template of smart card and same fingerprint application acts as access control to the central database. So if the hacker finds that smart card he might manage to get access to secure building, but could not gain access to central database because the fake smart card hacker generated would not have administrative rights into account. Renewing the biometric templates, which allows replicating another template while the current templates are leaked. Renewable features basically need the reversible possessions that permit biometric template to reissue in the same way that compromised templates are replicated. This feature is also implemented while cancelling and deactivating the compromised template without in disrupting the new substitution. In biometric encryption technology, a digital key is randomly created during the enrollment stage, even though the user does not know about it. When the biometric sample is captured, then biometric encryption algorithm securely combines the key to biometric sample to generate a biometric encrypted template. Therefore the key is considered as an encrypted key with the biometrics. While verifying, the users entered the biometric sample, then it is matched with the encrypted biometric template. At that same time the key acts as decryption key (Cavoukian & Stoianov, 2007). Implementing the multiple security policy or defence in depth technology is another solution for effective biometric technology. For instance, to gain access to highly classified information such as the bank central locker there should be multiple biometrics technology for identification and verification so that there would be no compromise in privacy and security. In this case implementing the multiple biometric techniques such as fingerprint, heart beat and facial recognition personally at the same time would be effective because if hacker creates the fake fingerprint and even the facial mask then it would not be possible to get biometric information on the heartbeat.

5. Experimental study and measurement

In this paper, the performance of biometrics system is measured in terms of FAR and FRR for authentication accuracy and protection of biometrics templates. The experiment is measured by how the experiment is carried out and how the performances of biometric templates are measured.

5.1. Conducting experimental outline

In order to investigate the research question and sub questions, an appropriate framework for research is needed. There are so many methods and models that could be implemented in this research, such as qualitative, quantitative, mixed, etc., but quantitative research methodology has been implemented in this research. The main reason to choose quantitative is that the survey will be used as a tool for data collection and the result of this research will be compared with the previous for reliability and validity. There will be questions related to encryption, detection and security and privacy which will be easier to get results in the numbers such as in the scale of 1-10 where 1 is low and 10 is high and collecting data through multiple choice questions where answers are provided in option rather than participants saying that I have no idea about the topic you are talking about. The research initiates from stating the problems along with the objective of the research. Literature review has been conducted to identify if there is any gap in relation to this research and how this research fulfil those gaps. The survey will implement as a tool for data collection from the organization and the survey questions will be related to organization, attitude and opinion on biometrics security and privacy and also to ensure whether organization are interested in long term investment in biometrics technology. A survey would be the worthy research methodology for solving our research questions and sub questions. In questionnaires, some of the factors such as cost, user friendly, easy to use, accuracy and reliability and other desired security and privacy level could be measured which other research may or may. Online survey would be the most effective for this research and the security and privacy of participants would be kept in mind because in the interview there would be face to face interaction within interviewer and participants. While collecting data there are few things that need to keep in mind such as the level of user understanding of biometrics technology, security incidents occurred within biometrics systems and there should not be any offensive questions such as have you ever created security incidents in organization during work?

6. Performance calculation of biometrics templates

Biometrics templates are calculated based on the False Accept Rate (FAR), False Reject Rate (FRR), Failure to Enroll (FTE) and Failure to Capture (FTC) performance. FAR calculates the rate of users in percentage that are successfully admitted as real users and FRR calculates the user's percentage rate who are admitted as real users but rejected during the authentication process. Both FAR and FRR could normally be substituting adjacent to themselves by modifying certain factors. Although sometimes, both FAR and FRR are identical commonly known as Equal Error rate (EER). The biometrics system could be more precise if there is low EER. To get the low false rate biometrics system could imply certain factors such as biometrics devices are programmed with the high acceptance limit. For instance, in any biometric device three attempts are allowed to minimize FRR which means users are falsely rejected if user fails all three attempts for authentication (Prabhakar, Pankanti, & Jain, 2003).

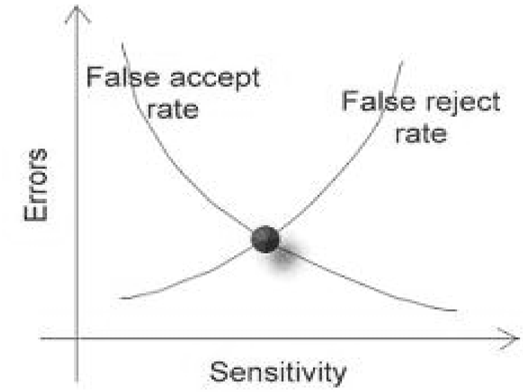

Figure 1: Calculating Biometrics templates performance (Prabhakar, Pankanti, & Jain, 2003)

