



Secure ATM Transactions Using Face Recognition & OTP

Pooja Surawse, Sonam Bhangre, Shreya Taru, Samruddhi Khot

Prof. Jayashree Mundada

Department of Computer Engineering,

Indira College of Engineering And Management Parandwadi, Pune, India

Abstract : We aim to avoid the ATM thievery, stealing and wrong person misuse the ATM so that we can make them to steer their life safely and securely. The proposed system is designed based on the intelligence system to make sure the ATM utilization without any hesitation delay and make the world to be a part of digitalization. Once customer place the card into the ATM system, the system continues the process and begins the face detection using the camera located near the ATM and frame a non-permanent identity database for the customer and user face authentication is performed on the ATM. Valid user will carry on with the normal process but the Invalid user cannot use the ATM card so they give the secondary password to the system automatically the another users would resumes with the transaction.

Key Words:- – Biometric, Face Recognition, OTP, Low Rank Representation, Virtual Shuffling Keypad.

I. INTRODUCTION

Due to rapid development in science and technology, upcoming creations are being built-up with strong security. But on the other hand, threats are also being posed to smash this security level. Though enhancement in automation has made a positive impact overall, but different financial institutions like banks and applications like ATM are still subjected to thefts and frauds. Due to the advancement in technologies fraudsters are finding new ways to assail and hence increasing the security. Biometric technology is a method that is the simpler to deploy and it can be used to achieve higher security levels in many fields. Biometric identifiers offer several advantages over traditional and current modes of authentication and security.

The recent ATM security authentication technique is fully dependent on pin-based verification. Factors such as emergency, reminds of pins, celerity of interaction, inadvertently pin sharing affects the system diversely. Cards with magnetic chips are easy to clone. The security and unguarded are opposite sides of the same coin, an automated machine becomes vulnerable due to weakness of its security. Automated teller machine manufactures go on strengthening and adding security features of Automated teller machine so then customer can carry out banking transactions hassle free and without any fear of siphoning of amount from their account and the same frauds works with similar speed to crack the innovated security feature so that they can have access over the Automated teller machine to exploit the accounts of bank customers.

The main Motivation of this project is to reinforce security of the conventional ATM module. We have postulate a new concept that enhances the overall experience, usability and convenience of the transaction at the ATM. Features like face recognition and One-Time Password (OTP) are used for the intensify of security of accounts and privacy of users. Face recognition technology help out the machine to recognize each and every user uniquely thus making face as a main key. This completely dispose the chances of fraud due to larceny and duplicity of the ATM cards. To Develop the ATM system where LRR algorithm will be used for face detection of the user while authenticating the genuine user of the account. System will also have the other option for login i.e. Another user.

II. EXISTING SYSTEM

The existing ATM system authenticates transactions via the card and PIN based system. Thereafter, it grants access to bank transactions. The ATM system compare the PIN entered as opposed to the stored authorization PIN for every ATM user. The need for a novel simple as well as secure method of access is thus mandatory. In the present work, PIN is generated by user and this PIN is made available to the ATM system by the means of a (SIM) Subscriber Identity Module in the user's Mobile Phone.

This PIN can be trapped by any user and can be led to fraud. If there is a match the system validate the user and grants access to all services available via ATM. If there is a mismatch the user authentication process aborts and the user is given two more lucky chance to enter the correct PIN. If the inaccurate PIN is entered the card gets blocked and retained by the ATM. Nowadays fingerprint have been performed in a few ATM system, but it can also lead to cheating. Hackers use the thieved fingerprint easily to break into the security system.

III.PROPOSED SYSTEM

In order to provide authentic security solution to the people, the concept of ATM security system based on face detection is come up. The Area of work is basically intent on Design and Implementation of Face Detection based ATM Security System using LRR algorithm. Limitations of existing system are conquered in our proposed system. In order to make any transaction, system will provide choice to process. First Self user, where in system will ask for “Detect Face” and allow to proceeding transaction if it be a match of with Image store in banks database apart from that system will decline the transaction after couple of warnings. . for Guest User, where in system will ask for “OTP” and allow to process transaction if Guest User enter the correct OTP which has been sent to authorized User.

