INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Security and Privacy Implications in the Deployment of Biometric-Based ID card for University Students and Staff

Adigwe A. I.
Federal Polytechnic Oko, Nigeria
Egere A. N.
Federal Polytechnic Bali, Nigeria

Abstract:
Being an automated measurement of biological or behavioural traits that identifies an individual, biometric identification provides a reliable solution to the security mechanisms of user authentication and integrity in identity Management systems. With the recent widespread deployment of Biometric systems in a variety of applications, there have been an alarming concern about the Security and Privacy of what has been seen by many people as an emerging technology with an unfolding security vulnerabilities and threats. The acceptability of this emerging technology, however, by the general public, is absolutely a function of the system designers to prove that these systems are sturdy and have an infinitesimal error rates with respect to the fundamental properties of security systems such as availability, confidentiality, integrity and accountability. Given the above, therefore, this paper presents an overview of the various security threats of biometric system and countermeasures that have been proposed to address the privacy implications associated with deployment of Biometric-based ID card for University students and staff. An important issue such as biometric templates is also being highlighted. Unlike password as an authentication mechanism; Biometric template is a one-way function and cannot be reissued when compromised.

1. Introduction

There is no gain saying that an identity theft has shown an unprecedented growth during the last decade. Approximately 10 million Americans are affected by identity fraud each year, according to the U.S. Federal Trade commission [1]. In order to combat this glaring epidemic growth in identity theft and to meet the increased security requirements in a variety of applications, ranging from internal border crossing, passport, time and attendance monitoring, ID cards, IT user system authentication, automated crowd surveillance, physical access control to fraud prevention, a reliable identity management system is the most wanted. Establishing identity of a person is a critical task in any identity management system [3]. The production of Biometric ID card is difficult when it is dispersed throughout a jurisdiction, but these technical challenges can be overcome, according to *Mr. Gills, Assistant Director,* UK Immigration Service, home office [2]. Studies, however, show that the use of RFID enabled ID card and password as a representation of identity and access control security mechanisms are no longer sufficient for reliable identity determination because they can be shared, especially in the UK University Systems, and masqueraded at the same time. This process leads to risk analysis; studies have equally shown that human beings are the weakest link in the security mechanism of any system [4].

Biometric recognition is an automated measurement of biological and behavioural traits that discloses the identity of an individual. The most common methods of Biometric technology include finger print, hand geometry, Voice, Iris, face, hand written signature, Palm print and Gait to mention but few. Biometric characteristics, being used as an authentication token, have a number of features such as reliability, convenience, and so on. These traits led to large-scale deployment of biometric authentication systems. However, in spite of this glaring success achieved by its deployment, there are still some contentious security and privacy issues or implications concerning the deployment of biometric-based ID card that need to be addressed in order to ensure the integrity and public acceptance of this supposedly emerging technology.

2. The Working Principles of Biometric Authentication System

Before delving into Biometrics methods, it is pertinent to explore the major components of Biometric authentication systems and the interoperability between those components. Because except we have accrue on the working principles of these components, we would be unable to establish the security and privacy implications of deploying such system under review.

Basically speaking, generic Biometric authentication system is made up of five major components; namely, sensor, feature extractor, template Database, Matcher, and decision Module.

Sensor is the interface between the user and the authentication system and its function is to scan the Biometric traits of the user. The feature extraction Module, on the other, processes the scanned Biometric Data to extract the salient information (feature set) that is useful in distinguishing between different users. In some cases, the feature extractor is preceded by a quality assessment module which determines whether the scanned biometric trait is of sufficient quality for further processing. During enrolment, the extracted feature set is stored in a database as a template marked by the user identity information. Since the template database could be geographically distributed- made possible by the use of Global positioning System (GPS), and contain millions of records, maintaining its security is an important task. The Matcher Module is usually an executable Program designed to accept two Biometric feature Sets XT and XQ from template and query respectively, as inputs, and outputs a match score showing the similarity between the two sets. Finally, the decision Module makes the identity decision and initiates a response to the query [3].

