Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

CARDLESS AUTOMATIC TELLER MACHINE (ATM) BIOMETRIC SECURITY SYSTEM DESIGN USING HUMAN FINGERPRINTS.

Madhuri More [1], Sudarshan Kankal[2], Akshaykumar Kharat[3] , Rupali Adhau[4]

[1,2,3] B.E Student, Dept. of Computer Engineering, D. Y. Patil Institute of Engineering & Technology,Ambi, Talegaon Dabhade, Pune University, India

[4]Assistant Professor, Dept. of Computer Engineering, D. Y. Patil Institute of Engineering & Technology [3], Ambi, Talegaon Dabhade, Pune University, India

ABSTRACT:- *Aim of this research paper is to propose an enhanced feature to improve the service of ATM cash withdrawal in less time with more level of security. This research is to combine the ATM & Mobile banking to reduce the time of withdrawal money from ATM with increasing level of security by adding a new feature in the Mobile banking. There is no change required to the existing system but some addition required, which makes no impact on existing system. This research, which will increase the speed of cash withdrawal almost 3 times fast; could have positive impact on the customer's satisfaction, if proper functioning is ensured by the banks. The research can be used by banks to improve the services of ATM and can enhance the overall satisfaction of their customers & save cost for new ATMs*

General Term:-*Innovation and new idea, Easy authorization process, Mobile control Way to monitor ATM networks*

Keywords:- *QR Code Reader ATM, Smart Phone, PIN, OTP, Android Studio.*

1. INTRODUCTION

The present day ATMs are using pin based security. When we are about to carry out the transaction, the pin number is fed as the input which is encrypted at the client side and the data is decrypted at the server side. When the comparison gets satisfied, we can carry out the transaction. As the technology is getting improved, the crackers are easily retrieving the data and hence the frauds are going on increasing. The data are made available on cloud [4], so that the transaction time gets reduced. When the data is available in the cloud, data can be easily retrieved for fraudulent activity, which is the biggest drawback. Hence the only way to secure the datum is to replace the computer generated numbers with the biometric security. Second leading cause of death for people between the ages of 18 and 35.

EXISTTING SYSTEM

The existing ATM system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawal and deposits, account to account transfers, balance enquiry, top-up purchases and utility bills payment. The ATM system compares the PIN entered against the stored authorization PIN for every ATM users. If there is a match, the system authenticates the user and grants access to all the services available via the ATM. If there is a mismatch on the other hand, the user authentication process fails and the user isgiven two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM.

An instance of cash withdrawal on the existing ATM system is depicted in the transition diagram in Figure. 1. Entry of a correct PIN is adequate to authenticate a user to the bank system and thereafter grant access to the system for withdrawal as depicted in Figure 1 .The existing system also retains ATM cards after entry on an incorrect PIN thrice thereby eliminating further attempts to gain unauthorized access.

2 . LITERATURE SURVEY

Research Background

The increase of automated teller machine (ATM) frauds has actuated the development of new authentication mechanisms to overcome security problems of personal identification numbers (PIN). These authentication mechanisms are usually assessed based on speed, security, and memorability in comparison with traditional PIN entry systems [8]. The biometric authentication technique seems to be the most popular emerging alternative mechanism as against PIN-based ATM authentication. This authentication technique however has its own flaws. Fingerprints, for example, are unique but they are not secrets. We leave them everywhere with everything we touch, therefore, they can easily be forged with a film [9]. The fingerprints on a person can get damaged and also, it changes with age [10]. In addition to this, another serious flaw with the fingerprints is that the theft of a person's bio-metric leads to some serious issues as re enrollment is not possible unlike the onetime password/code as well.

As a rule, the ATM's give users three tries to authenticate to the bank system. Inan event where the user fails to authenticate to the bank system, the bank card will typically be blocked and also confiscated by the ATM. If the user were to be a fraudster, confiscating the bank card would prevent the fraudster from further guessing the correct PIN and subsequently withdrawing from the card owner account via the ATM. However, in a situation whereby the fraudster is in possession of both the bankcard and correct PIN, there is no way of preventing such withdrawals via the ATM machine. Thus, this paper proposes the second-level authentication mechanism as a means to improve the security of ATM usage and operations.