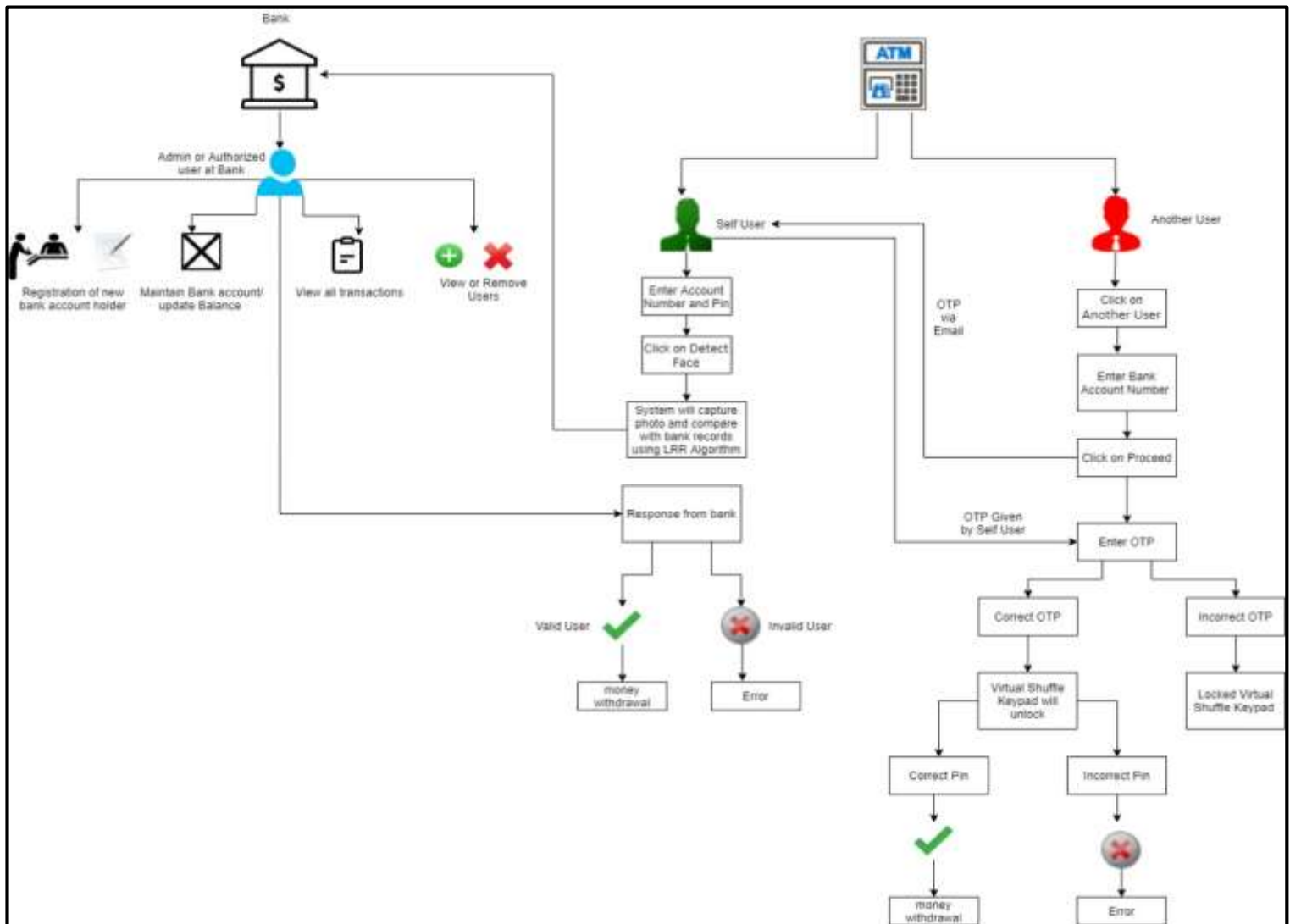


Fig.1.System Architecture

IV. MODULES

A. BANK ADMIN MODULE:-

Here in Bank Admin module, the admin can create his/her account by adding up his personal information and also his profile photo. The admin is able to view all the users of the bank. The users can make transactions i.e. deposit the amount, withdrawal of the money. Also the admin has the access to remove the users and the users are able to see their transactions easily. The user of bank has the ability to make changes in his/her existing account i.e. old phone number to new phone number, change his/her pin number, update their email id, also they have to update their profile photo after six months for better security.