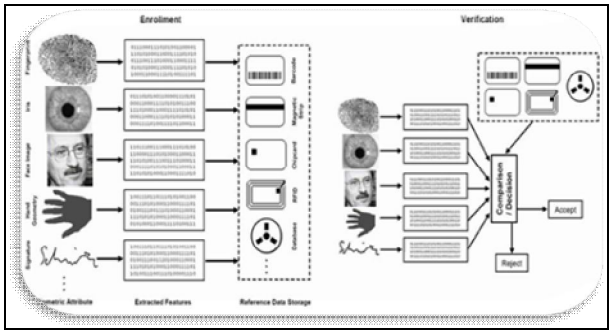

Figure 1: [2] General Biometric processing Steps

3. Biometric Methods

Having briefly explored the functionalities of the major components of Biometric systems in the previous section, this section focuses on some of the popular biometric methodologies and considers how they work, type of characteristics of the biometric techniques under review, and what applications they may be best suited for.

Category	Method	Type	Remark
Hands	Finger print	Static	Unique
	Palm print	Static	Unique
	Hand geometry	Static	Not distinct
	Hand, Palm and wrist vein.	Static	Not distinct
	Spectroscopic Skin Analysis	Static	Not distinct
Heads and Face	Face Recognition	Static	Not distinct
	Iris	Static	Not distinct
	Retina	Static	Highly distinct
	Ear Shape, Size	Static	Not distinct
Other Physical Characteristics	Blood Salinity	Static	Not distinct
	Blood Chemistry	Static	Not distinct
	Body Odour	Static	
	DNA	Static	Unique
Behavioural	Gait	Dynamic	Conditional
	Voice	Dynamic	conditional
	Signature Recognition	Dynamic	N/A
	Keystroke dynamics	Dynamic	Not distinct

Table 1: [5] Biometric Methods

Having observed the two basic biometric methods, then, the question, "***which biometric is best***", remains one of the most often asked when people are looking at this technology. ***The best answer to such technical question is that there is no best biometric method; it***

all boils down to what we are trying to achieve, with whom and what prevailing conditions exist. A methodology which works well within a contained and constant office environment may be less suitable for a busy public airport or a factory shop, for example [5].
In considering biometric methodologies for possible deployment, there is need for clear understanding of the application and the situation from the user's perspective and being objective about the benefits of introducing the technology into a given process. For example, face recognition template may cease to be unique where an individual under goes plastic surgery in case accident. Given the above scenario, therefore, let's now look at some of the more popular examples of biometric methodology. But due to the limited volume of this paper, a concise analysis is being focused on, in terms of the category, techniques and the type of characteristics of the biometric system. See table1-[5].

4. The Security and Privacy Implications of Biometric System

4.1. Failure on Students and Staff
As a result of rapid growth in sensing and computing technologies, biometric systems have become affordable and are easily embedded in a variety of consumer devices such as mobile phones and key fobs, making this seemly emerging technology vulnerable to the malicious designs of common criminals. In order to subvert any possible security crises, vulnerabilities of the biometric system must be identified and resolved systematically, otherwise, the deployment of such highly sensitive technology will, undoubtedly, continue to raise fear in the minds of general public as far as privacy is concerned. A number of researchers have analysed potential security breaches in a biometric system and proposed methods to counter those breaches, as mentioned below. Formal methods of vulnerability analysis such as attack trees have also been used to study how biometric system security can be compromised [3]. So, let's look at classes of the vulnerabilities associated with biometric-based ID card, which of course points to the privacy implications in broader perspective.
Biometric system vulnerability can be broadly categorized into two classes; namely, *intrinsic failures and failure due to an adversary attack*. Intrinsic failures occur due inherent limitations in one or two of the biometric components discussed earlier in this paper, and as well as the limited criminality of the specific trait. In adversary attacks, a result oriented hacker attempts to circumvent the biometric system for personal gains. The adversary attacks are further classified into three based on factors that enable an adversary to compromise the system security. These factors include system administration, no secure infrastructure, and biometric covertness. Thus, assumptions (security services relying on kernels and other agents to supply correct data) and trust underlie confidentiality mechanism, and hence violets the privacy of the users of such technology.