A. ***Related Work***

Many recent studies have focused on using biometric techniques in enhancing the security of the ATM. However, a few studies have also exploited the use of GSM Technology, while some have adopted a combination of both techniques. Table 1 summarizes some of the related studies, the techniques they adopted, the contribution and limitations of

Table 1: Comparison of Different Papers and Their Features

Authors	Technique adopted	Contribution	Limitations
Oko S. and Oruh, J. (2012) [11]	Finger print biometric token.	• Developed an ATM based fingerprint verification and simulated it for ATM operations by incorporating the fingerprints of users into the bank's database.	1. The system developed was inefficient because there was no finger print matching algorithm. 2. The system developed was not built as an enhancement of the existing system.
Ravikumar et al. (2013) [12]	Finger print recognition in digital image processing using both primary and reference fingerprint to authenticate users instead of the traditional pin number	• A new business model which would enhance ATM security was proposed.	1. Another reference fingerprint belonging to a nominee or a close family member was adopted which also lead to a security could breech, thus compromising the security of the account owner. 2. The proposed system was not built on the existing system.
Padmapriya V. and Prakasam S. (2013) [13]	A combination of fingerprint biometric token and GSM technology	• Proposed a system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.	1. Another reference fingerprint belonging to a nominee or a close family member was adopted which also lead to a security could breech, thus compromising the security of the account owner. 2. The proposed system was not built on the existing system.
Padmapriya V. and Prakasam S. (2013) [13]	A combination of fingerprint biometric token and GSM technology	• Proposed a system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process. Activates send a pre-stored SMS to a predefined phone number.	1. A nominee or third party's finger print was incorporated in the architecture. 2. There is a discord between the main user and the nominee user in the proposed system architecture
Jimoh R.G. and Babatunde A. N. (2014). [1]	Short Message Service (SMS) verification.	• Developed an algorithm for enhancing ATM authentication system using Short Message Service (SMS) verification. • 2.Conducted a usability testing of the proposed system	1. The developed algorithm only considered a minimum withdrawal amount.

4. PROPOSE SYSTEM

The proposed system is an enhancement of the existing system, and, it is built upon the existing card and PIN-based system. The proposed system is in two different modes; the first will improve the security of the ATM by applying second level authentication on the existing ATM process for withdrawal, after entry of correct a PIN, while the second will apply second level authentication in a scenario where a customer-specified withdrawal limit is attained.

Figure 2 depicts an instance of withdrawal on the ATM for the proposed system which is an enhancement of the existing system. The entry of a correct PIN is inadequate to authenticate to the bank system. This is because an additional level has been incorporated for the authentication process which requires the customer to enter a valid code which will be sent to the customer's pre-registered mobile device via SMS gateway. If a correct code is supplied the customer gets authenticated and is granted access for withdrawal. However, if an incorrect code is supplied even after the entry of a correct PIN, the authentication process fails and the customer is denied access for withdrawal.

The second mode depicted in Figure 3 is also an instance of withdrawal on the ATM. This mode gives the customer the opportunity to choose the second level authentication process as an additional level of authentication for withdrawal in order to guarantee the security of the account owner. With this mode, a customer-specified withdrawal limit must be attained before the system prompts for entry of a valid code. If a valid code is supplied, the authentication process is complete and the customer is granted access for withdrawal. On the other hand, if an invalid code is supplied, the authentication process fails and the customer is denied access for withdrawal. It is imperative to note that if a customer-specified withdrawal limit is not in place, the entry of a valid PIN will be sufficient to authenticate the customer to the system and thereafter grant access for withdrawal. This implies that the second level authentication process would not be applied in such instances.

In addition, the entry of an incorrect PIN still guarantees maximum security in the proposed system because the bank card gets blocked and retained by the ATM in such instances..

