IMPLEMENTATION OF BIOMETRICS TECHNOLOGIES IN INTERNET BANKING

Syed Masaid Zaman[*]

Akash Ahmad Bhat[**]

Dr. Qamar Parvez Rana[***]

ABSTRACT

Internet banking permits customers to conduct financial transactions on a secure and safe website operated by their retail or virtual bank, credit union or building society. The providers of (E-Banking) Electronic banking services must be more responsive towards security requirements. While there isn't any doubt that Internet banking transaction should have layered protection against security hazards, the service providers should approach security considerations as a component of their service offerings. The new solution to address the issues of security and privacy is Biometric based authentication and identification. Using biometrics for identification curb individuals from access to physical spaces and electronic services. A successful authentication technique should have client acceptance, scalability, reliable performance to accommodate growth and inter-operability with current frameworks and future plans. This study mainly concentrate on providing banking services to clients using web with highly secured technology, the security issues in E-banking and its solutions in biometrics and its compliance in the consumer market are studied using exploratory and descriptive research. The methods of descriptive research are used to gain information concerning the major security issues in Electronic-Banking (E-banking). The research had been concluded on the basis of secondary data (online journals national as well as international, scientific journals, surveys).

Keywords: Biometrics, e-banking, electronic banking, e-security, secure transactions, security issues, Identity thefts

[*] Department of Information Technology, Shrivenkateshwara University Gajraula , Amroha

[**] Department of Computer Sciences, Shrivenkateshwara University Gajraula ,Amroha

[***] Course Director CCNA, Jamia Hamdard ,Hamdard University New Delhi

Introduction

Banking sectors have been delivering their services to consumers and businesses remotely for years. Electronic funds transfer (EFT), including small payments and corporate cash management systems, as well as ATM machines for currency withdrawal and retail account management are global fixtures. However, delivering financial services over public networks such as the Internet is bringing about a fundamental shift in the banking services industry.[1] According to Heikki et al. (2002), the shift from the traditional banking towards e-banking has been a 'leap' change. The expansion in information access terminals along with the growing use of information sensitive applications such as e-trade, e-learning, e-banking and e-healthcare have produced a genuine requirement of reliable, easy to use, and generally acceptable control techniques for confidential and essential information. On the other hand, the need for privacy must be balanced with security requirements for the benefit of the general public. Payment systems are experiencing radical changes stirred largely by technical advancement such as distributed network technology, real-time processing and online consumers' inclination to use electronic-banking interfaces making the study of biometrics even more vital in this new E-World.[2] Financial organizations offering Internet-based products and services to their clients ought to utilize viable techniques to authenticate the identity of customers using those products and services.[3] An precise automatic personal identification is critical to a wide range of application domains. Traditional personal identification methods (e.g., passwords, PIN) suffer from a number of drawbacks and can't fulfill the security requirement of our highly inter-connected information society. Biometrics alludes to automatic identification of an individual based on her physiological or behavioral attributes. While biometrics is not a recognizable or identification panacea, it is beginning to give effective and very powerful tools for the problems requiring positive identification. [4]

Electronic-BANKING – THE PRESENT SCENARIO:

In August of 1995, A $10 million computer fraud against Citibank was the first successful penetration by a hacker into the system which had transferred trillions of dollars a day around the world. Out of the $10 million dollars, $400,000 was not found. [5] In August 2000, three persons were arrested by British police in connection with an attempt to defraud the Internet bank Egg. The bank was reportedly the target of an effort to get cash through fake records however no cash was stolen and Egg declared that none of its PC frameworks had been breached. According to the BBC, hackers had tried to obtain thousands of pounds (GBP) via different and multiple savings accounts and loans. [7] In April 2010, a company namely fire alarm in Arkansas lost more than $110,000 in a month when hackers stole the company's online banking credentials and empty its payroll account. Over the course of the previous few days, someone had approved two batches of payroll payments — one for $45,000 and another for $67,000. A few days later, Melanie Eakel, chief executive of JE Systems Inc. , was informed by the bank that it was the "web, Internet" address that was used to process the payments, and the online banking user name and password.[6] In such a situation, information security is essential to a financial institution's ability to deliver electronic-banking services, protect the confidentiality and integrity of customer information, and ensure that accountability exists for changes to the information and the processing and communications systems. A major challenge for electronic-Banking that requires innovative approaches stems from the need to crush the effects of rapidly growing cyber-crime. Recent statistics show that the internet usage has gone up dramatically since last decade with Asia's penetration itself being 21.5% and 37.9% population of penetration for the rest of the world [8]. Further statistics report that 35.9% of financial sector is the target of Phishing frauds [9]. According to Javelin 2010 identity theft report, the number of identity theft victims and the amount of fraud increased by 12 and 12.5% respectively, the highest rate ever issued by the company. Organizations such as banks with dedicated Internet connections face greater risk of someone from the Internet by gaining unauthorized access to their computer or network than those who use dial-up modem. However, the electronic banking (e-Banking) system users still face the security risks with unauthorized access into their banking accounts. Therefore, it is very important to build in non-reputability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates.[5]

LEGAL AUTHORITIES REGULATING E-BANKING:

Most legal regulations with respect to the protection of customer interests by guaranteeing the security of e-Banking stages are considering:

- Ensuring the security and secrecy of client's data;
- Protection against any anticipated threats or risks to the security or trustworthiness of such information;

- Protection against unapproved access to or utilization of such information that could bring about considerable damages or inconvenience to any customer.

Different formal set of laws that manage e-trade and e-banking are established in various nations with the common aim of securing cyber crimes. Few of them are Electronic Commerce Act (Ireland), Electronic Transactions Act (UK, USA, Australia, New Zealand, Singapore), Electronic Transactions Ordinance (Hong Kong, Pakistan), Information Technology Act (India), Information Communication Technology Act Draft (Bangladesh) [11]. In Romania, particular legislation has been made by the advancement of Law no. 455/2001 on Electronic Signatures, Regulations of National Bank of Romania no. 4/2002 concerning transactions by electronic payment instruments and the relationship between members in these transactions and the Law no. 365/2002 on electronic commerce [10]. The Reserve Bank of India, similar to peers in Malaysia, Indonesia, the Philippines, and different nations around the globe, has made rules for e-cash issued by non banks to address a past regulatory vacuum [12]. The Information Technology Bill, 1999 and Electronic Commerce Bill, 1999 in India are planned to be general purpose legislation covering mostly issues like secure electronic records and signatures, digital signatures acceptance, duties of confirmation authority, liability of network service providers, computer crimes and information assurance. Both the bills deal with electronic contracts and they are being advanced by the Government of India primarily to encourage introduction of Electronic Data Interchange in the business division [13]. A brief examination of information security and bank secrecy regulations in developing nations uncovers an patchwork of rules issued by a variety of offices with covering purview and oversight (Lyman, Pickens, and Porteous 2008). As a sample of contrasts among nations, bank secrecy rules don't unequivocally apply to operators in India, while they do in Brazil, Peru, Colombia, and Mexico. (In India, however, providers are liable for the acts of omission and commission of their agents in all respects, including bank secrecy.) While Peru and India have information and data protection regulation, Brazil has none. [12] In India, Enactment of the IT Act 2000 and IT (Amendment) Act 2008, Anti Money Laundering Act 2002, foundation of Adjudication Officers and Cyber Appellate Tribunal, Financial Intelligence unit – India, have facilitated in giving essential legitimate system to carry out the transaction in the web/internet media. Basically the Act has given the essential legal recognition to the electronic records with the purpose of conducting e-business activities. Several offenses concerned with digital/cyber media have been identified and essential punishments in the form of imprisonment and/or with fine have been figured to control the digital/cyber crimes. The IT Act 2000, u/s 3(2) accommodates a specific innovation (viz., the asymmetric crypto system and hash function) as a method for verifying electronic record. The IT (Amendment) Act 2008 has made a notice of electronic authentication and confirmation technique, the details of which however are not specified in the Schedule II of the Act. The digital signature innovation identified in the Act needs to be compatible with the innovation adopted by the banks. Reserve Bank of India vide its rules/guidelines dated June 14, 2001, has made it compulsory for the banks to adopt digital signature as authentication tool/technique for the purposes of verification and non-revocation.

