An Impact of Biometric System Applications Services on Biometric Service Market

Manoj Diwakar
(Department of Computer Science & Engineering),
DIT University Dehradun,
India

Pawan Kumar Patel
(Department of Computer Science & Engineering),
IIT Kanpur,
India

Kunal Gupta
(Department of Information technology),
HCT, Muscat,
Oman

Amrendra Tripathi
(Department of Computer Science & Engineering),
DIT University Dehradun,
India

ABSTRACT

ISO (the International organization for stadardiization) and IEC (the International Electrotechnical commission) form the specialized system for worldwide standardization. The first standard of this deals with the threat and countermeasure of biometrics and biometric system application models. Additionally, this international standard provides requirements and guidelines for the secure and privacy –compliant management and processing of biometric information. We analyze here that inclination of people towards biometric for using it as a security measure is mainly due to Identity Theft. we study various biometric system application models and analyzed that because of Identity theft problem most companies provides physical access control and logical access control services in perspective of three factors that is Business case, Technical performance and User acceptance.

KEYWORDS: Identity Theft, Biometric Application system Model, SELT.

1. INTRODUCTION

Mr. MyungGeun Chun, Project Editor of ISO/IEC 24745:2011 explains "As the Internet is increasingly used to access services with highly sensitive information, such as ebanking and remote healthcare, the reliability and strength of authentication Mechanisms are criticalBiometrics is regarded as a powerful solution becauseof its unique link toan individual that is nearly or absolutely to fake"[1].

Biometrics is coming of age so the availability and advancement of technical standards for biometrics are also developed.

The first biometrics standards were in the area of law enforcement ,where the need to exchange fingerprint data lead the US national bureau of standards in 1986 to publish the first such standards ,since that time, commercial standards have emerged and continue to expand and evolve[2].

The newly issued standard, designated as the ISO/IEC 24745:2011, Information technology – Security techniques – Biometric information protection, is designed to provide guidance for the implementation of biometric technology to further protect sensitive online transactions as identity theft case occurred in recent years are becoming very harmful in both social and economic point of view.

2. BACKGROUND: NEED AND EFFECT OF BIOMETRICS

With increasing identity fraudandemphasis on security, there is a growing and urgent need to efficiently identify humansboth locally and remotely on a routine basis. We require biometric security for-

•Whether it is a smart card, access tokenor biometric techniqueemployed on the front end, the secret to positive identificationis a robust technological infrastructureon the back end.

•From the point of view of security, biometric measures to prevent interference by unauthorized personsconstitute a particularly important means of protecting critical infrastructures.

•A global breakthrough by biometrics in identity verification technologyseems to be imminent in the form of its use in identity documentsand corresponding biometrically-based controls at frontiers.

•In considering the possibility of a new (biometric) identity card, any country should think of electronic identity as infrastructure, like a railway, electricity or transportation

The biometric enhancement of identity documents and smart cards and their global use in identity controls constitute a task on such a scale that experience to date can, at best, provide only a rough estimate of the outcome.

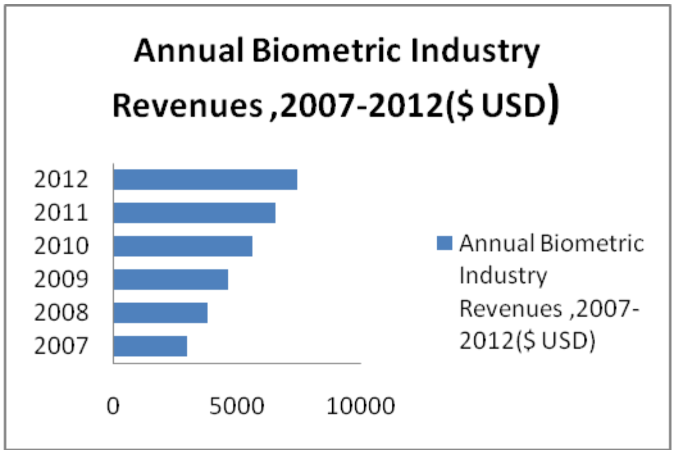
2.1 RESEARCH ANALYSIS ON EFFECT OF BIOMETRICS

-According to IBG (International Biometric group) report the estimated value of biometrics market in 2007 is ~ $3,000,000,000 which represents a huge number.