4.2. Intrinsic Failure
Intrinsic failure is the security lapse due to an incorrect decision made by the biometric system. A biometric verification system is liable to two types of errors in decision making; namely, *false accept and false reject.*
A legitimate user may be falsely rejected by the biometric system due to large differences in the user's stored template and query biometric feature sets (see fig. 1). These intra user variations may be as a result of interoperability between the user and biometric system(changes in pose and expression in face image) or due to noise introduced at the sensor(for example, residual prints left on fingerprint sensor). False accepts are usually caused lack of uniqueness in the biometric trait which can lead to large similarity between feature set of different users (similarity in the face images of twins and siblings). Both intra user variation and inter user similarity may also be caused by the use of non-salient feature and non-robust matchers. Sometimes, a sensor may fail to acquire the biometric trait of a user due to limits in sensing technology or adverse environmental conditions. For instance, a fingerprint sensor may be unable to capture a good quality fingerprint of dry/wet fingers. This leads to failure-to-enroll (FTE) or failure-to-acquire (FTA) errors [3].
Intrinsic failure can also occur even when there is no explicit effort by an adversary to circumvent the system. So this type of failure is known as zero-effort attack. It poses a serious threat if the false accept and false reject probabilities are high. However,
ongoing research is directed at reducing the probability of intrinsic failure, mainly through the design of new sensors that can acquire the biometric traits of an individual in more reliable, convenient, and secure manner, the development of invariant representation schemes and robust and efficient matching algorithms, and use of multi-biometric systems [6].

4.3. Adversary attack
In this situation, an adversary purposely initiates an attack on the biometric system whose success relays on the lapses in the system design and the availability of adequate computational and other resources to the adversary. In this paper, adversary attack is categorized into three main classes, which include administration attack, non-secure network infrastructure, and biometric covertness [3].

- **Administration attack**
  This kind of attack is often refer to insider attack, which points to all vulnerabilities introduced due to improper administration of biometric system, such as integrity of the enrolment process between the adversary and the system administrator or a legitimate user, and abuse of exception processing procedures.

- **Non-secure Network Infrastructure**
  In a networked environment, biometric system is composed of hardware, software, and the communication links between the various modules. There one and thousand ways in which an adversary can manipulate the biometric infrastructure and that can lead to security breaches.
- **Biometric covertness**
  Studies have shown that it is possible for an adversary to covertly acquire the biometric characteristics of a legitimate user (e.g. fingerprint impression lifted from a surface) and use them to create physical gummy finger of the biometric trait. Hence, if a biometric system is not capable of distinguishing between live biometric presentation and an artificial spoof, an adversary can circumvent the system by presenting spoofed trait [3]. This, undoubtedly, undermines the integrity and confidentiality of the users of such systems, and hence violets their privacy.

When a biometric system is compromised, it can lead to serious privacy implications; namely, Intrusion and Denial-of-Service (DOS). Intrusion refers to an impostor gaining illegitimate access to the system, resulting in loss of privacy (e.g., unauthorized access to personal information) and security threats such as interception, modification, and fabrication of students and staff data being transmitted via the network infrastructures or those currently stored in the University data bank. All the four factors, as mentioned previously, that causes biometric system vulnerabilities (intrinsic failure, administrative abuse, insecure network infrastructure, and biometric covertness) can result in intrusion.

Denial-of-service *(DOS)* is a situation where a legitimate user is prevented from obtaining the service that he is entitled to. A system hacker can undermine the infrastructure (e.g., physically damage a fingerprint sensor) hence preventing users of Biometric-enabled ID card from accessing University facilities. Intrinsic failures such as false reject, failure-to-capture, and failure-to-acquire also lead to denial-of-service. In addition, Administrative abuse such as modification of biometric templates or the operating parameters of biometric systems may also be contributing factor to the denial-of-service effects. Thus, assumptions that the security services can rely on the kernel to supply correct data, and lacks of trust on the part of other agents underlie confidentiality mechanism. Matt Bishop et al [4].