SECURITY THREATS IN E-BANKING:

Since Electronic Banking is new innovation that has numerous capabilities and also numerous potential issues, clients are reluctant to utilize the technology. The quantity of malicious applications focusing on online banking transactions has increased dramatically in recent years. The disclosure of imperative data that ought to stay private, by unapproved persons or that exceed their power can cause significant losses for financial institutions. Change of data by entering, adjusting or overwriting information into the system without approval or by exceeding one's authority is a kind of attack that could possibly harm significantly the banks and their customers. [10] A common mistake made by end users is trusting that their online banking session is superbly safe when they use a SSL connection. Security specialists persistently express that everything is safe if there is a yellow padlock symbol in the browser window. But SSL is composed as a safe passage from the end user PC to the bank centralized/mainframe computer and does not secure the end users computer. [14] The attackers install a Trojan, for example, key logger program, on a client's computer. This happens when clients visited certain websites and downloaded programs. As they are doing this, key logger program is additionally introduced on their computer without their insight. When users sign into their bank's site, the data keyed in during that session will be captured and sent to the attackers [15]. Minor interruptions with respect to third party service providers can expose banking associations to potential monetary loss and considerable legal and reputation risk. Complexity is also added by multiple vendor/service provider relationship that regularly supports electronic-banking operations. Real security ruptures in a bank or a non-bank contender's site could undermine general customer or business sector trust in banks' ability to appropriately manage Internet-based transactions. [1] Man-In-The-Middle attack is the sort of attack where attackers intrude into a current connection to intercept the exchanged information and infuse false information. It includes eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying information. Phishing attackers use email or malicious web-sites to request personal data by acting like a reliable organization. Pharming is a kind of misrepresentation that includes redirecting the customer Internet connection with a fake site, so that even when he enters the right address into his browser, he ends up on the forged WebPages. Pharming can be led either by changing the hosts file on a victims PC or by misuse of a vulnerability in D.N.S server software. In recent years both pharming and phishing have been utilized for online fraud data. The most common threats included viruses, Worms, Trojan Horses, drive-by downloads, spoofing attacks.[10]

Security threats can affect a financial institutions through various vulnerabilities. No single control or security gadget can satisfactorily protect a system associated with a public network. Numerous issues concerning the security of transactions are the result of unprotected information being sent in the middle of customers and servers. E-Banking platforms offer several methods to ensure a high level of security: (a) identification and authentication, (b) encryption, and (3) firewalls mechanism. The identification of of an online bank takes the type of a known Internet address or Uniform Resource Locator (URL), while the client is recognized by his login ID and password to ensure only approved user can access their account. On the other hand, messages in the middle of clients and online banks are all encrypted so that someone else can't see or view the contents of messages. The normal encryption standard adopted by most browsers is called Secure Socket Layer (SSL). Firewall is a set of devices designed to allow, deny, encrypt or decrypt all computer traffic between various security domains based upon a set of rules. A multi-layered security design containing firewalls, filtering routers, encryption and digital confirmation can guarantee that client account data is shielded from unapproved access. [10] At least, a two-factor authentication should be implemented in order to verify legitimacy of the data relating to Internet banking services. The first authentication component can be the use of passwords and the second validation factor can be the use of tokens, for example, a smart-card. However, for a superior/better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric. This discovers who one is, biologically.[15]

Biometrics Introduction:

Biometrics are automated techniques of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face, fingerprint, hand geometry, iris, signature, retinal and voice. Biometric technologies are turning into the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security ruptures and transaction fraud increases, the requirement for profoundly secure Identification and personal verification technologies is becoming apparent.