5. SYSTEM DESCRIPTION

A. QR Code Generator Application

This QR Code Use for Scan to ATM Machine and Verify.

B. ATM PIN

This password is already required to do the transaction on ATM machine. Correct ATM password is still required when "cash withdrawal" option is selected from Mobile banking to proceed with other options.

C. ATM PIN Attempt

It is same as on ATM machine, there is limit of wrong ATM PIN attempts. If wrong attempts exceed the limit, ATM card will get blocked, which can be unlocked by contact bank.

D. OTP [8]

When we normally withdrawal the cash from ATM machine, ATM PIN is used to login. We have to take extra carefrom others, while entering the PIN. Whereas using "cash withdrawal" feature of Mobile banking, OTP is required to complete the transaction or to get the cash from ATM, which is a random number for every transaction. So, do not worry while entering OTP in front of others. Vasco (An Authentication Company) recommended OTP for user authentication to combat man-in the middle attacks.

E. OTP Attempt

It is same as ATM PIN, there is limit of wrong OTP attempts as well. If wrong attempts exceed the limit, ATM

5.1 ARCHITECTURAL DESIGN

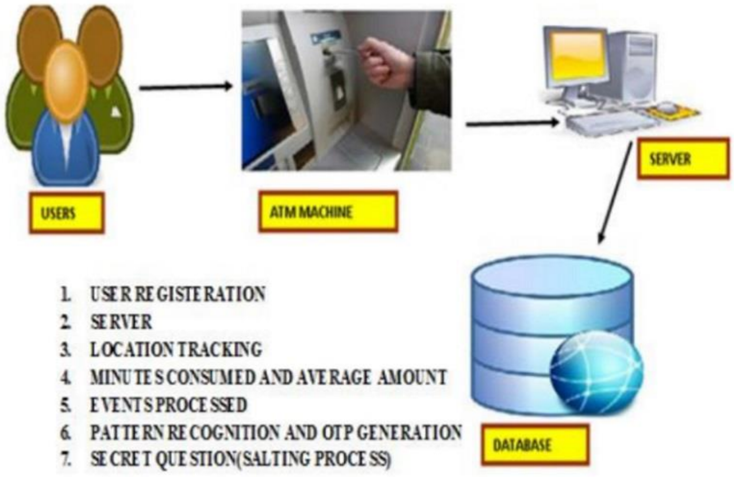
USERS
ATM MACHINE
SERVER
DATABASE
1. USER REGISTERATION
2. SERVER
3. LOCATION TRACKING
4. MINUTES CONSUMED AND AVERAGE AMOUNT
5. EVENTS PROCESSED
6. PATTERN RECOGNITION AND OTP GENERATION
7. SECRET QUESTION(SALTING PROCESS)

Fig 1: System Architecture

If any misbehavior take place it will block the enter transaction. One might think that it could be very plausible to have deviation from one of these parameters on a regular basis for the original user of the ATM card. For that purpose, our model declares a transaction as fraudulent only if 3 or more of the 4 factors mentioned above are deviated from the user' srecord then it is Post Declaring Fraudulent /Legitimate Action. If the transaction is declared as legitimate, the use may proceed with the withdrawal of cash from the ATM. But if the transaction turns out to be fraudulent one, which could happen with a slim possibility for the original user, the use would be sent a text message with a One Time Password to his/her mobile through the ATMs record searching ability and network connectivity. The user may then unblock the transaction with that password. In case of a fraudulent user, the original user would be notified that someone is performing an identity theft with their ATM card and would be prompted to take appropriate action after the realization of such an event. In case of signal problem occurs then use the secret quiz process to unblock the process.

