Secured ATM Pin Recovery Using Fingerprint Technology and OTP Verification

Linda John[a], Rutik Gharat[b], Kunal Patere[c], Aniket Patil[d]

[a]Assistant Professor, Department of Information Technology, St. John College of Engineering and Management Palghar
[b c d] U.G. Student, Department of Information Technology, St. John College of Engineering and Management Palghar

_____

Abstract : In the existing system, user go to ATM center then user inserts an ATM card into ATM machine then enters the pin for authentication. User will get three chances to enter the right pin, if user unable to enter right pin in three attempts then user get chance to set a new pin. If the user unable to enter the right pin after three chances, the card gets block automatically and to reactivate the ATM card user will have to go to the particular bank. We have designed a system that allows users to reset ATM password at ATM center itself, by identifying fingerprint and OTP. User will get OTP on user's registered mobile number. The main objective of this technology is to avoid time consumption. As user can reactivate ATM card in ATM center itself, user can save plenty of time.

Keywords : ATM, Fingerprint, Pin, OTP.

_____

1. Introduction :

ATM stands for Automated Teller Machine. ATM machine is used to perform number of transactions. The most common uses of ATM machines are withdrawing money, checking bank balances, or changing the password [3].

We have developed the android application which can be used for resetting the ATM pin with the help of fingerprint and OTP. Our main motive is to make the good security system by with the help of fingerprint technology in the ATM machine. Biometric technology is used for authenticating the person based on his/her biology. Biometric is a technology which keeps your data extremely unique. Biometric technology is used to identify the person by using their fingerprint, face, etc.

In the existing system, user go to ATM centre then user inserts an ATM card into ATM machine then enters the pin for authentication. If the pin entered by a user is correct, user will allow for the further transaction. But if the entered pin gets wrong, then the user will get two more chances to enter the correct pin. If user enters wrong pin for all the three chances, then the card will get blocked and to unblocked the card user has to go to the bank and has to do some formalities which takes time.

2. Significance Of The Study :

ATM user can successfully reset his/her ATM pin using this application with the help of OTP verification and fingerprint technology at any place which saves the time of ATM user.

3. Hypotheses Of The Study :

This ATM security system provides a mechanism for recovery of ATM PIN by using OTP verification and fingerprint identification. If the pin entered by user is wrong then user gets an alert message. ATM user can successfully reset his/her ATM pin at any place which saves the time of ATM user.

4. Review Of Related Studies :

In this digital world, we use a number of applications for which we have to set passwords. Remembering all these passwords is a tedious task. Nowadays, all the people use ATM machines to perform a number of transactions. Our research is based on introducing Fingerprint technology in the ATM System. To overcome this issue regarding ATM systems, we propose biometric technology for ATM pin recovery. We gave more security to the current ATM Systems with the help of Biometric Authentication and OTP [1].

We are planning to use this technology to increase security aspect for all the customers for easy transaction process in the ATM center. The fingerprints are different for each human being. Out of different technologies that are used for ATM security purposes, it is observed that fingerprint technology has better performance rate than other technologies. This technology maintains a user-friendly environment with users and ATM machines. Fingerprint Technology is the most promising technology for money transactions [2].

In our proposed system, User has to give the mobile number for registration. If the user fails to enter the right pin thrice, user has to enter the OTP that is sent on the registered mobile number [4].

We can use this OTP only one time. If the OTP is correct then user gets an option to give fingerprint, system authenticate that fingerprint, if this fingerprint is valid then user gets an option to reset the ATM pin.

Biometrics is a rising security system. Biometrics data are unique is cannot be matched with any other person and cannot be lost [5].

Biometrics is a hardware used to capture the user's biometric for verification purposes. These scans match with the saved biometric data in the database to approve or deny access to the system.[3]

Nowadays ATMs are widely used because they are easy use. In this paper, electronic transaction safety is used to create resolution in ATM warrant. Here anti-theft device is applied with the help of RFID [6].