Biometric technologies should be viewed as and evaluated giving full consideration to the following characteristics:

I. Universality: Every individual ought to have the characteristic. People who are mute or without a fingerprint will need to be contain in some way.

II. Uniqueness: Mostly, no two individuals have identical characteristics. However, identical twins are difficult to recognize.

III. Permanence: The characteristics should not vary with time. A person's face, for example, might change with age.

IV. Collectability: The characteristics must be effectively collectible and measurable.

V. Performance: The strategy must convey exact results under fluctuated natural circumstances.

VI. Acceptability: The overall population must accept the sample collection routines.

VII. Circumvention: The innovation ought to be hard to mislead.

Types of Biometric Identifiers

Biometric characteristics of a person are unique. Most of such keys are difficult to copy and exactly produce. Theoretically these are perfect keys. But by utilizing biometric identification a lot of specific problems appear.

All biometric identifiers can be isolated into two big groups:

1) Physiological (physical)

2) Behavior

Despite the fact that behavior biometrics is less expensive and less unsafe for the user, Physiological (physical) characteristics offer highly exact identification of a person. Nevertheless, both two types provide high level of identification proof than passwords and cards.

Physiological (physical):

1. **Fingerprints**: Analyzing fingertip pattern.

Today fingerprints consider being one of the oldest and popular among other biometric technologies. Fingerprint identification is also known as dactyloskopy.

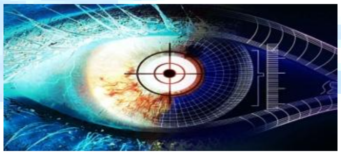
2. **Face (Facial) Recognition**: Measuring facial characteristics.

During the whole history of humanity, people used face to distinguish one person from the other. Facial (face) recognition is a computer application that automatically identifies or verifies a person with the help of a digital image or a video frame from a video source.

3. **Hand Geometry**: Measuring the shape of the hand.

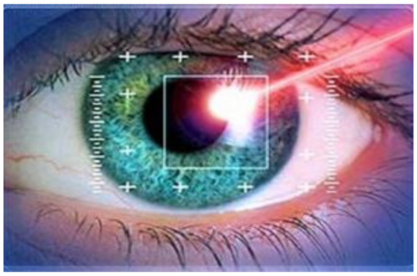
Hand geometry is the use of geometric shape of the hand for recognition purposes.

4. **Iris Recognition:** Iris is a unique characteristic of a person. The primary visible characteristic of iris is the trabecular meshwork, that makes possible to divide the iris in a radial fashion. It is formed in the eighth month of gestation. Iris is stable and does not change during the whole life. Iris recognition is considered to be one of the exact methods of biometrics. Iris is protected by eyelid, cornea and aqueous humour that make the likelihood damage minimal unlike fingerprinting.



5. **Vascular Patterns:** Analyzing vein patterns.

6. **Retinal scan**: Analyzing blood vessels in the eye.



Behavior

1. **Speaker Recognition**: Analyzing vocal behavior.
2. **Signature**: Analyzing signature dynamics.
3. **Keystroke**: Measuring the time spacing of typed words

Biometrics in internet banking

Using biometrics for internet banking is becoming convenient and impressively more accurate than current techniques (such as the utilization of passwords or PIN's). This is because biometrics links the event to a specific individual (a password or token may be utilized by someone other than the authorized/approved user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide a review trail and is becoming socially acceptable and inexpensive**.**

Advantages of using Biometric

Biometrics in banking has developed with many new ways of implementing biometrics into the banking world. Banking is only one of the industries that are being significantly influenced by the advances in this security innovation.

