



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ATM MACHINE AUTHENTICATION USING FINGERPRINT BASED IOT

Name1

S. Ashika,
MCA Branch-computer Application
Department of Computer science
College
Prist university thanjavur , Tamilnadu, India.

Name2

G Preethi mca M.Phil PhD
Asst. Professor,
Department of Computer Science,
College
PRIST university thanjavur ,Tamilnadu,India.

ABSTRACT

Fingerprint Based ATM is a web based application where fingerprint of the user is used as an authentication. The finger print minutiae feature is unique for each human being so the user can be identified uniquely. Instead of using ATM card PIN number Fingerprint based ATM is safer and secure. There is no worry of losing ATM card and no need to memorize ATM card PIN number. The customer has to login using his fingerprint in order to do further transaction where the IOT is been used for identifying the finger print using mapping segmentation in Gaussian Smoothing Algorithm of the user from the multiple user. The customer can withdraw cash from his personal account. Customer can transfer cash to various accounts by mentioning account number. In arrange to withdraw cash user has to go through the amount he desire to withdraw and has to talk about from which account he desire to withdraw (i.e. saving account, current account) .The consumer must have suitable balance in his ATM account to do transaction.

Keywords: ATM, Fingerprint based ATM Gaussian Smoothing Algorithm, PIN

I. INTRODUCTION

Fast growth of banking machinery has changed the way banking activities are dealt with. Banking technology that has impacted absolutely and negatively to banking activities and transactions is the advent of automated teller machine (ATM). It is a mechanized machine intended to

dispense cash to bank customers without need of human interaction. They use the ATM cards for banking transactions like balance enquiry, mini statement, withdrawal, etc. ATMs are connected to a host processor, which is a common gateway through which various ATM networks become available to users. Different banks, self-governing service providers owned this host processor. Account information of user is stored on the magnetic strip present at the back side of the ATM card. ATM card holder's pin is different from each other. The password is the only identity so anyone can access the account when they have the card and correct password. Once the card and is stolen by the culprit and if he/she comes to know the password by any means then the culprit can take more money from the account in the shortest period, it may bring huge financial losses to the users. In the recent days, there have been many such ATM fraud cases. Due to some of the flaws in our present ATM system such as use of static pin and ATM card, its users face many kinds of problem and there have been many issues associated with the present system. To overcome the problems associated with the present ATM System, in our project we are using biometric features.

An Automated Teller Machine is an electronic telecommunication device that enables the customers of a financial institute to perform financial transaction, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller. On the majority modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip that contains a exclusive card number and some security information such as an expiration date. Verification is

provided by the customer entering a personal identification number (PIN). Using an ATM, customer can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones.

To use an ATM with Finger print recognition system it needs digital camera. In a day, computer will automatically initiate a face recognition procedure, whenever the computer detects a finger in finger print that obtains a picture of your finger, then the computer will compares the image of the face to the images of registered customers in its database. If the finger (as seen by the ATMs Machine) matches the picture in the data base, it automatically authenticate. The machine will then play a recording that will be heard through a loudspeaker, which says " your face is recognized". ATM is a machine which made money transactions easy for customers. This paper proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic finger recognition.

2. LITERATURE SURVEY

Roger A. Leite [1] this paper one of the primary concerns of financial institutions is to guarantee security and legitimacy in their services. The credibility of these Detect and avoid fraudulent schemes institutions also enhanced. Currently, still lack Visual Analytics techniques still lacks the fraud detection approaches. This paper proposed a Visual Analytics process that tackles the main challenges in the area of fraud detection. Financial field becomes the main challenges of fraud detection. While existing approaches employ static data displays a VA approach, focusing on fraud detection, and customer monitoring. The need of the pipeline combines efficient fraud detection techniques (i.e., AI techniques and fraud detection metrics) with VA methods.