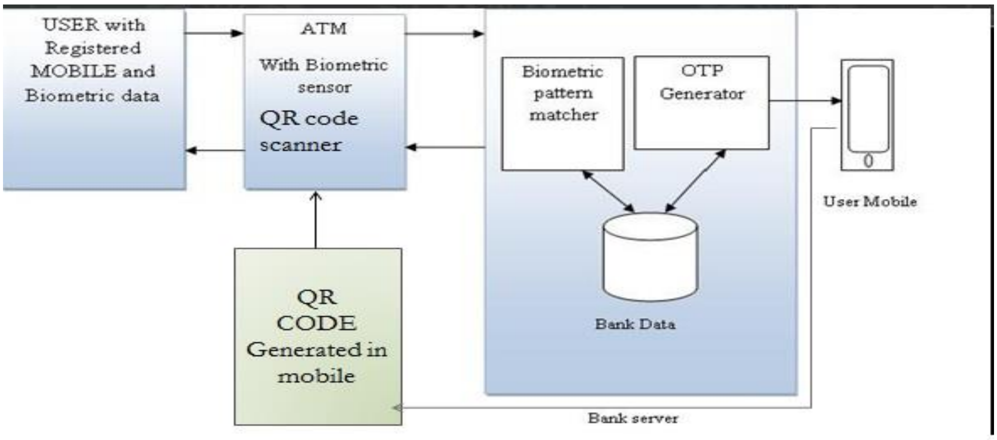
USER with Registered MOBILE and Biometric data
ATM
With Biometric sensor
QR code scanner
Biometric pattern matcher
OTP Generator
User Mobile
Bank Data
QR CODE Generated in mobile
Bank server

Fig2. System Architecture

6 ATM Algorithm

Title: To develop the problem under consideration and justify feasibility using concepts of knowledge canvas and IDEA Matrix.

Refer [?] for IDEA Matrix and Knowledge canvas model. Case studies are given in this book. IDEA Matrix is represented in the following form. Knowledge canvas represents about identification of opportunity for product. Feasibility is represented w.r.t. business perspective.

I	**D**	**E**	**A**
INCREASE : Access the ATM using Human Biometric.	**DRIVE:** Secure ATM Transaction.	**EDUCATE :** The user to log-in to the ATM system using human fingerprint and access account.	**ACCELERATE :** Log in ATM using Biometric and perform operation.
IMPROVE: Authentication of ATM system.	**DELIVER:** Secure access of ATM system	**EVALUATE :** ATM system	**ASSOCIATE:** Bank sector

Project problem statement feasibility assessment using NP-Hard, NP-Complete or satisfy ability issues using modern algebra and/or relevant mathematical models.
input x, output y, y=f(x)

