CREDIT CARD TRANSACTION USING FINGERPRINT RECOGNISATION AND TWO STEP VERIFICATION

C. Jyotsna Priya[1], R.V. Deepti Rosini[2], M. Likitha[3], Ms. Dhanalakshmi .R[4]

[1,2,3]UG Scholars, Department of Computer Science and Engineering, R.M.K Engineering College, Tamil Nadu, India.
[4]Assistant Professor, Department of Computer Science and Engineering, R.M.K Engineering College, Tamil Nadu, India.

---***---

Abstract - *The rapid growth in the number of Bank Transactions demands more security and resistance against various threats. In this paper we are going to enhance the security of the credit card transactions in the ATM machines using three step verification process. Here we use password, fingerprint and OTP to increase the level of security in the transaction. The use of biometrics, which is unique to each and every individual, to strengthen the authentication of individual users and to eliminate fraudulent from using the legitimate account. To verify the password, we use KNN Clustering algorithm which gives consistent results. When there is a mismatch of password, dummy balance will be shown in the ATM machine display screen and an alert message will be send to the nearby police station. The KNN clustering algorithm is effective and can be easily implemented. Improvements in KNN speed is possible by using proximity.*

Key Words: Credit card transaction, Fingerprint, OTP, Biometric,
ATM card transaction.

1. INTRODUCTION

Traditionally we had one step verification which is by using a password to authenticate a legitimate user. In this case the initial password is provided by the respective bank of the ATM card. The user can reset the password of his/her wish and should maintain it secretly. If the user losses the ATM card or if someone steals the card and by using the Brute force attack the culprit can do the transaction within a short span of time even before the legitimate user finds out that the card is missing. The Brute force attack is used in situation to guess the password by trial and error method. Since most of the people will keep their name, family members name, birthplace, DOB etc as their password. If the culprit is from their own family, then it is very easy for that person to guess any of those and succeed in transaction. The best way to overcome this problem is to use biometrics technique to authenticate a legitimate user. There are various biometric technique available like face recognition, fingerprint recognition, palm vein recognition, iris recognition, vein recognition, voice recognition, handwriting etc. These characteristics remains constant and unique throughout the life. Using such scanning hardware turned out to be costly for the banks but its gives a high level of security which makes it worth of using the biometrics. Image processing is another important task which should be performed carefully so that the fraudulent is not allowed to access a legitimate users account and the legitimate user is not denied to access his own account. Initially the bank captures the fingerprint image of the user while issuing the ATM card and that captured image is stored as template. During transaction the user's fingerprint is scanned by the fingerprint scanner and the captured image will be compared with the stored template in database for matching. The template is a collection of minutiae points, which is bifurcation and ridge ending. Bifurcation is a ridge splitting into two ridges. A template is nothing but an image with black ridges and white furrows with high lightened minutiae points. A threshold value is set by the bank, a minimum match value between the captured image and stored image, because exact match is not possible due to certain factors. The factors be like pressure on the fingerprint scanning device, cuts, wear and tear of the device, weather conditions etc. Finally the OTP is generated from the database to the registered mobile number and verification has to be done by entering that OTP value in the ATM machine screen. Though the process seems to be complex but the security provided by three level authentication is unbeatable and entirely safe from threat.

2. EXISTING SYSTEM

Credit card authentication using fingerprint and OTP is proposed in a paper [2], where the Fingerprint based authentication system uses power supply, microcontroller, fingerprint module, LCD, GSM module to send OTP to the registered mobile number. The initially captures the fingerprint of the user following which processing has to be done to extract the characteristics vectors and it will be stored as template. During transaction the user will place the finger on the fingerprint scanning device, that image will be enhanced and will be compared with the stored template for matching. If matching succeeds, the GSM module will send the OTP to the registered mobile number and that OTP should be retyped on the ATM screen and if the typed OTP is correct then the transaction will be successful else the transaction will be terminated. The existing system project is different from the proposed system in the following ways.

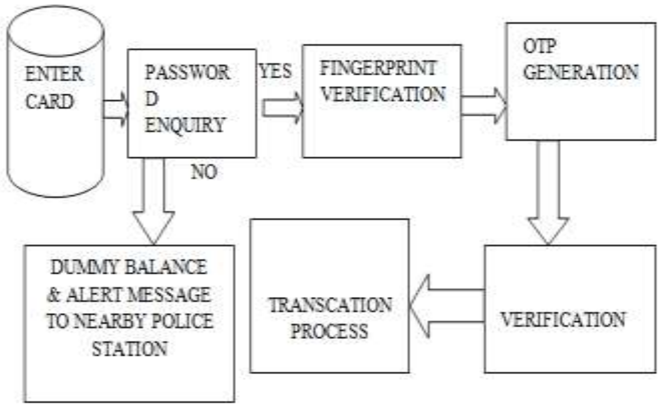
1. In our paper, the user will enter the password prior to the fingerprint processing and OTP generation, which makes it three level security.

2. We set threshold value in order to eliminate any discrepancies in the fingerprint processing so that a legitimate user is not denied of accessing his own account.
3. During an unfavourable situation, when the user enters incorrect password, a dummy balance will be shown in the ATM machine screen and an alert message will be send to the nearby police station.
All these makes the proposed system more secure and resistant against any form of attacks or threats that would cause financial losses to the stakeholders and would protect the transaction from the outsiders.

