Cardless Multi-Banking ATM System Services using Biometrics and Face Recognition

Ashwini C[1], Shashank P[2], Shreya Mahesh Nayak[3], Siri Yadav S[4], Sumukh M[5]
Assistant Professor[1], BE Student[2345]
Department of Computer Science and Engineering[12345]
Global Academy of Technology[12345]
Bangalore, India[12345]

Abstract - An extortion assaulting the Automated Teller Machine (ATM) has expanded throughout the decade which has inspired the utilization of biometrics with picture for individual recognizable proof to obtain elevated level of security and precision. This project portrays a framework that replaces the ATM cards and Personal Identification Number (PIN) by the unique physiological biometric validation and facial acknowledgment. Additionally, the component of One-Time Password (OTP) gives security to the user and liberates him/her from reviewing PINs. The procedure of transaction starts by capturing and coordinating the fingerprints and facial images. The framework will consequently recognize genuine attribute and phony examples. A 6-digit OTP is created by SMS Gateway to the enlisted mobile number. After the substantial OTP is entered the user can choose among one of the multiple banks to perform bank transactions. In any sort of phony access endeavors the user will be notified.

Keywords - ATM; Biometric; Fingerprint validation; Face Recognition; PINs; OTP

I. INTRODUCTION

ATM is abbreviated as Automated Teller Machine. We can get cash whenever and at anyplace just through ATM machines. Traditional ATM Machines allow the transactions to be made through the use of PINs (Personal Identification Number) [1]. To perform safe transactions there is a need for biometric verification. Biometric Authentication is a developing and controversial field. Today biometric laws and guidelines are in process and the biometric industry standards are being tested. There are three famous assaults against ATM: Skimming, PIN logging and Integrity infringement. There are likewise assaults against cell phone: Fake versatile applications establishment, key logging programming and snatching of PIN number during transmission. Other than that, an assault may likewise be a mix of the two sorts of the said assaults [3].

Likewise, the data can be abused by a side channel assault. It is discovered that assailants attempt to get the users information that are recorded on the magnetic strip present at the back of the ATM card. Secret PINs are the main characters that can be used to confirm the ownership of the ATM card. It implies that anybody can get access to the bank records through ATM machine as the secret PIN entered is right. So, when the ATM card and passwords are lost or stolen, they can withdraw the cash from that account effectively without the issue of user verification. Hence, it can be seen that the most difficult issue brought up in ATM card security is about user validation. User confirmation is significant on the grounds that it prompts the trustworthiness and infringement of bank data. Other than that, it is emphatically accentuated that the security issues need innovative upgrades and better security arrangement as a countermeasure.

As a counter measure for these issues this project presents three degrees of security during ATM transactions. It introduces biometric verification and facial recognition measures alongside the OTP (One Time Password) generation process. The fingerprint and the facial images of the user must be scanned and verified during the login procedure [4]. An OTP will be sent to the user which confirms them as genuine. In the wake of verifying all the three factors the user will be allowed access to the ATM operations. Since the unique finger impression and facial pictures are in possession of the user always it leaves almost no degree for frauds. The OTP guarantees the freshness of the session. Thus, this project aims to improve the security of ATM exchange.

EXISTING SYSTEM

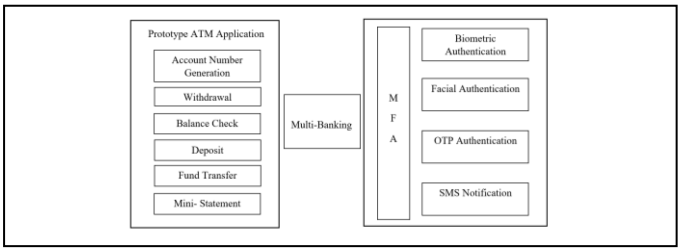
The existing ATM system authenticates transactions via the card and PIN based system. Thereafter, it grants access to bank transactions. The ATM system compares the PIN entered against the stored authorization PIN for every ATM user. If there is a match the system authenticates the user and grants access to all services available via ATM. If there is a mismatch the user authentication process fails and the user is given two more opportunities to enter the correct PIN. If the incorrect PIN is entered the card gets blocked and retained by the ATM. Nowadays fingerprint have been implemented in a few ATM system, but it can also lead to fraud. Hackers could use the stolen fingerprint easily to break into the security system.