Roger Almeida Leite [2] paper financial institutions are always interested in ensuring security and quality for their customers. Banks need to identify and avoid insecure transactions. To detect fraudulent operations, data mining techniques based on verification and customer profile generation are commonly used. Still Visual Analytics technique approaches are not supported. The proposed a Visual Analytics approach for supporting and fine-tuning profile analysis and reducing false positive alarms. Based on these challenges we propose a VA approach for profile analysis to support fraud detection and user monitoring. An integrate this VA approach into the fraud detection process to efficiently combine AI techniques with interactive visual means.

William N. Dilla a [3] interactive data visualization is potentially useful for detecting fraudulent transactions. Analyze factors influencing the efficiency and effectiveness of this technology. This analysis includes a set of testable research propositions. To detect transaction anomalies is an important fraud detection procedure the data are analyzed. To change the representation of data from text to graphics and filter out subsets of transactions for further investigation have ability to make the detection of fraudulent transactions more efficient the investigators allows the Interactive data visualization tools. This framework will developed research questions and testable propositions related to this topic. The paper concludes that how academic research might proceed in investigating the efficacy of interactive data visualization tools for fraud detection.

Johnatan S. Oliveira [4] the security of transactions is currently one of the major challenges facing banking systems. The biometric authentication using the face becomes the adopted technique due its convenience and acceptability. Nowadays, almost all mobile and computers devices have built-in cameras. User authentication approach is attracted by the large investments in banking and financial institutions, especially in cross-domain scenarios, where the facial images from ID documents that are compared with digital self-portraits (selfies) taken with the mobile devices, for the immediate opening of new checking accounts or financial transactions authorization.

T. Suganya [5] ATM though banking becomes easier, it also became feeble. There has been infinite gear of abuse in banking transactions. It is essential to provide high security. In this paper the amalgamation of Face Recognition System identifying verification process engaged in ATMs to enhance the security system is been proposed. Facial verification software at present have the task of provided that important match rates for use in ATM transactions. By adding the facial recognition systems to the identity confirmation process used in ATMs will reduce transactions to a great extent.

3. METHODOLOGY

3.1 EXISTING SYSTEM

Established ATM system confirm usually by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The current technique of user verification, which involve the use of moreover passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), undergo from more than a

few limits. Passwords and PINs can be illegally acquire by direct covert observation. Credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct individual code. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be.

DISADVANTAGE

- Less security
- Customer experience
- Can be forgotten or lost
- Environment and usage can affect measurements
- Systems are not 100% accurate.

3.2 PROPOSED ALGORITHMS

With the existing system the number of criminal cases is increasing frequently in recent years. A lot of cases associated with ATM crime have been registered where the hackers tamper with the ATM system and steal customer's card details by unauthorized ways. If the user's ATM card is been stolen and the PIN is hacked then the user's account is exposed to attack. So the existing system is not fully secured to provide security to the authorized user. To overcome these security related disadvantage of the existing system we have proposed a system where authorized user is verified with the fingerprint technology. The proposed system uses the fingerprint technology because the fingerprint provides uniqueness to identify authorized user and it is most reliable and affordable than any other technology. The proposed system operated using only ATM card and fingerprint scanner. This system provides high level of security to cardholders since there is low possibility of misuse of card and theft. With this proposed system the customer has no need to worry about the money even if the card is stolen as the customer knows that no one can replicate his/her fingerprint and withdraw the money.

ADVANTAGE

1. Fingerprint scanning technology in ATM provides accuracy because identical matches of fingerprints are nearly impossible.
2. The image template of scan fingerprint requires less memory to store.
3. Implementation of this system provides more security to ATM transaction and improves authentication
4. Fingerprint verification is cheaper and affordable.

IV. EXPERIMENT AND RESULTS

The proposed system has been implemented using

PHP tool. In the login module the authenticated admin will enter the valid username and the password to enter in the home page. This module will be accessed by the authorized user who knows the password which is developed. This module will be the gateway module for the project that will help to enter the data. Customer details Uploading module is to enter the bank customer details that are having the account. This module includes customer id, customer name, branch name, city and other particulars. The data are entered by the authorized admin. In the account transaction module the total account transaction is updated by the admin. The transactions are as transferring, withdrawing, depositing and other. This will be regularly updated. This updating can be viewed by the admin. The customer report module will display the whole report of any particular customer account transaction. This can be cross checked by the authorized admin if needed. In the finger print login module the customer will imprint their finger print before withdrawing the money from their account instead of giving the PIN number. This is the special feature that will enhance the security more efficiently.