Since banking is such a sensitive industry that often requires consumers to recognize themselves, biometrics security offers numerous excellent advantages. Certain forms of identification are easy to counterfeit, which has prompt to a rise in identity theft today. By making utilization of biometrics technologies, the banking industry can enjoy enhanced security, providing consumers with better security that ensures their money, financial information and identity.

Using biometrics for identifying people in internet banking offers some unique advantages given as follows:

i. Biometrics can be utilized to identify you as you.

ii. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, can be lost, stolen, duplicated, or left at home.

iii. Passwords can be forgotten, shared, or watched. Moreover, today's quick-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth.

iv. Biometrics holds the guarantee of quick, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.

v. Another key aspect is how "user-friendly" a system is. The process should be speedy and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner.

vi. As biometric technologies mature and come into wide-scale business use, dealing with numerous levels of authentication or various cases of authentication will become less of a burden for users

Biometric authentication

The word “biometrics” came from Greek and we can divide it into two roots: “bio” means life and “metrics” – to measure. Biometrical authentication or just biometrics is the process of making sure that the person is who he claims to be. Authentication of identity of the user can be done in 3 three ways: 1) something that person knows (password), 2) something the person has (key, special card), 3) something the person is (fingerprints, footprint). Biometrics is based on anatomic uniqueness of a person and as follow it can be used for biometric identification of a person. Unique characteristics can be used to prevent unauthorized access to the system with the help of atomized method of biometric control which , by checking unique physiological features or behavior characteristics identifies the person.

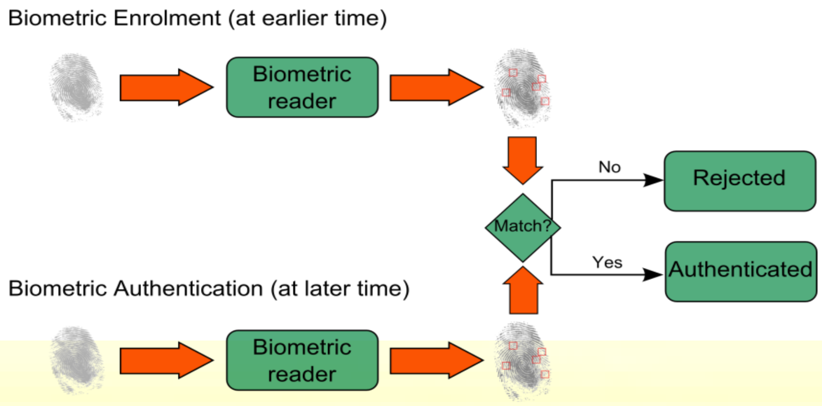
Biometric devices consist of a reader or scanning device, software that converts the gathered information into digital form, and a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value thatcan be compared with biometric data in the database .All Biometric authentications require comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). Individuals must first register their form of identity with the system by means of capturing a raw biometric to be used in the system. This process is called Enrolment and is composed of three distinct phases: Capture, Process and Enroll [6].

Capture: A raw biometric is captured by the Biometric sensing device.
Process: Characteristics that are unique to individuals and distinguish individuals from one another are extracted from the raw Biometric and transformed into a biometric "template".
Enroll: The processed template is stored in a suitable storage medium such as a database on a disk storage device or on a portable device such as a Smart Card, whereby later comparisons can be made easily.

Once Enrolment is complete, the system can authenticate individuals by means of using the stored template. Authentication is the process whereby a new biometric sample is captured by the individual who is authenticating with the system and compared to the registered (enrolled) biometric template. There are two forms of Authentication: Verification and Identification. Identification performs the process of identifying an individual from their biometric features. Identification asks the question **"Who are you?"** Verification involves matching the captured biometric sample against the enrolled template that is stored and requires the user to assert a specific claim of identity such as a user name unique key. Verification asks the question **"Are you who you say you are?"** The success of a system in performing verification is measured using the metrics below.