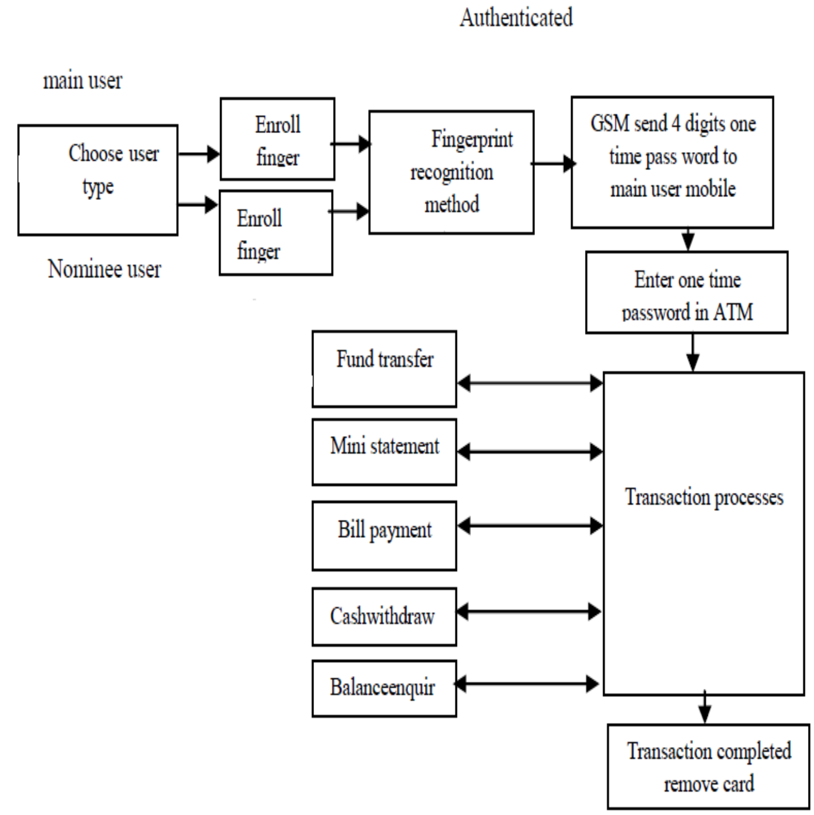

Fig3.Funational Daigram

Client Login Request:

System Data storing, identifies user and transition management, update account, save the sates of account

User login: request and make transition parameter take the responsibility for financial loss via ATM rather than being allowed to pass on the risk to the banks. In the future, we will implement the proposed system using the second-level authentication model discussed in this paper.