The withdrawal of cash module will help to withdraw the cash of the customer that are in their account. This will be maintained in the record of the mini statement. The user can transfer the money from their account to other. This feature will enhance to be updated and maintained by the admin. This will create the mini statement to the user. The view balance module the user can view their account current balance of the user. This will help to view the mini statement of the account transaction. This module the transaction particular will be viewed by the user. This module will display the whole transaction details.

4.1 USE CASE DIAGRAM

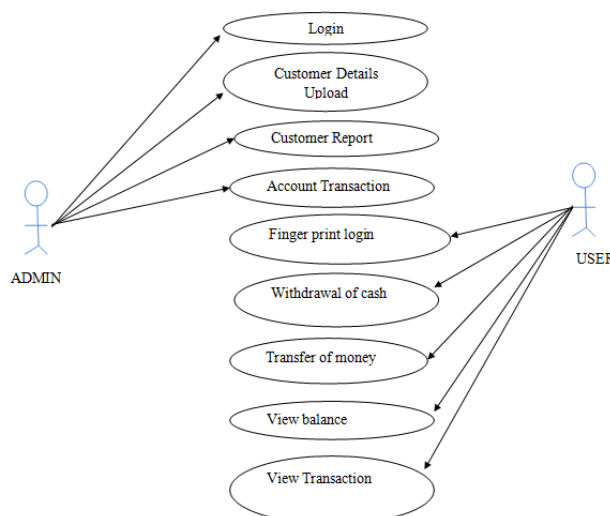
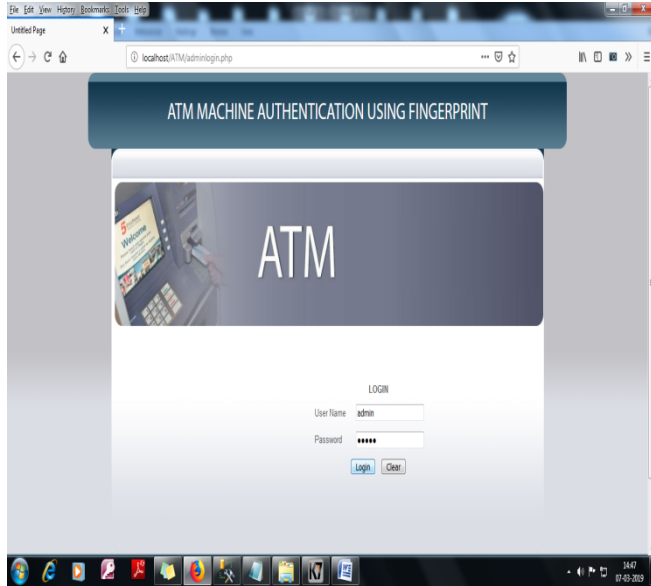