-The market share of three core technologies that is face, iris and fingerprint recognition is >75% of total biometric services market; it shows that major development occurred in these three biometric measures.

-Number of people caught since 2003 at UAE borders using iris recognition are >50,000.

So above numbers present that biometrics shows a better solution than we aspect not in context of as a security measure but also in economic and social acceptance point of view.Fig.1 represent the total biometric industry revenues (copyright © 2006-2007 International Biometric Group)[3].



According to copyright © International Biometric Group the market share of biometric technology in different biometrics are given by as shown in Fig.2.It shows that fingerprint, face and AFIS/scan are three major biometric in market today.

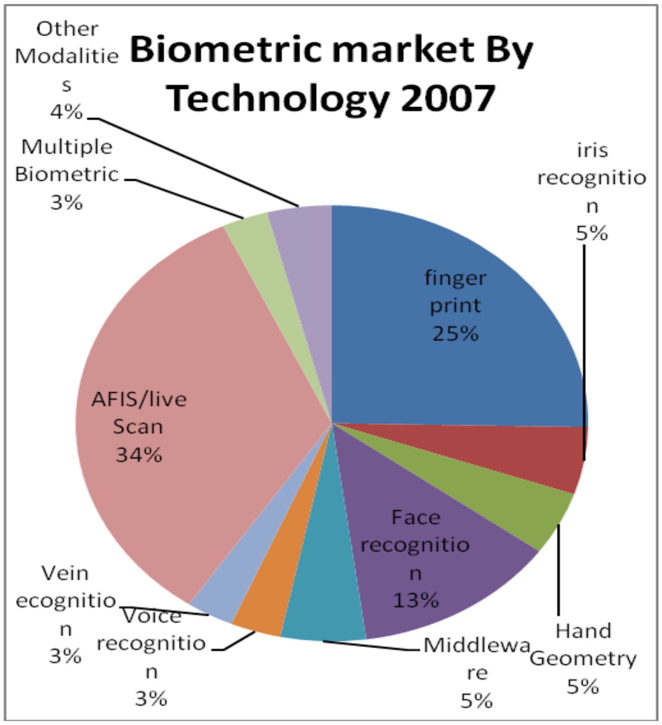


Fig.2 Biometric Market by technology 2007.

3. IDENTITY THEFT AND BIOMETRIC SYSTEM APPLICATION MODELS

There are a number of reasons why identity theft is a challenging problem to tackle. In some cases there is a lack of incentives for the parties in possession of identity data to secure the data adequately. From an individual perspective, there is a lack of awareness about the negative utility that can arise from identity theft. The Internet and the increasing importance of electronic transactions exacerbate the problem as it becomes easier for an identity thief to carry out fraud. Identity theft is growing because of the increasing potential usage of identity information in our Society.

A biometrics study has been recently carried out by the ICT unit team/IPTS/EC and biometric technologies have been examined from a SELT perspective (social, economic, legal and technological) [4].

biometrics and identity are connected, i.e. when identity information is related to appearance such as hair color, eye color (one kind of offline identity information) but also fingerprint, face etc. or a digital biometric template (one kind of online identity information). In general life We leave biometric traces every day in every place; fingerprints on a glass, video records of your face, etc. this results from the fact that biometric features are not secret and are available in the public domain. And as spoofing a biometric system with an artificial finger or a fake template is real vulnerability [4], identity theft is a real threat of the wide implementation of biometrics.