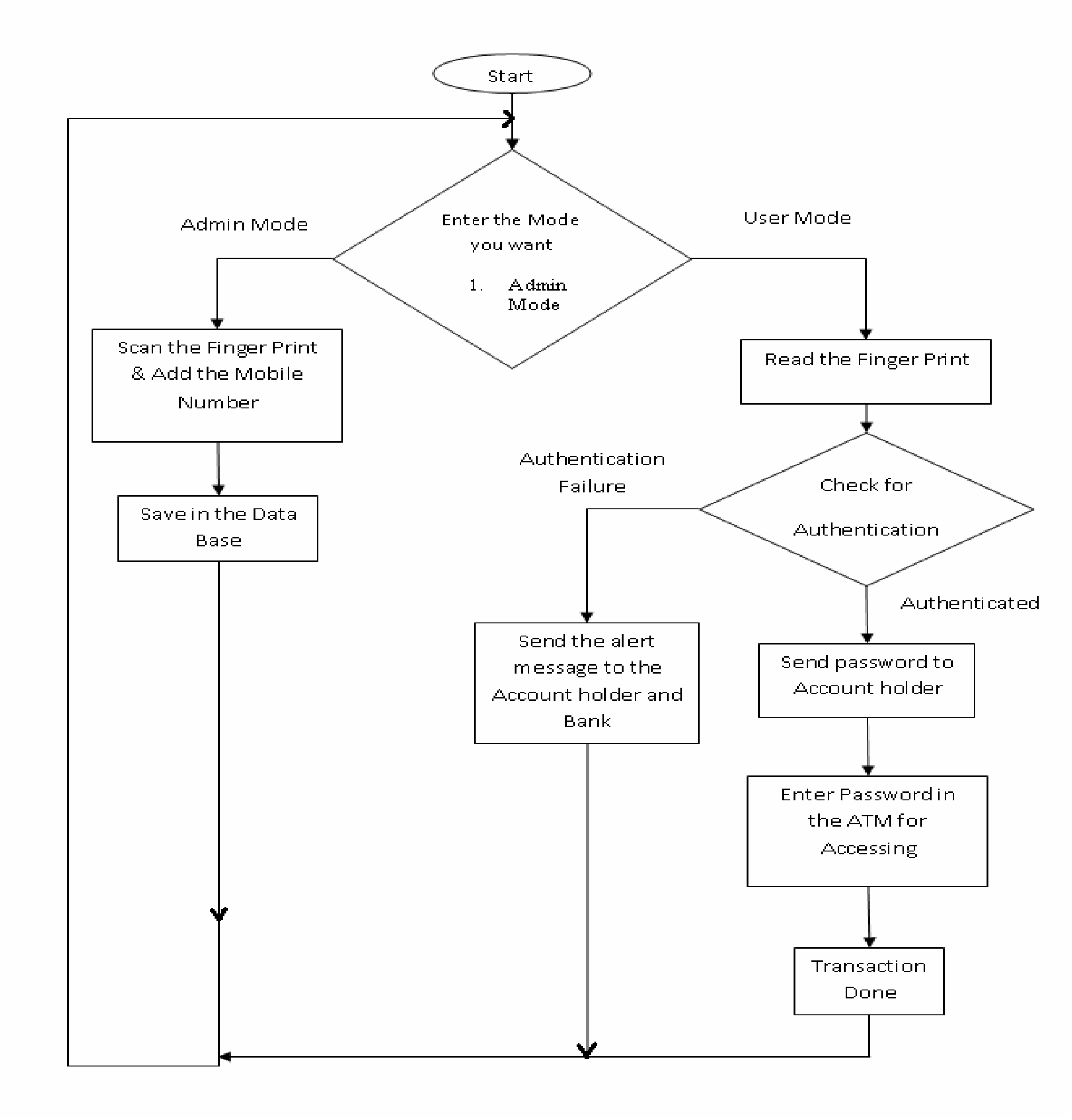

Fig4. The overall flow chart of software

6.2 The design of fingerprint recognition algorithm

The design of algorithm based on fingerprint recognition is so vital for the whole system. We would approach two steps to process the images of fingerprint.

1) The detail of fingerprint recognition process.

The first step was the acquisition of fingerprint image by above device mentioned in the algorithm, and the results could be sent to the following process. secondly, pre-processing the images acquired. After obtain the fingerprint image, it must be pre-processing. Generally, pre-processing of one's is filtering, histogram computing, image enhancement and image binarization. Lastly, the characteristic value was extracted, and the results of the above measures would be compared with the information of owner's fingerprint in the database so as to verify whether the character is matched, and then the system returned the results matched or not.

2) The design of fingerprint image enhancement

Fingerprint recognition module is an extremely important part of the system, the high-quality images was the major factors of influencing the performance in the system. The algorithm of fingerprint recognition based on the algorithm of Gabor and direction filter was used. fingerprint enhancement algorithm based on Gabor filter could be better to remove noise, strengthen the definition between the ridge and valley, it could significantly improve the image enhancement processing capacity, but this algorithm was slow in dealing with the high capacity requirements.

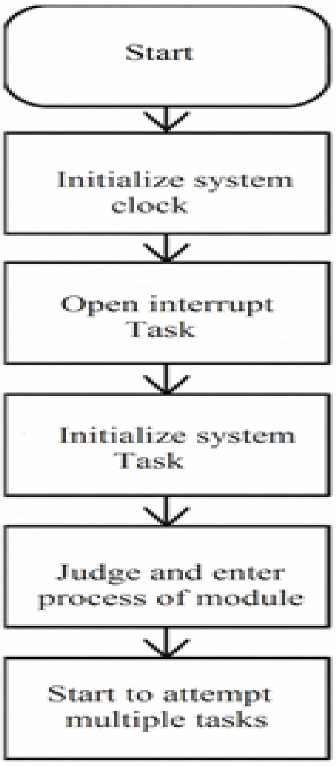

Fig5. The flow chart of fingerprint recognition

8 CONCLUSION

The adoption of the ATM as an electronic banking channel has positively impacted the banking industry worldwide because it is very effective and convenient for bank customers [20]. The advent of ATM fraud has however been a menace for many banks all over the world and many banks now aim to eradicate fraud costs to the bank. The proposed system can provide a practical and workable solution that addresses the requirements of the regulatory authority of the banks. The adopted technology of the proposed system is also cheaper to deploy than the biometric authentication technique because it utilizes the components of the existing system. The model can also provide for high withdrawal limits to cater for the demands of a cash-focused customer base. In general, it will positively impact the banking industry and the society by reducing the rising levels of crimes that are associated with ATM transactions.