3. PROPOSED SYSTEM

This paper overcomes the security problems faced by the people in the existing system. Here to make a transaction through credit card, we use a three step verification process which includes entering the PIN number, scanning the fingerprint and OTP generation. As the card holder swipes the card and enter the PIN number, the system verifies it with the stored database. This verification here is done by KNN clustering algorithm which groups the provided PIN number by the user as one group of data and checks this data with the bank's stored database for similarity. If the PIN number verified is incorrect, it shows a dummy balance on the ATM display screen. If the entered PIN number is correct, it proceeds with scanning the fingerprint of the user. This biometric helps in a way that only authorized user can access their own account. After scanning the fingerprint embedded in the ATM machine, it check whether it is matched with the fingerprint stored in the bank's database, which is stored at the time of registering a card holder's account. If the fingerprint gets matched, the user is gets an One Time Password (OTP) to the registered mobile number. This OTP is valid only for one time and it is useless for the hacker to use this next time. After entering the OTP, the process gets completed and the transaction is made to be successful.

BLOCK DIAGRAM OF PROPOSED SYSTEM



4. SOFTWARE DESCRIPTION

4.1 MATLAB:

Mat lab is a matrix based programming tool and a high-performance language for technical computing. Matlab image processing works with the principle of, image loading, using the right format, storing data having different data types, displaying an image and conversion of image formats, etc. The different image formats that are supported by Matlab are BMP, HDF, JPEG, PCX, TIFF, XWB. The common formats are, intensity image, binary image, indexed image, RGB image and multi frame image. Mat lab works on three basic window, Command window, Graphic window, Edit window. Unlike other programming language, it provides mathematical expressions using Variables, Operators, Numbers and Functions. Mat lab stores information in form of three types of files which are M-files, Mat-files and Mex - files.

5. RESULT AND ANALYSIS

As the card holder swipe his card in the ATM machine, all the user credentials get scanned through and checked with the database. Then the user enters the four digit credit card PIN number. If the entered PIN number is correct, then it is an authorized user. If it is incorrect, then a dummy balance will be displayed.

Next the system asks for the user's fingerprint. The card holder has to place his/her thumb in the fingerprint sensor embedded in the ATM machine. If the scanned fingerprint matches with the stored fingerprint of the bank's database then the user is allowed to proceed the transaction. When the fingerprint gets matched, an OTP will be sent to the registered mobile number. After entering the OTP the transaction will be completed.

6. CONCLUSION

Automated Teller Machine have become a vital technology for providing financial services to an increasing segment of the population. In this paper, we use the fingerprint biometric so that only authorized user can able to proceed the transaction. This proposed system enhances a reliable form of secured access and a high level of modification to the existing system by using both fingerprint sensor and OTP generation. OTP generation removes fraudulence since it can be used only once at a time. It describes in brief about the extraction and matching of fingerprint images with the bank's database. Overall this proposed system provides a high level of authentication in the credit card transaction using Fingerprint and two step verification.

7. REFERENCES

1. Dr.M. Umamaheswari, S. Sivasubramanian, B. HarishKumar, "Online Credit Card Transaction Using Finger print Recognition", Dr.M. Umamaheswariet al. /International Journal ofEngineering andTechnologyVol.2 (5), 2010, 320-322.

2. P.Meenakshi, B.Vinothkumar, "Survey on credit card secured transaction using OTP", International Journal of Advanced Research in Electronics and Communication Engineering(IJARECE)Volume 4, Issue3, March2015.

3. AbhinavMuley, VivekKute, "Prospectivesolution to bank card systemusing fingerprint", in Conference Paper · January 2018.

4. Aruna R,Sudha V, ShruthiG,UshaRaniR,Sushma V, "ATM Security using Fingerprint Authentication and OTP", International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) Vol 5, Issue 5, May 2018.

5. Priyanka Mahajan, SupriyaMalekar, Anuja More , Amol Wairagade, Prof. B. Mahalakshmi, "Secured Internet Banking Using Fingerprint Authentication", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2016.

6. Ashish M. Jaiswal, MahipBartere, "ENHANCING ATM SECURITY USING FINGERPRINT AND GSM TECHNOLOGY", Ashish M. Jaiswal et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 28-32.

7. Krishna NandPandey, Md.Masoom, Supriya Kumari, Preeti Dhiman, "ATM Transaction Security Using Fingerprint/OTP" , JETIR (ISSN-2349-5162) March2015,Volume2,Issue3.

8. Bharathiraja N, Ravindhar N.V, Loganathan V, "Secure PIN Authentication for ATM Transaction using Mobile Application", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-6 Issue-2, May 2016.

9. NeenuPreetam, Harsh Gupta, "Cardless Cash Access using Biometric ATM Security System", Journal on Science Engineering & Technology Vo1ume 1, No. 04, December 2014.

10. Pramila D. Kamble, Dr.Bharti W. Gawali, "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization", International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012 ISSN 2250-3153.

11. S. Jathumithran, V. Thamilarasan, A. Piratheepan, P. Rushanthini, J. Mercy veniancya, P. Nirupa and K. Thiruthanigesan, "ENHANCING ATM SECURITY USING FINGERPRINT", ICTACT JOURNAL ON MICROELECTRONICS, JULY2018, VOLUME:04, ISSUE:02.