In biometrics context, identity theft has different implications but it is mainly considered as a generator of economic and social impacts. Indeed, the economic importance of identity is growing in a digital society, but the strongest identity protection is not necessarily the optimal one. The concept of optimal identity is regarded as an important point in the biometrics . In fact, identity errors and abuse may become less frequent, but when they happen, they could potentially be more dangerous. For example identity theft may become less frequent but more severe and with wider social repercussions. There is a serious danger that the biometrics identification market – and markets that depend on identity – may fragment into clusters that will not interoperate, thus becoming vulnerable.

It can be seen by the following analysis of identity theft in conventional methods, Fig.3 gives the statistical analysis on how people are threatened by identity theft and Fig.4 shows that because of identity theft in conventional security methods people are willing to shift to adopt biometric as a security measure.

The Gallup poll conducted a survey in 2009 in USA [5], the statistics given by survey is based on the questionHow often do you yourself worry about the following things-frequently, occasionally, rarely or never?

The statistics are shown in Fig.3.

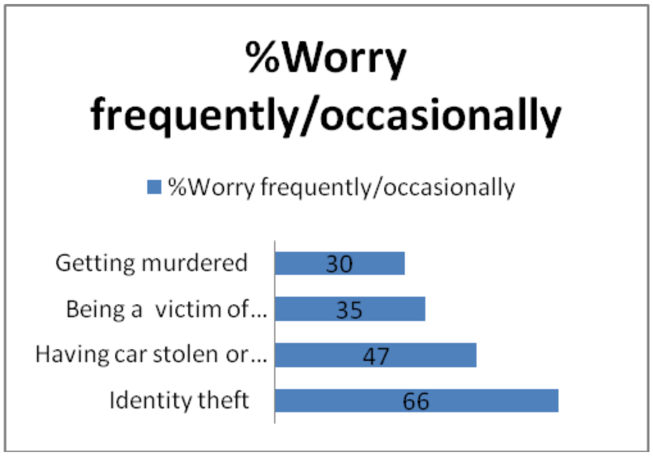


Fig.3survey conducted by Gallup Poll in 2009

The main concern for clients of biometrics devices is the accuracy of measurability, and cost effectiveness. Again, as technology improves and costs decrease, identification and verification systems will be implemental by industries who find it in their best interest (cost vs. necessity) to safeguard their data and assets.Bi-annual Unisys Security Index [6], which surveys more than 1,000 Americans for consumer views on a wide range of security concerns, indicated that more than three-quarters of respondents would stop dealing with an organization entirely in the event of a security breach, underlining the need to better protect customers’ personal data shared electronically.

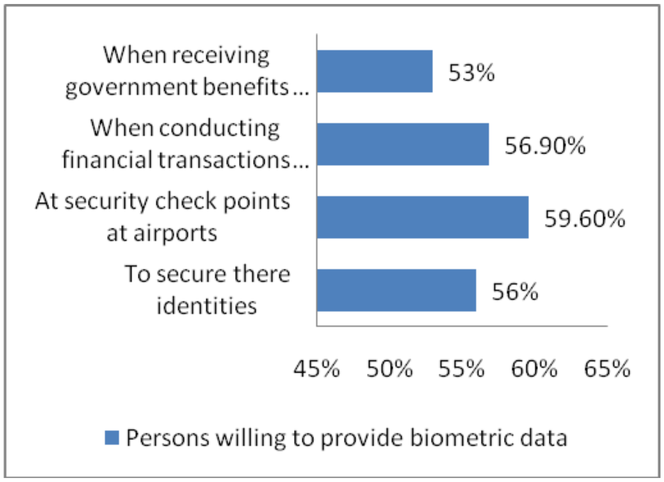


Fig.4 Survey conducted by Unisys Security index in2011

Still, only 21.3 percent were willing to give their biometric data to social media sites, suggesting a perception that either these entities were less careful with their data, or that the risk was simply not worth the reward.