PROPOSED SYSTEM

The proposed system is an enhancement of the existing system. It will improve the security of the ATM by applying three levels of security for authentication. The proposed system replaces the traditional card and PIN based ATM systems with biometric, face recognition and OTP authentication technologies. Since fingerprint and facial characters are unique to each individual, it can be used efficiently to replace the current ATM system. Both the fingerprint and the image of the customer will be captured and stored in the database. After successful authentication it gives all the distinct account list of the customer. To gain access to the prototype application an OTP is required which is sent by SMS gateway to the registered phone number. After successful authentication of three levels of security the Multi-Factor Application (MFA) provides access to the prototype application (ATM) to perform transactions on the accounts. In case of forgery or fraud the user will be notified by an email/SMS. This overcomes the drawbacks of the existing traditional systems with enhanced security.

System Architecture

For an application to grant an access to the end user, the user has to undergo the registration process and then the login process. To get an access to the prototype application the user has to undergo series of authentication. This series of authentication is controlled by Multi-Factor Authentication Application (MFA) as shown in the Fig. 1



System Architecture

The series of authentication are:

Biometric Authentication

The Fingerprint based authentication module will further be re-used by the MFA application as one of the steps in the multiple factors of the authentication scheme. The fingerprint-based authentication requires the user to register their biometric fingerprint data during the registration phase which has to be proved again during the login phase to get access to the system.

Facial Authentication

The Face Recognition based authentication scheme will further be re-used by the MFA application as one of the steps in the multiple factors of the authentication scheme. The Face Recognition based authentication requires the user to register his/her facial features during the registration phase which has to be provided again during the login phase to gain access to the system. Python's face-recognition API is used to capture and verify the user's facial features during the registration and the login phase respectively.

OTP Authentication

The OTP based authentication scheme will further be re-used by the MFA application as one of the steps of multiple factors of the authentication scheme. The OTP based authentication requires the user to enter 6-digit one-time passcode (OTP) received on their phone number during the login phase. This module is only applicable during the login phase. This module also provides an API to the MFA application to check if the OTP authentication is successful or not. This API will be used to grant the access to the prototype application at later stages.

Multifactor Authentication Application

This is the master application which manages all the authentication applications. This is the entry point for the end users to register their account and also to get access to the prototype application. The users will be redirected to this application from the prototype system when they try to login or register in that portal. This MFA application provides a convenient user interface to the users to perform the registration and the login operations step by step.

SMS Notification

A notification is sent to the user via SMS after a series of authentication. The user is notified upon every successful transaction. In case of fraudulent attempts to login to a genuine user’s account a notification will be sent to the user by means of multiple messages.

A. Multibanking

This is the list of all the banks that the user has registered at. The user will be allowed to choose one particular bank from the list and gains access to it.

B. Prototype ATM Application

This is the sample application developed to demonstrate how the security measures will be accomplished using the MFA application. This is the application that allows the ATM operations. The ultimate target for the users after the registration and the login process is this prototype application. When the users try to perform those operations in this portal, the portal redirects them to the MFA application which guides the users to complete the multiple phases of authentication before getting the access to the prototype.