In this system if someone is trying to give fake pin the alert message will sent to the user's register mobile number. So taking actions against thief will be easy. This system totally based on the fingerprint authentication. In this paper RFID card is also used so it is easy to classify users. We Can also add face detection iris scanner for enhancing security [7].

In this paper, bio-metric features and message authentication technique is used to provide better security. To identify a customer during ATM transaction process here Pin verification is combined with fingerprint recognition. Here Fingerprint is verified using extraction algorithm [8].

There is possibility of hacking keys and password so biometric is safest technology amongst all [9].

5. Proposed System :

We have developed the android application which can be used for resetting the ATM pin by using fingerprint and OTP. The proposed ATM system provides functionality for ATM pin recovery using fingerprint identification and OTP. After three wrong attempts to reactivate the ATM card, user has to enter the OTP that is sent on the registered mobile number.[1] If the OTP is correct then user gets an option to give fingerprint, system authenticate that fingerprint, if this fingerprint is valid then user gets an option to reset the ATM pin. Once the process of password reset is complete, the user will again receive a message of successful creation of new password.

6. Objectives Of The Study :

The main objective of this system is to reactivate ATM card on mobile application using OTP and Fingerprint. User can reactivate ATM card from anywhere which save user's time.
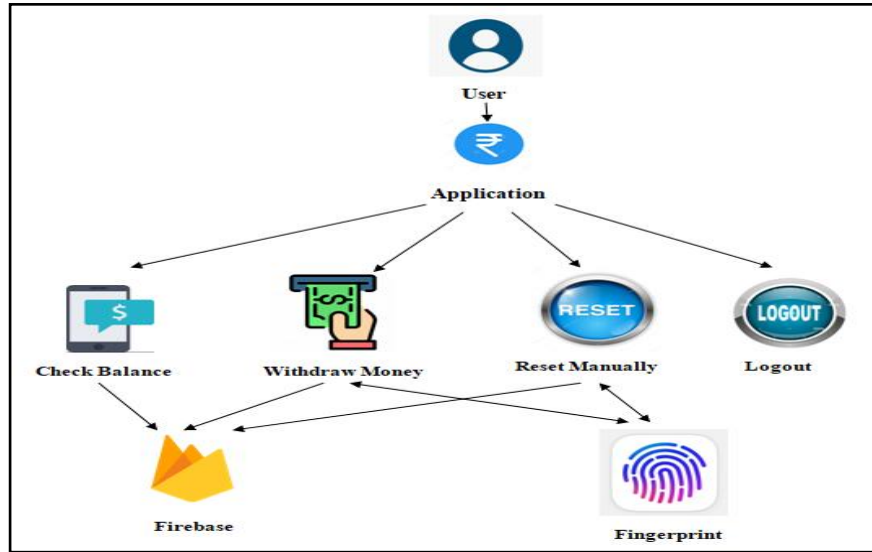
7. Methodology :
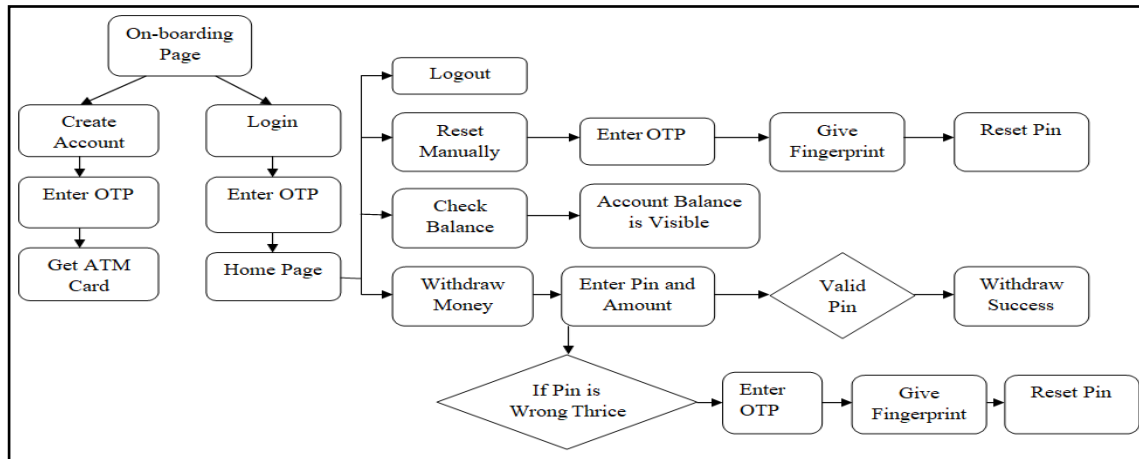