The latest results of the Unisys Security Index suggest that organizations face very real business and financial implications for security breaches,” said Steve Vinsik, vice president, enterprise security, Unisys. “Given recent highly publicized breaches that have exposed large amounts of sensitive data, the results should be a wake-up call for organizations to take more proactive measures to protect customer data”[6].

3.1 BIOMETRIC APPLICATION SYSTEM MODEL:

Physical access control

Biometrics includes everything that requires identity authentication by scanning a person's unique physical characteristics. It is used where high security is a necessity due to its superiority compared with conventional access control methods. Physical access control biometric devices and software store digital information that has been gathered from scanning the user's physical characteristic. To access the information or area protected by a biometric device, the laser sensors must recognize the unique pattern of the user's physical characteristic and match it with its stored digital template. Biometric devices use an algorithm to match templates and authenticate the user's identity therefore False Match and False Non Match rates are remarkably low (Fig.3).

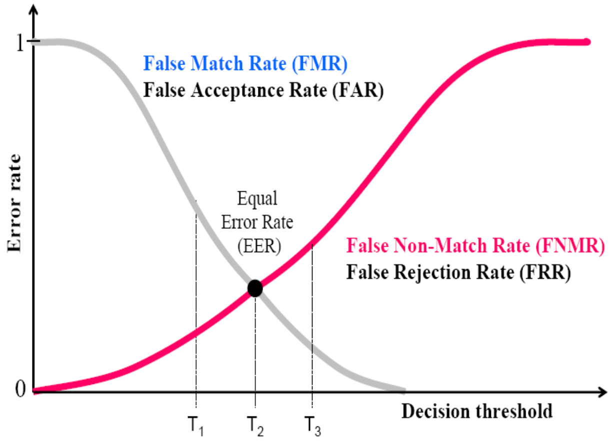


Fig.5 FMR and FNMR graph

It is important to ensure that only authorized users should be allowed to access places like airports, banks and government buildings. Moreover, physical access control in an organization is of great significance to avoid loss or theft of information and inventory. Keeping all this things in mind, constant research has given birth to biometrics with impressive application in this direction. Unfaithful employees also pose threats to physical access in companies who follows biometric security systems.

Logical access control

Logical access control refers to electronic access controls whose purpose is to limit access to data files and computer programsto individuals with the genuine authority to access such information. It is made possible by the use and application of OEM modules and algorithms for imaging authentication and differentiation. They produce very high accuracy rates due to highly sensitive stripe line sensors, optical and thermal sensors which recognize the similarity between existing templates and an authentic user's identity.

Militaries and governments use logical access biometrics to protect their large and powerful networks and systems which require very high levels of security. It is essential for the large networks of police forces and militaries.

Logical access control biometric systems distribute a user's unique information throughout all physical access points so that a registered user can be identified at any access point within the system. Microprocessors for logical access control devices usually contain multiple cores, complex algorithm processing and encryption engines. this complex composition is essential to support sensor accuracy and reduce false acceptance and rejection. Logical access control is different from physical access control biometrics in the sense that it only refers to computer network and systems access control. A large sever room for instance, would have a physical access biometric security system for the doors and a logical access security system for the actual computers.

Logical access control systems are replacing conventional network security solutions by becoming more cost effective. Biometric equipment and software is becoming more affording and the process of integration into an existing network is now seamless. In recent years, hospitals, airports, police departments, telecommunications companies and businesses of all sizes have been integrating biometric technology into their networks. Not only its security is greatly heightened, time is also saved by eliminatingtedious password management. Without logical access control security system’s highly confidential information would be at risk of exposure.