The user can perform different ATM services like:

- Withdraw
- Deposit
- Balance Check
- Generate Account Number
- Fast Cash

II. IMPLEMENTATION

The Project is implemented in two main phases as shown in the Fig.2

- Registration Phase
- Login Phase

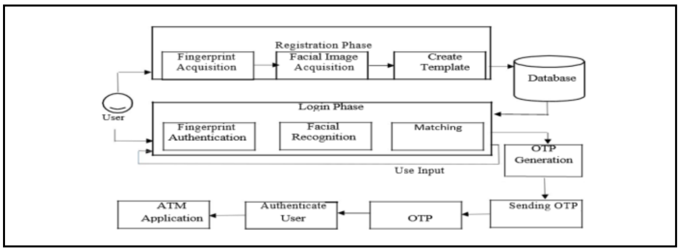


Fig. 1. Data Flow Diagram

A. Registration Phase

1) To capture the fingerprint of the user the MFS100 device with the suitable hardware drivers is used. A capture method provided by the MFS100 in-built

library is used to register the user's fingerprint to the database.

2) The user's facial image is captured and stored in the database which is implemented by the python face recognition API. It implements the built-in detect method to complete the registration process.
3) The user's personal details are acquired and stored in the database.

B. *Login Phase*

1) The fingerprint of the user is read and verified by the MFS100 built-in library. Success message is displayed upon successful verification of the user. A token is generated on completion of the fingerprint authentication process.
2) The python face recognition API implements the built-in verify method to turn on the camera and captures the image of the user. The captured image is compared to the one stored in the database. After successful verification a token is generated.
3) A 6-digit OTP will be sent to the user's registered mobile number. Upon successful verification of the OTP a token is generated.

Upon successful completion of all the various authentication processes the MFA will generate the master token. From the list of all the registered banks the user will be allowed to choose a bank which provides access to the prototype ATM application. The user can perform various ATM operations such as: Account Number Generation, Withdrawal, Balance Check, Deposit, Fast Cash and Mini-Statement.

III. CONCLUSION

The project aims at utilizing biometrics to make the ATM transaction framework increasingly dependable and secure. The OTP and face recognition idea added to the framework further improves the security and dodges the need to recall passwords. In addition, the system is implemented using JAVA which makes it easy to understand and non-intrusive. Contrasting the proposed system and the existing ATM systems, it shows that the precision and security of the proposed framework is most extreme and increasingly effective. The proposed framework gives more noteworthy level of security and comfort to the users for simple, quick and cardless ATM exchanges.

ACKNOWLEDGEMENT

I express my sincere gratitude towards my guide Prof Mrs. Ashwini C, Computer Science and Engineering Department, Global Academy of Technology for her valuable guidance. I also thank Dr. Guruprasad, HOD, Computer Science and Engineering Department Global Academy of Technology for their encouragement and support. Their insight and comments will definitely lead to a better presentation for the ideas expressed in this paper.

REFERENCES

[1] Muhammad-Bello, B.L., Alhassan M.E, Ganiyu, S.O "An Enhanced ATM Security System using Second-Level Authentication", International Journal of Computer Applications (0975 – 8887) Volume 111 – No 5, February 2015.

[2] Sowmya Ravikumar, Sandhya Vaidyanathan, Thamotharan, S.Ramakrishnan , "A New Business Model For Atm Transaction Security Using Fingerprint Recognition", International Journal of Engineering and Technology (IJET), ISSN: 0975-4024 Vol 5 No 3 Jun-Jul 2013 .

[3] V.Padmapriya, S.Prakasam, "Enhancing ATM Security using Fingerprint and GSM Technology", International Journal of Computer Applications (0975 – 8887) Volume 80 – No 16, October 2013 .

[4] Madhuri More, Sudarshan Kankal, Akshaykumar Kharat, Rupali Adhau, "Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using Human Fingerprints", International Journal of Advance Engineering and Research Development Volume 5, Issue 05, May - 2018.

[5] Apurva Taralekar, Gopalsingh Chouhan, Rutuja Tangade, Nikhilkumar Shardoor, "One Touch Multi-Banking Transaction ATM System using Biometric and GSM Authentication", 1549-8328 © 2018 IEEE.

[6] Mohsin Karovaliyaa, Saifali Karediab, Sharad Ozac, Dr.D.R.Kalbanded, "Enhanced security for ATM machine with OTP and Facial recognition features" International Conference On Advanced Computing Technologies And Applications (Icacta2015)