Fig. 1. Block Diagram of Proposed System

Fig. 2. Flowchart of Proposed System

User has to install an application. To create an account user have to enter the name and mobile number. After that user get an OTP on user's registered mobile number. User has to enter that OTP, if that OTP is correct then user have to give fingerprint. After all this successful steps user gets an ATM card in which user's name, ATM number, expiry date and one secret pin is mentioned. This secret pin is visible to user only once hence it is user responsibility to remember this secret pin. User has to use this pin for further transactions.

To login into the system user have to enter the registered mobile number. User will get an OTP, this OTP user can use only once, if that OTP is correct then user will redirect to home page of an application. On home page user gets three functions that are Withdraw Money, Check Balance and Logout. For withdrawal of money user have to enter the amount and transaction pin. If the entered amount and transaction pin is valid then the user gets a popup message "Withdraw Successful".

On first try if the transaction pin is invalid then user gets two more chances to enter the correct pin, if the user unable to enter the right pin after three chances, then user gets an OTP on registered mobile number. User have to enter the OTP, User can use this OTP only once. If that OTP is correct then user will have to give the fingerprint. System will authenticate that fingerprint. If the OTP and fingerprint both are authenticate successfully, then user get a chance to reset the transaction pin. After successfully resetting the pin user have to again login into the system to do the further transactions.

The second function is checking of account balance. In this user have to just click on "Check balance" button and then user get the account balance. To close the application, user has to click on logout button. After that user will successfully logout from the system.

8. Technology Used :

1. Firebase : Firebase is used to get the OTP. This OTP is sent on user's registered mobile number.

2. Mobile Fingerprint : Mobile Fingerprint is used for security purpose for resetting of ATM pin.

3. Java and XML : We have used this languages to build our project.

Procedures to implement the Biometric API Authentication :

1. First we have to provide some permission in the AndroidManifest.xml file.

2. Then we have to check if the current android device supports biometric verification or not. The user has to give app permission to access that fingerprint sensor. On that android device user has to register at least one fingerprint.

3. To reset the pin user have to provide his/her fingerprint , that time a fingerprint prompt dialog box display a message.

4. Next we have to use <u>BiometricPrompt.AuthenticationCallback</u> for authentication of various events from the users side. It comprises of three methods:

i) onAuthenticationSucceede : This callback function triggers when the fingerprint gets matched with one of registered fingerprint on that android device.

ii) onAuthenticationFailed : This callback function triggers when the fingerprint doesn't match with any of the fingerprints that are registered on the android device.

iii) onAuthenticationError : This callback function triggers when an unrecoverable error gets encountered and the authentication process has completed without success.

The different types of error codes that can occur are :

- <u>BIOMETRIC_ERROR_LOCKOUT</u> : Due to too many attempts the API gets locked.
- <u>BIOMETRIC_ERROR_LOCKOUT_PERMANENT</u> : Due to too many attempts the API gets locked permanently.
- <u>BIOMETRIC_ERROR_TIMEOUT</u> : The current request takes too much time to respond because of which timeout error occurs.
- <u>BIOMETRIC_ERROR_UNABLE_TO_PROCESS</u> : The sensor was unable to take the image of current fingerprint.
- <u>BIOMETRIC_ERROR_NO_BIOMETRICS</u> : The user does not have any biometrics registered in the device.