Justice and Law Enforcement

Biometricstechnology authenticates an individual's identity automatically, and has several useful applicationsin Justice and Law Enforcement. Biometric technology has the ability to recognize fingerprint, iris, voice, facial recognition, hand, palm or skin. Biometric authentication is greatly superior to card, token or password systems which can be stolen or counterfeited. Biometric technology is used in Justice and Law Enforcement because of the enormous capabilities of its automated (as opposed to manual) software. Sensitive information can be identified using regional or national databases and compared with multiple other platforms for superior authentication.

it is also applicable in analyzing crime scenes, through fingerprint capture technology. This technology can capture, with a reasonable degree of accuracy prints and compare them against databases for identification.

Here the threats in maintaining justice and law enforcements for government are that the governments seeking to enhance transparency and efficiency of key processes so there should be standards to provide this key consideration when using the biometric system.

Biometrics for Time and Attendance

There have never been more accurate technologies as helpful to people in search of a way to keep track of group activity as biometric time and attendance technology. Biometrics takes unique physical characteristics of a person and uses them for identification of their identity and verification that they are doing something they’ve been authorized to do. vascular patterns, hand print, finger print, iris patterns, and even voice can be used to ensure that they are who they say they are, and to let people know that they 've been given permission to do whatever it is they're attempting to do.

The simplest application in this sense is for an Employee to use an iris scan or thumb print to let an employer's system know when she/he enters and leaves the office. There will be an automatic log of the hours worked, and when exactly the employee was in attendance.Even if the employee works offsite, the technology can be used electronically over the internet to ensure that an employee's time is tracked. The employer can have the system tell not only when the employee was working, but also what they were working on and how long they spent at a given task.

Biometrics in Healthcare

Biometrics has revolutionized the healthcare security industry. Biometrics is the study and analysis of biological data. Devices can take unique information about you from your eye, or your hand print, or your thumb print and use it to identify you. This information can be used to ensure that you are who you say you are, and you have permission to be working with the healthcare information you are trying to access.

Privacy in healthcare is a huge issue in these days, especially given the fact that most computer networks are vulnerable to attack or intrusion. The HIPAA act in the United States [Health Insurance Portability and Accountability Act], and many such laws worldwide, guarantee a patient's privacy. Biometrics is making it possible for patients and healthcare professionals both to feel secure that their information is being kept confidential and only being released to those who have the right to see it.

Threats in this are- firstly in this fast age of training information it would be nice to be able to send a patient's record from their doctor on one side of the country to the other, where they've just moved, and feel that the data was securely sent without chance of interception, Secondly the money invested in applying the biometric technology may be higher than the conventional ways but now the health care industry realized that the money needed to invest in biometric technology is outweighed by the money they will lose to fraud.

Mobile Biometrics, PDAs & Laptop Fingerprint Readers

Mobile biometrics is quickly becoming a lifesaver to these industries in order to speed up processing of people and goods.

Portable computers have become a household item, and biometric PDA and laptop fingerprint readers are quickly becoming the most effective way to secure that portability. Smart phones, laptops, PDAs, net books, cell phonesetc are the things that almost every family will have nowadays. The relationship between these and biometrics is a natural partnership, with benefits for both.

Biometrics takes your unique physical characteristics and uses them for identification of your identity and verification that you are doing something you've been authorized to do. Your vascular patterns, finger print, hand print, iris or retina patterns, and even your voice can be used to ensure that you are who you say you are, and to let people know that you've been given permission to do whatever it is you're attempting to do. Not only can this technology solve the ongoing problem of securing access to your laptop or PDA, but the portable devices can also solve the ongoing problem of security on the road.

People love the convenience of taking their computer or personal data with them. Having your laptop with you enables you to have work or personal files on hand at any given point in time, and easy access to a computer that is now as powerful as a desktop, in increasingly smaller sizes. PDAs enable you to check your email at the drop of a hat, have everyone's address in an easily accessible and searchable form, and be able to instantly obtain the information you need.