5. Security Effectiveness of Biometric Based Systems

In spite of the glaring benefits offered by biometric verification to access control security applications, Universities have developed a cool feet in embracing this technology. Part of this reluctance may be attributable to the higher cost of biometric readers in comparison to the RFID-based card reader, coupled to the perceived extra complexity of implementation and subsequent running cost. However, a large part of it is undoubtedly due to reluctance from users who have sometimes perceived the concept as being intrusive or simply unreliable and harmful to their privacy. Early biometric vendors did not always help this situation as some of them made unrealistic claims as to the performance of their devices, which could often not be substantiated under real world Conditions (e.g., distinguishing an artificial biometric template from a real one) [5].

It is probably fair to say that vendors and system integrators have largely learned this lesson and that similar installations today can be expected to be much more reliable and successful, through a combination of intelligent deployment. However, it has taken a while to get to this point and poor early impressions are hard to erase from the public consciousness [6]. Given the above scenario, is a biometric-based ID card really viable with contemporary technology? The answer is undoubtedly yes, because almost all the known security threats, as mentioned above, can be countered.

Adversary attacks compromises the system vulnerabilities in at least one interface. Ratha et al. [7] identified eight points of attacks into a biometric system. This is includes, fabricate biometric, replay old data, override feature extractor, synthesized feature vector, modify template, Intercept the channel, and override final decision.

In this section, these attacks are grouped into four categories, which are, attacks at the user interface (input level) attacks at the interfaces between modules, attacks on the modules, and attacks on template database.

5.1. Attacks at the user interface

This kind of attack is mostly due to the presentation of a spoof biometric trait [5]. If the sensor is unable to substantiate between fabricated and genuine biometric traits, the adversary easily intrudes the system under a false identity. A number of efforts have been made in developing hardware as well as software solutions that are capable of performing aliveness detection [5]

5.2. Attacks at the Interface between Modules

A research study shows that an adversary can either sabotage or intrude on the communication interfaces between different modules. For instance, he can place an interrupting source near the communication channel (e.g., a jammer to interrupt a wireless interface). If the channel is not secured cryptographically, an adversary may also intercept and/or modify the data being transferred. So cryptography is a countermeasure being used for attacks at interface between modules. For example, Juels et at. [8]. *Outlined the security and privacy issues* introduced by insecure communication channels in e-passport application that uses biometric authentication. Insecure communication channels also allow an adversary to launch replay [9] or hill-climbing attacks [10].

A common way to secure a channel is by *cryptographically encoding* all the data sent through the interface, say using public key infrastructure. But even then, an adversary can launch a replay attack by first intercepting the encrypted data passing through the interface when a legitimated user is interacting with the system and then sending this captured to a desired module whenever he wants to break into the system. A countermeasure for this attack is the use of time-stamps [3].

5.3. Attacks on the Software Modules

The executable program at a module can be modified such that it always outputs the values desired by the adversary. Such attacks are known as *Trojan-horse attacks*. A secured code practice [11] should be used as a counter measure for such attack.

5.4. Attacks on Template Database

Studies further prove that one of the most potentially damaging attacks on a biometric system is against the biometric the biometric templates stored in the system database. Attacks on the template can lead to the following three vulnerabilities. (i) A template can be replaced by an impostor's template to gain unauthorized access to the system. (ii) physical spoof can be created from the template [3] .to gain unauthorised access to the system (as well other systems which use the same biometric trait). (iii) The stolen template can be replayed to the matcher to gain unauthorised access. A potential abuse of biometric identifiers is cross-matching or function creep [37] where the biometric identifier for the purposes other the intended purpose. For instance, a fingerprint template stolen from a bank's database may be used to search a criminal fingerprint database or cross-link to person's health records [3].

The most effective way to secure the biometric system, including the template, is to put all the system modules and the interfaces between them on a smart card (or more generally a secure processor). In such systems, known as match-on-card technology, sensor, feature extractor, matcher, and template reside on the card [38]. The above scenario obviously points to biometric based ID card technology. The good news about this technology is that the biometric information never leaves the card. However, systems on card implementations are not appropriate for most large-scale applications; they are expensive and users must carry the card with them at all time. In addition, the possibility that the template can be gleaned from a stolen card is not ruled out. So it is vital to protect the template even in match-on-card applications. Passwords and PIN have the property that if they are compromised, the system administrator can issue a new one to the user. It is desirable to have the same property of revocability with biometric templates [3]. Other properties needed in order to ensure an ideal biometric- ID card scheme include; diversity, Security and performance.