9. Result and Discussion :

Fig. 3. On-boarding Page

This is an On-boarding page. By using this page user can create a account and then login into the system.

Fig. 4. ATM Card

After successful registration user gets this card in which user name, account number, validity and secret pin is present. This secret pin is visible only once to the user. These pin user have to use for transaction purpose.

Fig. 5. Home page

This is home page. In this page user can see their card details. Also there are many features of application present like withdraw money, check balance and logout.

Fig. 6. OTP Page

During the transaction if user enters the wrong pin thrice then user get one OTP for resetting the transaction pin. This OTP is sent on user's registered mobile number. User have to enter that OTP.

Fig. 7. Fingerprint

User has to give his/her fingerprint for further process.

Fig. 8. Pin Reset

User has to set the new transaction pin.

10. Recommendation :

- Don't share your secrete key and OTP details.
- To use this application use a android smart phone which supports fingerprint sensor.
- Don't add others fingerprint in your personal smart phone.

11. Future Scope :

There is no technology that can store human fingerprint on server with the help of mobile fingerprint. In this case we can use fingerprint sensor model to store fingerprint on server.

In the proposed system we have not used bank database so the user have to enter the hypothetical amount during the creation of account. In this case we can collaborate with bank to over this issue.

12. Conclusion :

The proposed ATM security system enables user to recover his/her password without blocking card. This system is able to authenticate the user based on OTP verification and fingerprint identification. This system doesn't require any additional hardware device for fingerprint verification. The system can send an alert message to the owner of ATM card for entering the wrong PIN three times. User can do transaction without physical debit card because we provide virtual card to the user. The UI of our application is user friendly and easy to use.

13. Acknowledgment :

Professor Linda John, our mentor, and the entire Information Technology department are to be thanked for their continuous support and encouragement, which they gave us. It means a lot to us that they put their trust in us. Finally, we would like to thank all of our friends and family members for their encouragement and support. It was our members' commitment and excitement that pushed us ahead.

14. References :

Aditya M Ramesh , Sindhuja H , C K Vanamala. "ATM Pin Recovery based on Fingerprint Identification". International Research Journal of Engineering and Technology (IRJET) Volume: 07 Issue: 04 | Apr 2020 e-ISSN: 2395-0056 p-ISSN: 2395-0072

Sayan Hazra. "Smart ATM Service". 2019 Devices for Integrated Circuit (DevIC), 23-24 March, 2019, Kalyani, India

Prof. Venkatesh, A. Bhandage "ATM Pin Recovery based on   Fingerprint Identification".

Aruna R, Sudha V, Shruthi G, Usha Rani R, 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

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, JULY 2018, VOLUME: 04, ISSUE: 02

Jacintha V M.E(Ph.D), Jamuna Rani S, Glory Beula J, Jeba Johnsly J "An Extensive Resolution Of ATM Security Systems". 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)

Gokul.S, Kukan.S, Meenakshi.K, Vishnu Priyan S S, Rolant Gini J, M.E.Harikumar "Biometric Based Smart ATM Using RFID". Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)

Mithun Dutta*, Kangkhita Kaem Psyche, Tania Khatun, Md. Ashiqul Islam, Md. Azijul Islam "ATM Card Security Using Bio-metric and Message Authentication Technology". 2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET)

Ahmad Tasnim Siddiqui "Biometrics to Control ATM Scams: A Study". 2014 International Conference on Circuit, Power and Computing Technologies [ICCPCT]Abraham, S, Brooke R. Noriega, Ju Young Shin (2018). College students eating habits and knowledge of nutritional requirements. Journal of Nutrition and Human Health, 2(1), 13-17.