The very portability of laptops and PDAs, however, presents a problem. If you can take it with you, it can be taken from you. You turn your head for two seconds, someone else has decided they'd like it, and it's gone, along with your personal information, your email, and your photos - everything to which you wanted instant access. For this reason, security of portable devices has been an online problem for as long as there have been portable computers. We don't want anyone getting at our personal data.
Threats and countermeasures in this are the size of the application user is very large so that maintaining that will be of high consideration, and also the alternatives and solutions for what if the mobile biometrics gadget is lost.

3.2analysis On Impact Of Identity Thefton Biometric Service System Applications

There are three success factors which contributes the success of biometrics in applications. These are

-Technical performance

-User acceptance

-Business case

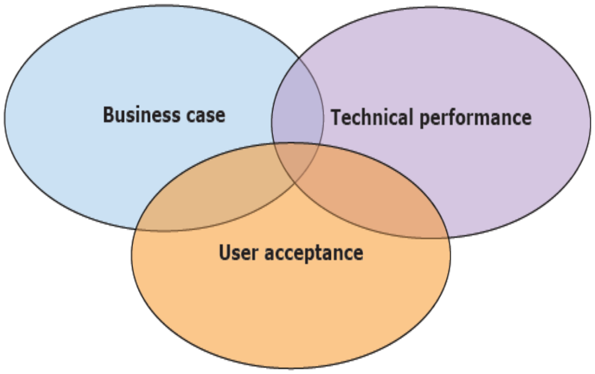


Fig.6 Success factors for Biometrics system application models

Technical Performance

As wehave seen that Identity theft become a primary problem now a days so to overcome this problem Biometric System model should be more advance in order to provide high level of security that require highly developed technology to implement them.

We have analyzed85 topcompanies [7] that provide biometrics services for different applications, most of the companies almost 55% Emphasizes on the technical and financial challenges for the biometric services. For example one of the top companies among those that provides Biometric services "Precise Biometrics "have mentioned the Technological Development as their Primary Risk factors in their annual report 2010.

Wealso have seen that most of the companies provide basically services for physical and logical access control (as shown in Fig.7) that are related to manage the Identity Theft at physical and logical level.

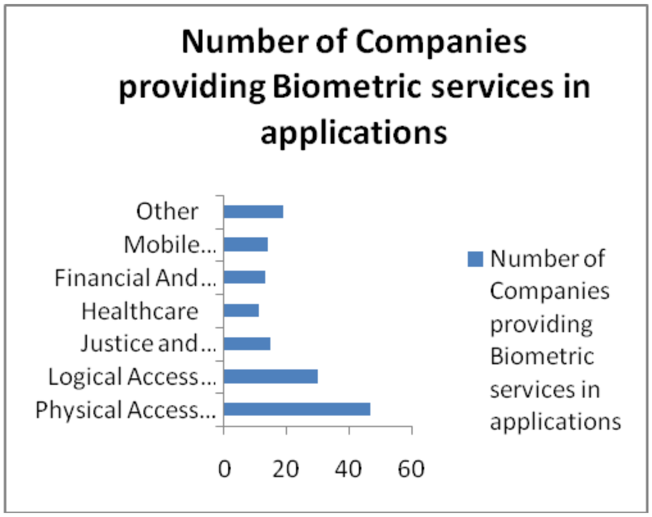


Fig.7 Companies providing Biometric service applications

User Acceptance

User acceptance also play major role for the development of biometric application models.Nowadays, several studies have been done to quantify users' acceptability and satisfaction of biometric systems such as: NIST Biometrics Usability group has performed a usability test on fingerprints [8]. The survey was conducted on 300 adults recruited from a pool of 10,000 people. There were 151 women and 149 men ranging in ages from 18 to over 65 years. 77% of participants were in favor to provide fingerprint images as a mean of establishing identity for passport purposes. 2% of participants have expressed concerns about the cleanliness of the devices with which they would have physical contact. Another study has been done by NIST to examine the impact on fingerprint capture performance of angling the fingerprint scanners (flat, 10, 20 and 30 degrees)on the existing counter heights (99, 114.3 and 124.5 cm) is presented in [9];

