ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Enhancement of Bio Metric Security of Automated Teller Machine through Integration of Bank Account with AADHAR Account and Using One Time Password to Avoid Fraudulent Transaction.

K Kajendran* and A Pravin.

Department of Computer Science and Engineering, Sathyabama University, Chennai, Tamilnadu, India

ABSTRACT

Debit cards with traditional PIN authentications were more prone to security breach that helps fraudster to carry out financial fraud. To overcome this, bio metric based authentication can be used, which is more secure than PIN authentication. But, the drawback of bio metric authentication is that it restricts only the account holder to withdraw money, not by family members. Second drawback is that Even though it is highly secured, there are advanced technologies through which bio metric information such as pattern of finger, iris, and retina can be stolen and misused by culprit to withdraw money in an unauthorized way. This paper suggests an alternate solution to enhance ATM security using palm vein with more user friendly way by allowing their family members also to withdraw money from ATM machine using their palm vein image as mode of authentication. To make bio metric based authentication highly secured and more user friendly, this paper proposes AADHAR linked biometric authentication in the ATM machine, since AADHAR database consist palm vein images of all family member. To make this authentication more secure, generation one time password(OTP) is integrated with bio metric authentication

Keywords: Palm Pattern Recognition, Bio Metric Security, ATM Security

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Automated Teller Machine is part of people's day to day life to meet their daily financial need that saves lot of customer time for withdrawing their money from bank account without being physically present in the bank in which they have their bank account. Automated Teller Machine is the one which is often misused by the culprit to withdraw money from other customer account by using fake ATM card. ATM center is the one of the common place where security breach of customer's sensitive information takes place, which includes customer's name, ATM card number, personal identification numbers (PIN) and other details through skimmer machine installed in the ATM center. Other way of obtaining customer sensitive information includes shoulder surfing, using spyware, key loggers, and through spoofing web site. Online transaction is another dangerous place where customer can lose their debit card details to the hackers, wireless network makes security breach even worse. There could be Malware running on customer's computer through which debit card detail get compromised. It is the duty of financial institutions such as banks to offers enhanced security in the ATM center to protect their customer from losing their valuable information of their bank details to hackers. Bio metrics based authentication always has its own merits compare with traditional authentication such as using user and password, or ATM PIN, because it provides highest degree of protection to customer's bank account.

News about security leakage of debit card details of various customers is often appearing in news paper. In India, On 20th October 2016, there was a news appeared in news paper about leakage of debit card details of about 3.2 million customers from the ATM of a private sector bank. The breach is originated in malware introduced in systems of Hitachi Payment Services which serves Yes Bank, enabling fraudsters to steal information allowing them to steal funds. Due to this leakage ICICI Bank, HDFC Bank and Yes Bank have asked customers to change their ATM pin numbers. HDFC Bank, SBI also advised its customers to use its own ATMs for carrying out any transaction.

This paper proposes solution to protect customer bank account from unauthorized withdrawal of money from ATM machine. Linking of AADHAR account with customer's bank account and using palm vein based bio metric authentication can help to guard customer's bank account against unauthorized access. This interlinking also helps family member of the account holder to withdraw money from ATM machine using their palm vein, which is stored in AADHAR database. Inclusion of One Time Password (OTP) password prevents fraudster from withdrawing money from ATM machine in unauthorized manner

LITERATURE SURVEY

Initially, people use to go to bank to withdraw money in various denominations which used to purchase commodities and various products. The traditional paper and metal based currency is now modernized with plastic money in the form of debit card, now around the world purchase of anything is done online by the use of debit cards, credit card[1], which facilitate the customer to purchase any product from home without physically going to the shop. Once ATM is become popular, people now a day's literally never go to bank to meet their daily monetary need, instead they started using debit card in the ATM machine withdraw money, by entering their four digit PIN. Using PIN for authenticating ATM transaction is not safe, .because this system introduces its own level of security breach which includes disclosing ATM card details and PIN to the hacker via skimmer unknowingly installed in ATM machine, which leads to monetary loss to actual customer. Remembering four digits PIN numbers of various smart cards introduce significant overhead to ATM users [6]. When customer feels insecure then they avoid using ATM for their money transaction. To protect customer and their money from being looted by hacker all banks were introduced another level of security in the form of one time password (OTP). This concept was originally introduced by Google to improve the security of Google App and Gmail account into another level in addition to traditional username and password authentication. The same concept is suggested is suggested by Prof. (Dr.) Prashant P. Pittalia [2] to protect ATM user from being victimized by ATM financial fraud which includes integration of one time password with ATM Transaction

The bio metrics authentication system is generally classified into the following: physiological based bio metric and behavioral based biometric. The physiological biometrics consists of face, fingerprint, hand, eye and the behavioral biometrics consists of signature, voice, and keystroke. Among these various biometric authentication suggested fingerprint matching, iris recognition and palm recognition are popular which offers better accuracy and reliability. Integrating two or more biometric authentication yield high level of protection,

compared with the use of single biometric authentication. In his paper he also proposes assessment of image quality to identify if the image captured is a fake or real image sample by comparing the different qualities based on following characteristics: degree of sharpness, color luminance levels, local artifacts, and entropy [3].