- **Diversity**: the secured template must not allow cross-matching across databases, thereby ensuring the user's privacy.
- **Security**: it must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.
- **Performance:** the biometric template protection scheme should not degrade the recognition performance of the biometric system [3].

6. Conclusion and Recommendations

Given the dramatic increase in the incidents involving Identity thefts, illegally use of University resources by the host communities, unauthorized staff and students, and various security threats, it is vital to have reliable identity management systems. Biometric systems are being widely deployed to achieve reliable user authentication, a critical component in identity management. But the indisputable fact remains that biometric systems themselves are vulnerable to attacks.

Going by the analysis of this research paper, it can easily be understood that the existing biometric template protection schemes are not yet sufficiently matured for large scale deployment; simply because they do not meet the requirement of diversity, revocability, security, and high-recognition performance. These four properties should be given a serious consideration when deploying an effective biometric-based ID card.

In addition, large scale deployment of such technology is costly but real savings can be realized through the appropriate use of a biometric card system. This technology, however, is new and there is considerable ignorance about their use and implications, which are yet to be erased from the minds of the general public.

There is need for international biometrics standard to be able to work in multijurisdictional context. No matter how strong RFID-based ID card, which has been in use in most Universities in the UK, it cannot be compared with iris and fingerprint-based identifier, which are among the biometric template to be integrate into any reliable oriented biometric ID card.

To sum up, there is no point saying that good administration and management remain the most valuable keys for the successful deployment of biometric-based ID cards in the UK Universities.

***7.* References**

1. David M. (2002). Prospective Analysis on Trends in Cybercrime from 2011 to 2020. p3 –p14. Retrieved 26 August, 2014 from http//www.mcafee.com/us/local content/white papers/wp id theft en.pdf
2. Paul J. and Patrick j.(1999). Introduction to biometric identification technology: capabilities and applications to the food stamp program. Retrieved 2 September 2014 from http://www.fns.usda.gov/sites/default/files/biomeval.pdf
3. Catherine P.(2013). Fundamental concepts in network security. Retrieved 30 August 2014 from http://www.ciscopress.com/articles/article.asp%3Fp%3D1998559
4. Matt B. et al (2002). Computer Security: Art and Science. Addison Wesley. Retrieved 1 September, 2014 from http://www.slideshare.net/NanthiniAnbu/niscomputer-security-art-and-science
5. Ashbourn, J. (2000). Advanced Identity Verification. The Complete Guide. Computers & Security, Vol.21, No.3, pp.220-228.
6. Nikolaos, V(2009). Advanced Signal Processing and Pattern ... - Danish Biometrics. Retrieved 28 August 2014 from http/www.iti.cs.uni.agdeburg.de/~sschimke/5681_48.pdf

7. Brindha V.E, (2012). Biometric Template Security using Dorsal Hand Vein. Retrieved 30 August 2014 from http://omicsonline.org/biometric-template-security-using-dorsal-hand-vein-fuzzy-vault-2155-.
8. Juels A, Molnar D and Wagner D.(2005). " Security and Privacy issue in E-passports," Proceedings of the Conference on security and privacy for Emergency Areas in Communications Networks, Athens, Greece pp. 74-88.
9. Syverson P.(1994). " A taxonomy or replay," In proceedings of the Computer Security foundations Workshop Franconia, NH, USA. , pp. 187-191,
10. A. Adler,(2005). "Vulnerabilities in biometric encryption Systems" In proceedings of the 5th International Conference Audio and Video-Based BiometricPersonAuthentication, Hilton Rye Town, NY, USA. pp.1100- 1109.
11. R. Seacord,(2005). Secure coding in C and C++, AddisonWesley, Reading, Mass, USA