Successful systems will have high True Positive and True Negative values, a poor system will have high False Positive and False Negative values. Each metric is defined as follows:
TP: correctly allow access to an authorized user
TN: correctly deny access to an unauthorized user
FP: incorrectly allow access to an unauthorized user (FAR)
FN: incorrectly deny access to an authorized user (FRR)

A diagram illustrating the process of Enrollment and Authentication is shown below:


Biometric Enrolment (at earlier time)
Biometric reader
No
Rejected
Match?
Yes
Authenticated
Biometric Authentication (at later time)
Biometric reader

Conclusion:

In our study we have found that biometric technology has played an important role to control the risk factors through authentication system. Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Biometrics refers to automatic identification of a person based on her physiological or behavioural characteristics. It provides a better solution for the increased security requirements of our information society. As biometric sensors continue to become less expensive (and miniaturized), the negative perception of biometrics as encroachment on individual privacy continue to decline, and as the public realizes that biometrics is actually an effective strategy for protection of privacy/fraud, this technology is likely to be used in almost every transaction needing authentication of personal identities.[4] The market for biometric devices is not the only part of the industry that is growing. The number of technologies and manufacturers is also expanding. Some of the new technologies look at new unique attributes while others improve on ways to look at characteristics currently being used by today's biometric systems. Some new approaches are; the thermal pattern created by the blood vessel structure of a person's face, the pattern of veins and arteries on the back side of your hand, palm print. There is also work being done on an electronic nose. [21] All other factors remaining identical, the widespread use of biometrics will be stimulated by its adoption in the consumer market. The single most important factor affecting the adoption of biometrics is the cost of the biometrics systems; this includes the cost of the sensors and the related infrastructure. Additionally, biometric technologies requiring very little cooperation/participation from users (e.g., face and thermo grams), may be perceived as more convenient to users. A related issue is public acceptance. There may be a generally prevalent perception that biometrics are a threat to the privacy of an individual. The upcoming legislations (e.g., Health Information Portability Act (HIPA) may have a favorable impact on the biometrics industry. [4] Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. The one thing that can be said with certainty about the future of the biometrics industry is that it is growing! Biometrics are finding their way into all kinds of applications beyond access control. It is expected that more and more information systems/computer networks will be secured with biometrics with the rapid expansion of Internet and Intranet.

REFERENCES:

1. *Electronic Banking Risk Management Issues for Bank Supervisors Electronic Banking Group White Paper; Oct 2000; Retrieved from http://www.bis.org/publ/bcbs76.pdf (Accessed on Dec 2010)*

2. *.Sharma, K.; Singh, AJ, Biometric Security in the E World.* **.** *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering. Nemati, 2010; pp 289-337.*

3. *Authentication in an Internet Banking Environment; Federal Financial Institutions Examination Council (FFIEC); Retrieved from http://www.ffiec.gov/ffiecinfobase/resources/retail/ffiauthentication_guidance.pdf (Accessed on Dec 2010)*

4. *Jain A, Hong L, Pankanti S; Biometrics: Promising frontiers for emerging identification market; Feb 2000; Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=?doi=10.1.1.10.5497 (Accessed on Dec 2010)*

5. *Yang Y.J.; The Security of Electronic Banking. Proc. Nat. I International Systems Security Conference. National Computer Security Center. 1997; pp. 41-52.*

6. *Fire Alarm Company Burned by e-Banking Fraud; Retrieved from http://krebsonsecurity.com/2010/04/fire-alarm-company-burned-by-e-bankingfraud/ (Accessed on Dec 2010)*

7. Arrests made over Internet banking fraud; Internet Business News, Aug 2000; Retrieved from http://www.allbusiness.com/finance/615165-1.html (Accessed onDec 2010)

8. Internet World Stats - Usage and Population Statistics; Retrieved from http://www.internetworldstats.com/stats3.htm (Accessed on Dec 2010)

9. APWG ; Retrieved from http://www.antiphishing.org/ (Accessed on Dec 2010)

10. Vrancianu M.; Popa LA; Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests; The Amfiteatru Economic Journal. Jun 2010; 12(28): pp388-403