The proposed second level authentication mechanism for ATMs will increase customer satisfaction and also give customers the peace of mind they need considering the high level of security applied to their accounts. Finally, it will limit the financial risks of customers given that they most times

9 REFERENCES

[1] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering 2014. Vol:8 No:1 pp.14-17

[2] Adepoju, A.S & Alhassan, M.E. (2010). Challenges of automated Teller Machine (ATM) usage and fraud occurrences in Nigeria – A case study of selected banks in Minna metropolis. Journal of Internet Banking and Commerce. Vol 15, No. 2. pp. 1-10. [Online]. Available: http://www.arraydev.com/commerce/JIBC/2010-08/Solomon.pdf

[3] Siddique, M.I & Rehman, S. (2011). Impact of Electronic crime in Indian banking sector – An Overview Int. International Journal of Business & Information Technology. Vol-1 No. 2 September 2011 pp.159-164

[4] Leow, H.B. (1999). New Distribution Channels in banking Services. Banker"s Journal Malaysia, No.110, June 1999, pp.48-56.

[5] Aliyu, A.A. & Tasmin, R.B. (2012) Information and Communication Technology in Nigerian Banks: Analysis of Services and Consumer Reactions. In proceedings of 3rd International Conference in Business and Economic Research (3rd ICBER 2012) MARCH 2012. pp. 150-164

[6] Shoewu, O. and Edeko, F.O. (2011). Outgoing call quality evaluation of GSM network services in Epe, Lagos State. American journal of scientific and industrial research. Vol 2 No.3. pp. 409-417

[7] Rosenblatt, S. (2013). Two-factor authentication: What you need to know. Retrieved from: http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ Last updated on April 14, 2014. Accessed on November 23, 2014.

[8] De Luca, A., Langheinrich, M. & Hussmann, H. (2010). Towards Understanding ATM Security – A Field Study of Real World ATM Use. Retrieved from: https://cups.cs.cmu.edu/soups/2010/proceedings/a16_deluca.pdfAccessed on November 26, 2014.

[9] Kyle, C. (2004). Biometrics: An In Depth Examination. SANS Institute Information Security Reading Room. SANS Institute 2004. Retrieved from: http://www.sans.org/reading-room/whitepapers/authentication/biometrics-in-depth-examination-1329. Accessed on November 26, 2014.

[10] Liu, N. Y. (2013). Bio Privacy: Privacy Regulations and the Challenge of Biometrics. Taylor & Francis 2013.

[11] Oko, S. and Oruh, J. (2012): Enhanced ATM security system using biometrics. IJCSI International Journal of Computer Science Issues, September 2012. Vol. 9, Issue 5, No 3, pp. 352-357.

[12] Ravikumar, S., Vaidyanathan, S., Thamotharan, S. & Ramakrishan, S. (2013), A new business model for ATM

[13]. Maninder Singh, Shahanaz Ayub and Raghunath Verma, "Enhancing Security by averaging multiplefingerprint images," Proc. International Conference on Communication Systems and Network Technologies, IEEE 2013.

[14]. S.T. Bhosale Research Scholar V.P. Institute of Management Studies and Research, Sangli Dr. B.S.Sawant Director K. B. P. Institute of Management Studies and Research, Satara "Security in e-banking via cardless biometric ATMs," Proc. International Journal of Advanced Technology & Engineering Research (IJATER), 2012.

[15]. Roli Bansal, Priti Sehgal and Punam Bedi "Minutiae Extraction from Fingerprint Images - a Review," Proc. International Journal of Computer Science Issues(IJSCI), 2011.

[16]. Rajkumar Buyya, Chee Shin Yeo , Srikumar Venugopal, James Broberg, Ivona Brandic, Proc. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5thutility," (Elsevier), 2009.

[17]. A. J. Willis and L. Myers, "A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips", Pattern Recognition, vol. 34(2):255–270, 2001.

[18]. A.M.Bazen and S.H.Gerez, "Achievement and challenges in fingerprint recognition", in Biometric Solutions for Authentication i an e-World, 2002, pp.23–57.

[19]. L. Coetzee and E. C. Botha, "Fingerprint recognition in low quality images", Pattern Recognition, vol. 26(10), 1993, pp. 1441–1460.