Aru et al [5, 12] in their paper, suggested integration traditional debit card - PIN authentication with facial recognition of person who taking money from ATM. This mechanism could prevent fraudulent withdrawal using fake debit card from ATM machine. But this mechanism is difficult to implement.

Integration PIN based authentication with voice verification is suggested by Muhammad-Bello B.L.[4]. But as of now we have efficient technology for recognition of voice, so this proposed system was practically difficult to implement. Researchers [6,7,8] in their paper, all suggested the use of finger print matching along with traditional four digits PIN to increase ATM security to next level. The demerit of this solution is that if the hacker captures both PIN and finger print, there is the possibility unauthorized ATM transaction by hackers lead to loss of customer's valuable money [9, 10, 11]. The drawback of these systems is that the hackers can duplication and use pattern of iris and finger to execute unauthorized transaction with sophisticated technologies currently exists, because duplication is made easy due to area of iris and finger they required to duplicate is very small . Jobin J. et al in their paper proposes a new algorithm for palm recognition that can be efficiently, reliably used to identify person in ATM machine [13, 14].

IMPLEMENTATION

The pattern of every individual palm vein is unique from others. Once the bank account is being created by customer, to enable biometric based palm authentication, every account holder's record in the bank is linked with AADHAR database using family card number, which maintain images of palm veins of all family members. For fast transaction only the account holder's palm vein is stored in the bank database, other palm vein images are stored in the AADHAR database. To withdraw money from ATM machine, the people who attempt to withdraw money has to first insert their debit card then place the palm of the hand above the palm reader which take snap shot of palm image. Capturing of palm image is done using infrared rays. The image generated by palm reader is then compared with the palm image stored in the bank database. If there is match found then this system sends OTP to the register mobile number of the account holder. Only after validating OTP, this system allows the account holder to withdraw money from ATM.