11. Jamil ZU; Cyberlaw towards a new philosophy of Regulation; Retrieved from http://jamilandjamil.com/wp-content/uploads/2010/11/cyberlaw_supreme_cou rt_v10edit.pdf (accessed on Dec 2010)

12. Dias D, McKee K; Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options; CGAP Focus Notes; Sep 2010 Retrieved from http://www.cgap.org/gm/document-1.9.47443/FN_64_Rev.pdf Accessed on Dec 2010

13. Legal Framework for Electronic Banking; Retrieved from http://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=28 (Accessed on Dec 2010)

14. Candid Wüeest; Threats to Online Banking; White Paper: Symantec Security Response; Retrieved from http://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf(Accessed on Dec 2010)JIBC August 2011, Vol. 16, No.2 - 9 –

15. Zin ANM, Yunos Z; How To Make Online Banking Secure; The Star InTech; April 2005. Retrieved from http://www.crimeresearch. org/analytics/online_banking/ (accessed on Jan 2011)

16. Bielski L.; Striving to Create a Safe Haven Online: ID Theft, Worms, Bugs, and Virtual Eavesdropping Banks Cope with Escalating Threat; ABA BankingJournal, May 2003; 95

17. Khan B.; Khan MK.; Alghathbar KS, Biometrics and identity management for homeland security applications in Saudi Arabia; African Journal of Business Management, Nov 2010, Vol. 4(15): pp. 3296-3306.

18. Whelan S.; Biometrics Technology; CGAP IT Innovation Series; Retrieved from http://www.ruralfinance.org/cds_upload/1126265263594_Biometrics_technology pdf (Accessed on Dec 2010)

19. Ratha NK, Chikkerur S, Connell JH, Bolle RM; Generating Cancelable Fingerprint Templates, IEEE Transaction on Pattern, Analysis and MachineIntelligence, Apr 2007; 29(4), pp. 561-572.

20. Liu S.; Silverman M.; A practical guide to biometric security technology, IT Professional, Jan/Feb 2001; 3(1), pp 27 – 32

21. Spence B.; Biometrics In Physical Access Control Issues, Status and Trends; Retrieved from http://www.edsales.com.au/pdfs/biom_PhysicalAccess%20Control.pdf (Accessed on Jan 2010)

22. Alter S.; The work system method for understanding information systems and information system research Communications of the Association for Information Systems (Volume 9, 2002) 90-104

23. Hogan, M. (2003), Are you who you claim to be ?, National Institute of Standards and Technology, International Standards Organisation. http://www.iso.ch/iso/en/commcentre/isobulletin/articles/2003/pdf/biometrics0303.pf

24. Internet Banking Comptroller's Handbook, Comptroller of the Currency Administrator of National Banks, October 1999, USA

25. Misra and Puri , Indian Economy , Himalaya Publishing House , New-Delhi, India (2008)

26. Mathew Johnson , A New Approach to Internet banking, Technical Report University of Cambridge Computer Laboratory, September 2008 (http://www.cl.cam.ac.uk)

27. Michael E Whitman and Herbert J. Mattord, Priciples and Practices of Information Security,Cenage Learning , Indian Edition (2009)

28. Mitchell, T. M. (1997), Machine Learning, McGraw-Hill International Editions, p. 232.

29. U.S. Pandey and Er. Saurabh Shukla , E- Commerce and Mobile Commerce Technologies , S.
Chand & Company Ltd. , New- Delhi (2010)

30. Yazan K.A. Migdali, Quantitative Evaluation of the Internet Banking Service Encounter's Quality : Comparative Study between Jordan and UK Retail Banks, Journal of Internet Banking and Commerce- Vol.3, no.2(http:// www.arraydev.com / commerce/ jibc).

31. http://en.wikipedia.org/wiki/Biometrics cited 21.02.2012,

32. http://www.biometrics.gov/documents/biohistory.pdf cited 25.02.2012