Figure 4.1 Use Case Diagram

4.2 RESULT



4.2.1 Admin Login

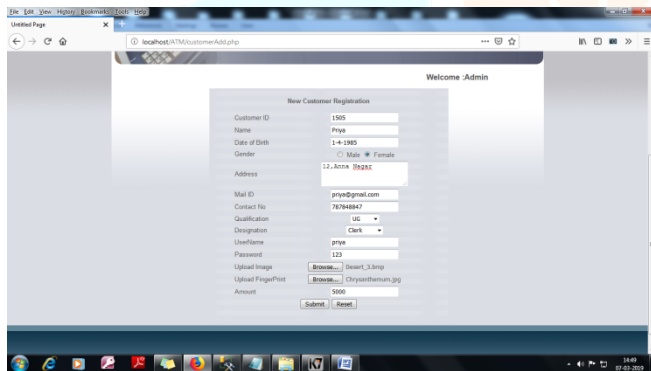


Fig: 4.2.2 Customer Registration

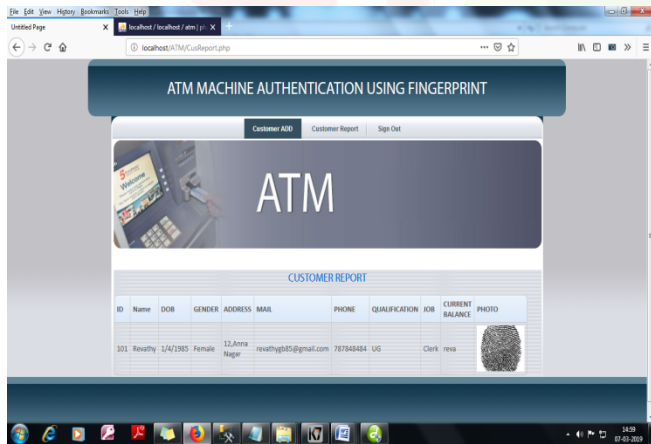


Fig : 4.2.3 Customer Report

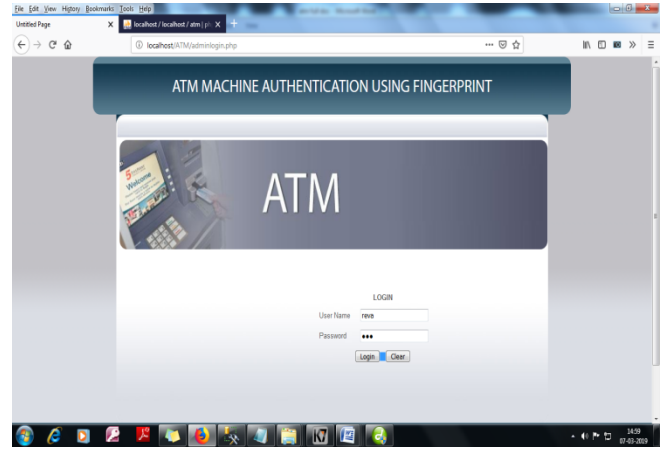


Fig: 4.2.4 User Login

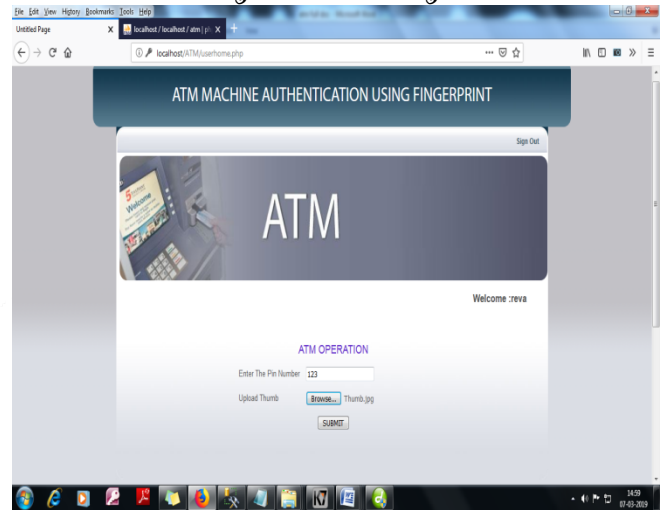


Fig : 4.2.5 ATM Open

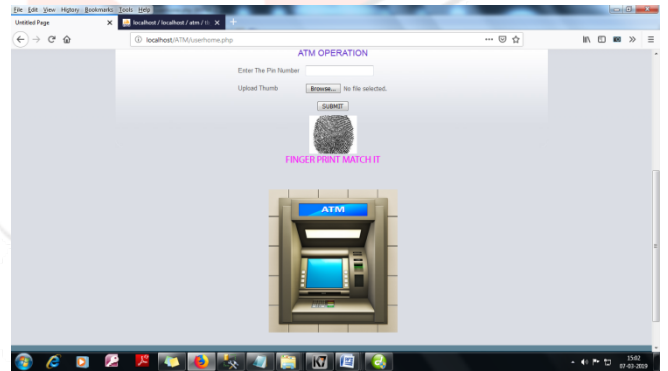


Fig: 4.2.6 Finger Print

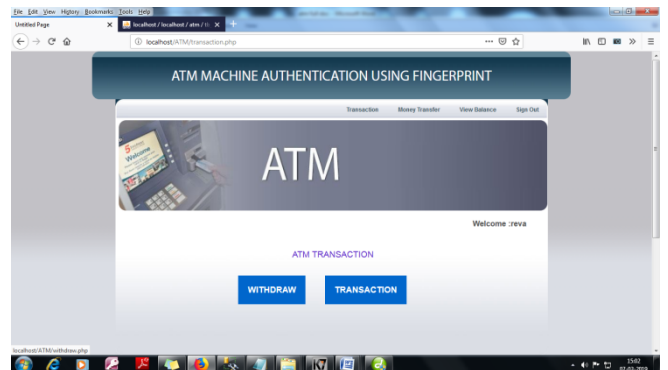


Fig: 4.2.7 Atm transaction

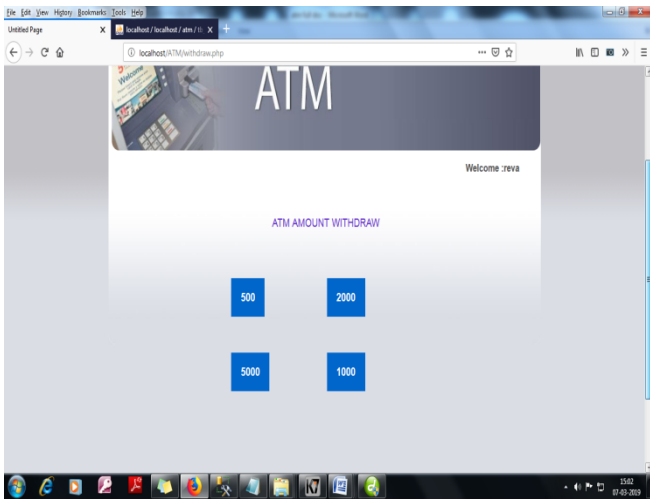


Fig: 4.2.8 Amount Withdraw



Fig: 4.2.II View Balance

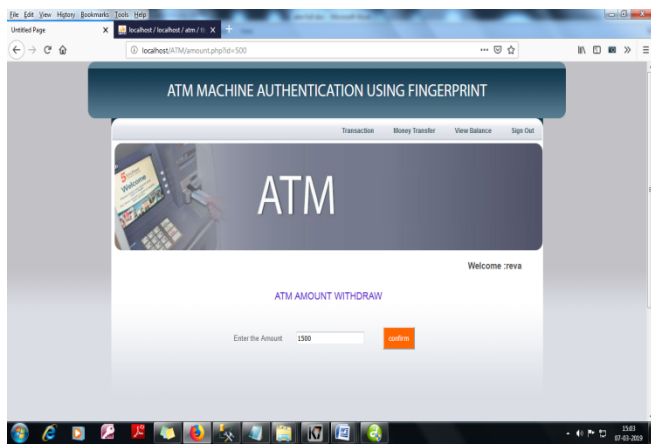


Fig: 4.2.9 Amount Withdraw

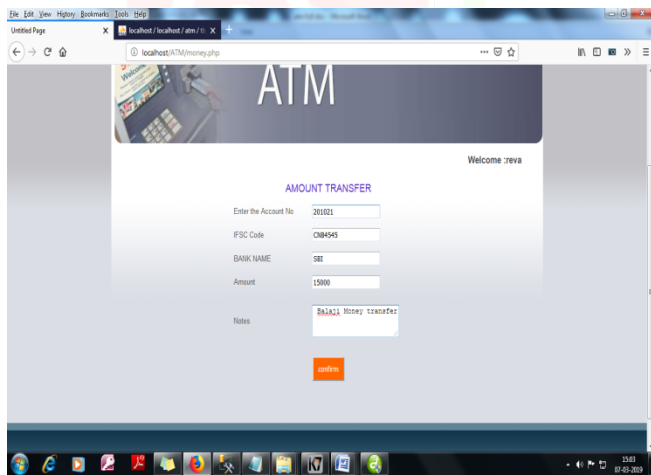


Fig: 4.2.I0 Money Transfer

V. CONCLUSION

The project presented a prototype design of an ATM access system using finger print technology. Automatic Teller Machines is the most used technology in the increasing financial transaction of the current world. There are various likely way to misuse ATM card using PIN. It's being used by bank for ATM approval and are becoming more common at grocery stores where they are utilize to mechanically distinguish a registered customer and bill their credit card or debit account. Fingerprint acknowledgment help to achieve an authentic state of security access through verification and validation. This paper identifies a high level model for the modification of existing ATM systems using both security protocols as PIN & Biometric fingerprint strategy. We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking

FUTURE ENHANCEMENT

Image Processing is useful architecture in much application like Multimedia & Graphics but still Texture Segmentation processor fingerprint many problems. So there are followings object is which my project: Here we will try to make novel algorithm which is fast as compare to previous algorithm. Here we are presenting new algorithm for Gabor filter using of error tolerant logic. Maintain image quality up to the mark with factor improvement in time complexity. Future Work These are so many fingerprint recognition models are available practice with new fingerprint recognition method. Try this with two or more nominees. Use the minutia approach for avoiding the database type attacks.

REFERENCES

- [1] Visual Analytics for Fraud Detection and Monitoring Author: Roger A. Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein, and Johannes Kuntner Year: 2013 Vol 24 pp.201-202
- [2] Visual Analytics for Fraud Detection: Focusing on Profile Analysis Author: Roger Almeida Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein & Johannes Kuntner Vol 323 Year: 2016 pp.1-3
- [3] Data visualization for fraud detection: Practice implications and a call for future research Author: William N. Dilla a, Robyn L. Raschke b Year: 2015 Vol 16 pp.1-22
- [4] Cross-Domain Deep Face Matching for Real Banking Security Systems Authors:Johnatan S. Oliveira, Gustavo B. Souza, Anderson R. Rocha, Flavio E. Deus and Aparecido N. Marana Year: 2018 Vol 22pp.
- [5] Securing ATM by Image Processing – Facial Recognition Authentication Authors:T. Suganya, T. Nithya C. Sunitha, B. Meena Preethi .vol:4 pp.913-916.Year:2014
- [6] Secured Banking operations with face-based Automated Teller Machine Authors: Olutola Fagbolul, Olumide Adewale2 Boniface Alese2and Osuolale Festus2. vol-10. pp.584-592.Year:2014
- [7] Face Detection based Locker Security System using Raspberry Pi Authors:Sandeep V. Guruprasad Hegde , Chetan N, Girish P Patil, Lad Bhavesh .vol-7. pp.73-77.Year:2016
- [8] P.K. Amurthy and M.S. Redddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.
- [9] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634,2001.
- [10] N.K. Ratha, S. Chikkerur, J.H. Connell and R.M. Bolle. "Generating Cancelable Fingerprint Templates", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, 2007. [8] B. Schouten and B. Jacobs, "Biometrics and their use in e-passport", Image and Vision Computing vol. 27, pp. 305-312, 2009.
- [11] S.A. Shaikh and J.R. Rabaiotti, "Characteristic tradeoffs in designing large-scale biometric-based identity management systems". Journal of Network and Computer Applications vol. 33, pp. 342-351, 2010.
- [12] C.A. Oyeka, An Introduction to Applied Statisticalmethods. Enugu, Nigeria: Modern Avocation Publishing Company. Pp. 4, 36, 56. 1990. (IIACSA) International Journal of Advanced Computer Science on Communication Systems and NetworkTechnologies, IEEE 2013
- [13] W.W.N. Wan, C.L. Luk, and C.W.C. in Hong Kong", International Journal of Bank Marketing, vol. 23, no. 3, pp.255-272, 2005.
- [14] Wikipedia the free encyclopedia, "Biometrics".Downloaded March 20, 2012 from <http://en.wikipedia.org/wiki/Biometrics>.
- [15] B. Richard and M. Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. Journal of Internet Banking and Commerce, vol. II, no. 2,2006. Downloaded March 15, 2012 from<http://www.arraydev.com/commerce/jibc/>