7. Results analysis

To explore the performance on verification of biometric system, it should be viewed on how biometrics systems responses to enormous biometric features inquisition from accepted users and unaccepted users. As a result of physical instability and limitations in computation, the outcomes of such research are indistinct and could be only forecasted to specific limit. To resolve the error rates which is false accept rate and false reject rate, the users judgement of yes or no are not accepted rather than principle extent of equality in between inquiry templates and stored reference templates in database(Biometrics performance determination for specialists, 2017). For large number of samples, the equality ratings which is also known as score values are gathered for both accepted and unaccepted users and frequency of prevalence is calculated for each score values. As soon as it becomes constant with the entire inquiry templates, an accepted and unaccepted user's statistical outcome creates estimation to the probability distribution function which gives the clear view of quantified approximation of particular equality ratings number of probability (n) of occurring for accepted users (pB(n)) and unaccepted users (pN(n)).

$$pB(n) = \frac{\text{total number of accepted users with same ratings}}{\text{total number of accepted users}}$$

$$pN(n) = \frac{\text{total number of unaccepted users with same ratings}}{\text{total number of unaccepted users}}$$

There will be more exact estimation when there are high volumes of accepted and unaccepted users. Sometimes there is no traverse or overlapping in the statistical distribution curves which means high equality ratings inquiry templates for accepted users and low equality inquiry templates ratings for unaccepted users (Biometrics performance determination for specialists, 2017). In such condition, decision threshold is used to identify the division in between accepted and unaccepted users but in realistic both distribution curves overlap because of large number of users.

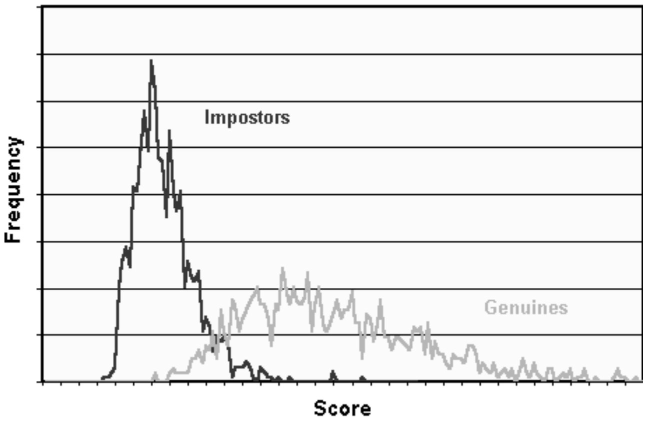

Figure 2: Frequency diagram of genuine and impostors

The error scale values of FAR is described as the probability of unaccepted users is accepted as authorized users and FRR is described as accepted user is unaccepted as unauthorized user. The distribution curves depend upon the amendable decision thresholds for comparison of scanned biometrics templates with the stored reference templates from database (Biometrics performance determination for specialists, 2017). The pursued source is directed below the approximation which is the equality rating value could be any number in between 0 and K and for easy favour the starting probability value of K would be 0.

When the common probability distribution function p is known for distinct alike values n then probability pM(th) of the scanned biometric templates with same rating n comes under threshold th9"misses)which is

$$PM(0) = 0$$

PM (th) =$^{th-1}$ p (n) th=1, 2... K

$\sum$

n=0

The total of accurate alike and dislikes should be identical to the total number of events. Therefore the probability PH (th) which has the same rating of the scanned biometrics templates attain or go beyond the thresholds th ("hits") is

PH (th) = 1 - PM (th) = Kp (n) th=1, 2, ..., K

$\sum$

$n=0$

For the False Match Rate FMR(th), the probability approximation which have same couple of separate templates neither could not attain the definite threshold value nor go beyond the definite threshold value th.

FMR (th) ~ PH (th) = 1- $^{th-1}$ pN (n) th=1, 2, ..., K

$\sum$

$n=0$

And similarly for False Non Match Rate FNMR (th):

FNMR (th) ~ PM (th) = 1- th-1 pB (n) th=1, 2, ..., K

$\sum$

$n=0$

Where pN =probability frequency function for unaccepted users

And pB=probability frequency function for accepted users

The symbol ~ denotes that the normal value of measures=d failure rates False Match Rate and False Non Match rate are similar to the probabilities PH and PM respectively and the limit values are as follows:

FMR (0) =1 FMR (K) =0

FNMR (0) =0 FNMR (K) =1

In order to measure the FAR and FRR, the threshold own Quality Rejection Rate which is same as Failure To Accept should be measured. While given false acceptance is allocated to false match then it will be achieved:

FAR (th) = (1-QRR) FMR (th)

FRR (th) =QRR+ (1-QRR) FNMR (th)

And for circumference value it will be achieved:

FAR (0) =1-QRR FAR (K) =0

FRR (0) =QRR FRR (K) =1

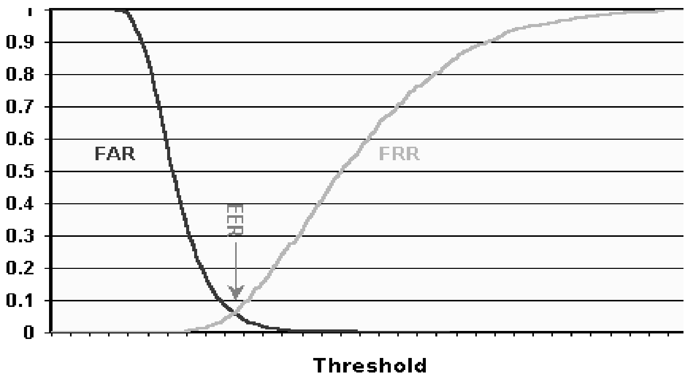

Figure 3: FAR and FRR graphical analysis

8. Discussion and future direction

Whenever there is an inside or outside attack, biometrics technology does not provide protection in authentication system by users. Here are some of the findings that organizations could implement in order to safeguard biometric authentication system. A database that stores biometrics data and information need to be encrypted with encrypted key. High priority should be given to audit logs and full attention should be given to detect if there is something wrong user does or happens which could compromise privacy and security. Standard logs should be put into effect which can identify the user who is not complying with the policy and procedure that may compromise the biometrics system. Biometrics encrypted data and information should be located in the central database rather than local workplace. This helps encrypt data and information less chance of interference and mess about (Zimmerman, 2002). And finally the most important is to educate and aware the user about biometrics technology such as how it works, what will happen when it gets breaches and what would role of user when there is intruding in biometrics technology. This paper also finds that extra biometrics technology should be implemented where possible. The analysis of security and privacy in relation to biometrics implementation find out that there are critical areas which needs more research and needs more focus beyond the technological limitation. Further research needs to be carried out to find out the factors that are responsible for the failure to capture during the enrollment process. There is no proper framework for measuring the success factor of biometric templates rather than false accept rate and false reject rate, therefore additional research need to be carried out. More research should be carried out in anti spoofing procedure which aspiring to create the smart biometrics components: identification and verification that differentiate the genuine and forged sample. More research should be carried out in live monitoring through security cameras and identifying and detecting the circumstances of biometrics presented from simulated devices.

9. Conclusions

The biometric system saves time during user identification and verification; the user does not have to remember the password and they do not have to hassle for changing password. Organization management should understand the need of organization, calculate the risk factor and must understand which kind of biometrics would satisfy the organizational needs prior to deploy biometrics system. There is no risk in implementing the biometric system, but primary concern is how these installed biometric systems should be protected so that it protects our privacy. The organization should always look for another option while in case of emergency so password policy also should not be forgotten as plan B.

In conclusion, this paper addressed some of the issues that arise in biometric privacy and some potential solution to address those issues. The purpose of this was to introduce the biometric system in real time environment for identification and verification process. The lawful execution of the biometric measures assists some of the families that have been identified and reunited with their parents and children through biometric DNA matching who were missing since the Second World War. Another example could be the death declaration of Saddam Husain and Bin Laden was identified by biometrics measures DNA because US military have got samples of those high profiles. Biometrics system would gain more and more interest and it will be the only most efficient measures for identification and verification.

References

Ann Cavoukian, A. S. (2007, 3). Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy. Accessed via www.ipc.on.ca/wp-content/uploads/Resources/bio-encryp.pdf on 27 August 2017

Zimmerman, M. (2002). Biometrics and User Authentication. SANS Institute: Accessed via www.sans.org/reading-room/whitepapers/authentication/biometrics-user-authentication-122 on 28 August 2017

Biometrics Performance Determination (for Specialists). (2017). Biometrica: Accessed via www.bio-metrica.com/biometrics-performance-determination 14 September 2017

Cimato, S., Gamassi, M., Piuri, V., Sassi, R., & Scotti, F. (n.d.). Privacy in Biometrics. Accessed via http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.649&rep=rep1&type=pdf on 26 August 2017

Iqbal, I. (2017). A Proposal for Factors Influencing Biometrics Technology Security. International Journal of Innovative Research in Computer and Communication Engineering , 3651-3657.

McConnell, J. M. (n.d.). Understanding biometrics: How to choose the right biometric technology for your organisation. Planet biometrics. Accessed via www.planetbiometrics.com/creo_files/upload/article-files/how_to_choose_the_right_biometric.pdf on 28 August 2017

Navaz, A. S., Sri, T. D., & Mazumder, P. (2013, 3). Face recognition using principal component analysis and neural networks. Research gate. Accessed via www.researchgate.net/publication/235950165_Face_Recognition_Using_Principal_Component_Analysis_And_Neural_Networks 13 September 2017

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003, 3). Biometric Recognition: Security and Privacy Concerns. Accessed via https://www.researchgate.net/publication/3437477_Biometric_Recognition_Security_and_Privacy_Concerns 28 August 2017

Sharifah Mumtazah Syed Ahmad, B. M. (2012). Technical issues and challenges of biometric applications as access control tools of information security. International Journal of Innovative Computing, Information and Control , 7983–7999.

Stelvio Cimato, M. G. (n.d.). Privacy in Biometrics. Accessed via http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.649&rep=rep1&type=pdf on 26 August 2017

Zimmerman, M. (2002). Biometrics and User Authentication. Accessed via www.sans.org/reading-room/whitepapers/authentication/biometrics-user-authentication-122 on 29 August 2017