Opinion Research Corporation International (ORC International) has presented in [14] the results of a phone survey OpinionResearch Corporation International (ORC International) has presented in [14] the results of a phone survey conducted on 2001 and 2002. The survey has been conducted among national probability samples of 1017 and 1046 adults, respectively, living in United States. The 2001 study showed that 77% of individuals feel that finger-imaging protects individuals against fraud. For privacy issues, 87% in 2001 and 88% in 2002 are worried for the misuse of personal information. There is a good percentage of acceptance, more than 75%, for U.S. law enforcement authorities requiring fingerprint scans to verify identity for passports, at airport check-ins and to obtain a driver license (see [10] for more details).

Business case

Business case is to provide the feasibility to select biometric technologies; buyers must choose solutions to business problems, solutions that demonstrate that the biometric makes sense from a cost-benefit and business Perspective [11].

Biometrics technologies have also been deployed in a variety of commercial and enterprise applications. In these commercial domains, the total cost of ownership (TCO) and return on invested capital (ROI) must be cost justified. And although the need for greater security and compliance represent important and necessary business expenses, they are generally viewed as an overhead business expense that should be minimized.

Any security solutions chosen for commercial applications must be non-intrusive, affordable and convenient. Operational efficiencies and process improvements must be realized and cost justified. Further, as one looks out to “greenfield” markets that might benefit the most from the use of biometrics, the question becomes whether the technology is reliable, robust and simple to use in the real world environment of the specific application.

So When It is About Business case in Context of identity theft the business case should justify the level up to which that business case will solve the problem .we can justify this by considering three factors to make an efficient business case they are scale ,usability and Accuracy. Scale defines up to which quantity the chosen biometric can work while maintaining accuracy and usability of the biometric used in application.

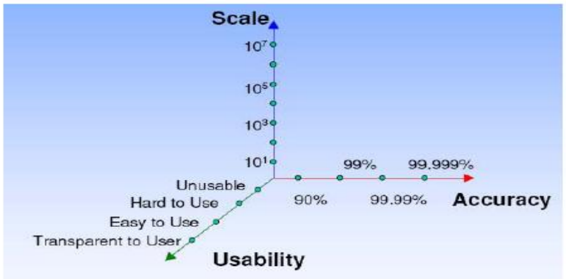


Fig.8 Factors considered for making business case

4. CONCLUSION

After analyzing the biometric application models in perspective of Identity theft we conclude that Identity Theft is a key reason for making biometric as a reliable and efficient security Measure alternative for biometric service market nowadays.

5. REFERENCES

[1] www.iso.org

[2] www.daon.com.

[3] scgwww.epfl.ch/courses

[4] [4] Sabine Delaitre ICT Unit, IPTS, JRC, European Commission in “Risk Management approach on identity theft in biometric systems context” in proceedings of First International Conference on Availability, Reliability and Security (ARES)© 2006 IEEE.

[5] www.sileo.com/identity-theft-statistics-gallup-poll

[6] www.unisys.co

[7] www.dmoz.org

[8] [8] M.Theofanos, B. Stanton, S. Orandi, R. Michaels, and N. Zhang, in“Usability testing of ten-print fingerprint capture,” National Institute of Standards and Technology (NIST), Tech. Rep., 2007.

[9] [9]M.Theofanos, B.Stanton, C.Sheppard, R. Micheals, N.-F. Zhang,J. Wydler, L. Nadel, and W. Rubin, “Usability testing of height and angles of ten-print fingerprint capture,” National Institute of Standardsand Technology (NIST), Tech. Rep., 2008.

[10] [10]Public Attitudes toward the Uses of Biometric Identification Technologies by Government and the Private Sector, Opinion Research Corporation International (ORC), Tech. Rep., 2002.

[11] www.itbusiness.ca

.