ISSN: 0975-8585

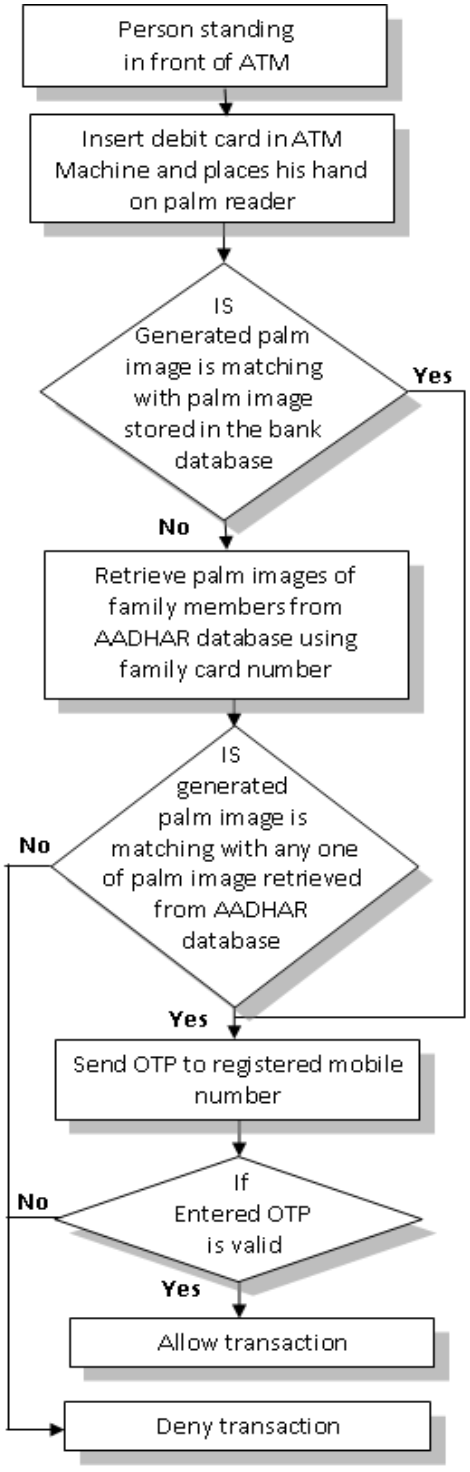

Figure 1: ***Flow chart of proposed system***

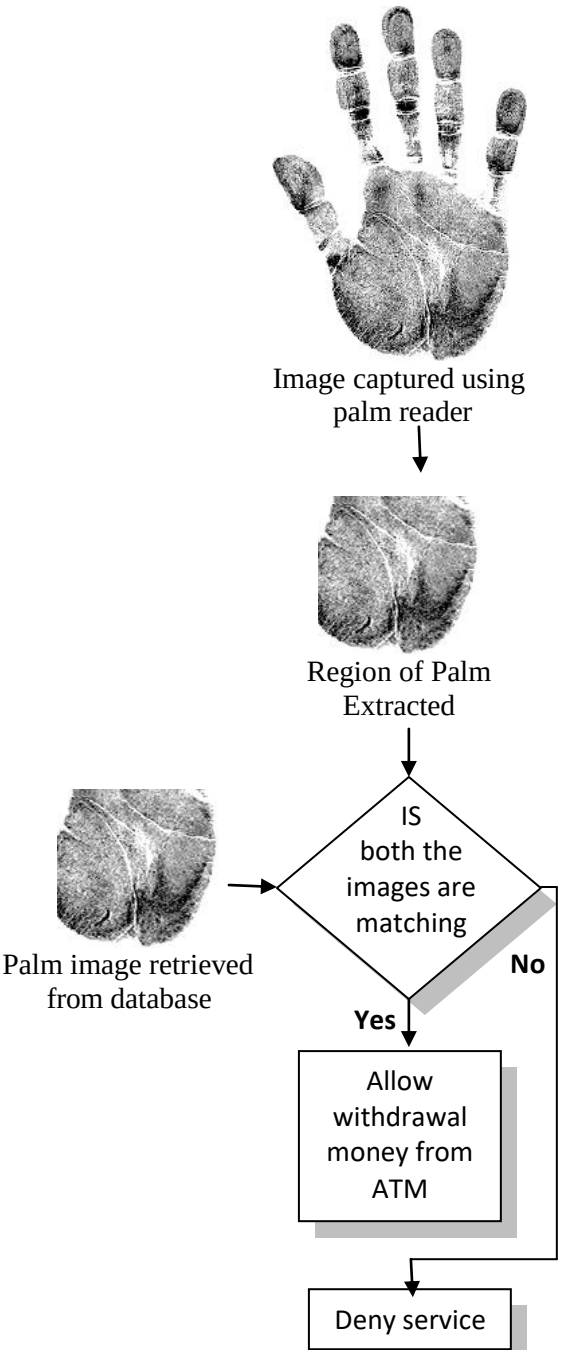

Figure 2: ***steps involved in palm processing***

If the palm image is not matching the one in the bank database, palm images of their family member is retrieved from AADHAR database using family card number, and these images are compared with palm image generated by the palm reader. If matching found for any one of the palm image retrieved from AADHAR databases then the person is allowed to withdraw money after validating OTP, otherwise withdrawal denied. This makes ATM transaction more secure and user friendly, preventing fraudster from withdrawing money from ATM, and allowing family members to withdraw money. Bank in such as *the Suruga Bank* and *the Bank of Tokyo-Mitsubishi* in Japan have already used palm vein validation sensor to validate account holder authenticity, which is proved very efficient. *Figure 3.1* describe the working functionality of the proposed system

CONCLUSION

The bio metric based palm vein authentication of ATM is proved to be one of the best and more secure among all existing bio metric authentication, if bank account is interlinked with AADHAR database. This authentication mechanism is more user friendly, because it allows the family members of the account holder to withdraw money from ATM by using their palm vein as mode of authentication. This authentication mechanism is made more secure by integrating it with one time password

REFERENCES

[1] Adepoju, A.S & Alhassan, M.E., "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, 2010

[2] Prof. (Dr.) Prashant P. Pittalia, "Enhancemnet of ATM Security and Theft Protection with the Use of One Time Password", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015

[3] Javier Galbally, Sebastien Marcel and Julian Fierrez, "Image Quality Assessment for Fake Biometric detection Application to Iris, Fingerprint and Face recognition",IEEE trans.on image processing ,vol. 23,No.2 February 2014

[4] Muhammad-Bello B.L. , Alhassan M.E., Ganiyu, S.O., "An Enhanced ATM Security System using Second-Level Authentication", International Journal of Computer Applications, Volume 111 – No 5, February 2015

[5] Aru, Okereke Eze, Ihekweaba Gozie, "Facial Verification Technology for Use In ATM Transactions", American Journal of Engineering Research, Volume-02, Issue-05, pp-188-193, 2013

[6] D.Shelkar Goud,Ishaq Md,P.J.Saritha,"A Secured Approach for Authentication system using fingerprint and iris",Global journal of Advanced Engineering Technology,Vol,Issue3-2012

[7] S.T. Bhosale and Dr. B.S.Sawant "SECURITY IN E-BANKING VIA CARD LESS BIOMETRIC ATMS", International Journal of Advanced Technology & Engineering Research, Volume 2, Issue 4, July 2012

[8] Rathishala Rajendran, Kavita Anandraj, Edwina Jacob, Chhaya Narvekar, "ATM Security using Fingerprint Authentication and OTP"

[9] Prof. Selina Oko and Jane Oruh, "ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012

[10] Biswas S., Bardhan Roy A., Ghosh K. And Dey N.,"A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

[11] Edmund Spinella SANS GSEC," Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", San Francisco, 28 May 2003

[12] Aru, Okereke Eze, Ihekweaba Gozie," Facial Verification Technology for Use In Atm Transactions", American Journal of Engineering Research (AJER), Volume-02, Issue-05, pp-188-193

[13] Khalid Saeed, Marcin Werdoni, "A New Approach for Hand-Palm Recognition", Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems, pp 185-194

[14] Jobin J., Jiji Joseph et al., "Palm Biometrics Recognition and Verification System", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 1, Issue 2, August 2012.