B. ATM MODULE:-

Here in ATM module, there are 2 sub-modules:

I) Self User-

In Self User, there is only access for the authorized users of the bank. The self user has to be registered and he/she must have their account number and password, but for the security purpose we have added the feature like Face Recognition for reducing the frauds. So once the user enters his/her account number and password, click a live photo screen, the user's photo will be captured and for that we are using the Low Rank Representation Algorithm. Now once the image is compared with live photo and database saved photo the results will be shown. If the user is valid they will be able to do the withdrawal of money and if invalid they won't be able to do the withdrawal and will be showed as error. User can change his/her PIN if they want to.

II) Guest User-

For Guest User i.e. person sent by the self user for his/her withdrawal of money. For guest user he/she need the Account Number of this user. First when they select on another user, they have to enter self user's account number. Once proceeded there will be a OTP sent to the self user and now this OTP has to be entered correctly for the further process, so self user will give his OTP to guest user and once guest user enters it correctly, then screen will show a shuffled keypad where they have to enter self user's PIN for withdrawal of amount. Also if the OTP is incorrect the virtual shuffled keypad will be locked and it will show as error. So same will happen if the PIN is incorrect it will throw a error message.

V. ADVANTAGES

- Only authorized person can access the Account using Face Detection.
- Guest User can access the Account using OTP and Shuffle Keyboard.
- Fraud person cannot access the Account.
- Uses Shuffling keypad Algorithm which reduces the shoulder surfing attacks, recording attacks, guessing password attacks.

VI. FUTURE SCOPE

Facial recognition technique seems more challenging in comparison with biometrics, thus more efficient algorithm can be developed. The deficiency in face recognition technique like the inability to determine face when beard, aging, glasses and caps can be rectified and eliminated or reduced. If the cost of retina or iris recognition decreases, it can be used instead of face recognition.

VII. Conclusion

The project aim to utilizing of biometrics to make the ATM transaction structure increasingly dependable and secure.

The OTP and face recognition idea added to the frame further improves the security. We thus develop an ATM model that is more authentic in providing security by using facial recognition software. In this project, we have tried to proffer a solution to the much worry about issue of fraudulent transactions through Automated Teller Machine by biometrics that can be made possible only when the account holder is physically available. Thus, it cancels cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further protect when another is used at authentication level.

REFERENCES

1. S. D V, A. R, E. R. K and A. S, "Enhanced Security Feature of ATM's Through Facial Recognition," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 1252-1256, doi: 10.1109/ICICCS51141.2021.9432327.
2. Ashwini C, Shashank P, Shreya Mahesh Nayak, Siri Yadav S, Sumukh M, 2020, Cardless Multi-Banking ATM System Services using Biometrics and Face Recognition, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCCDS – 2020 (Volume 8 – Issue 13),
3. J. Chen and J. Yang, "Robust Subspace Segmentation Via Low-Rank Representation," in IEEE Transactions on Cybernetics, vol. 44, no. 8, pp. 1432-1445, Aug. 2020, doi: 10.1109/TCYB.2013.2286106.
4. S. Kumaresan, G. D. Kumar and S. Radhika, "Design of secured ATM by wireless password transfer and shuffling keypad," 2020 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1-4, doi: 10.1109/ICIIECS.2015.7192993.
5. W. Park, D. Hwang and K. Kim, "A TOTP-Based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain," 2020 UFN), 2018, pp. 817-819, 10.1109/ICUFN.2018.8436784.

6. T. K. Hazra and S. Bhattacharyya, "Image encryption by blockwise pixel shuffling using Modified Fisher Yates shuffle and pseudorandom permutations," 2020 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017, pp. 1-6, doi: 10.1109/IEMCON.2016.7746312.
7. Sudar, S. K. Arjun and L. R. Deepthi, "Time-based one-time password for Wi-Fi authentication and security," 2021 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1212-1216, doi: 10.1109/ICACCI.2017.8126007.

