International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 05 | May 2021 www.irjet.net p-ISSN: 2395-0072

ENHANCED SECURITY SYSTEM FOR ATM

Ms. Vanshika Patil[1], Ms. Tejashree Mhatre[2], Ms. Srushti Karle[3]

*[*1,2,3] BE Student, Information Technology Engineering, Vidya Vikas Eductation Trust's Universal College Of Engineering, Mumbai, Maharashtra, India.*

*[4]**Prof. Yogita Mane**, Information Technology Engineering, Vidya Vikas Eductation Trust's Universal College Of Engineering, Mumbai, Maharashtra, India.*

Abstract - *The need for security has increased in the recent times due to the high level of technology we use today. The most frauds performed, are financial frauds which cause loss to many individuals or organizations worldwide. ATM (Automatic-Teller-machine) It enables a bank account holder to perform transactions i.e. specially cash withdrawal in a public space without the need of any authorized bank person. But this causes a threat to the safety of the account holder as his/her card or bank account details can be skimmed easily by the intruder which creates loopholes in the security system & these loopholes are further explored by the attacker or intruder to perform unethical actions on the users bank account. So, to overcome this we have come-up with the concept of 2-way authentication which provides or creates a 2nd layer of security to the existing system & making it difficult for any types of malicious activity.*

Key words: *ATM, 2-way Authentication, OTP, PIN, Security.*

1. INTRODUCTION

To improve the security in the current Atm system we have come up with a system which ensure 2 level authentication and in turn it will make the Atm transactions more safe and secure. In this paper the proposed system ensures 2 way authentication in which the first level is the static PIN assigned to a particular card and the second level of authentication is the OTP which is sent to the user on his/her registered mobile number when intended to do a withdrawal transaction. The OTP is dynamic in nature and it is also time-bounded hence making it safe and secure to transact without any major changes to the User Experience as well as physical Atm machine.

Motivation:

The security domain interest us because due to the technology we use today, there are many financial frauds taking place at a huge rate. Technology has mode our works easier & faster but with its drawbacks. ATM security is a major problem faced worldwide. Many People assume banks more risky than keeping the money at home or residence as banks are more likely to be robbed or hijacked. Here we saw the security domain to be to interest & worth working on. Recently there is a rise in ATM fraud cases like Card Skimming, Pin tapping, etc.

Most of the attacks are performed successfully because the PIN we use to perform transactions is static & can be traced easily by the intruder. Hence we came-up with the concept of OTP (One-time- password) which will help us provide 2- way authentication.

Problem Statement:

The need for the system 2-way authentication system arises due to the increase in the number of ATM frauds which cause financial loss to the individual and in turn to the bank or organization as well. The PIN is can be easily traced by the intruder, & ATM frauds take place.

The generation of OTP eliminates the frauds or risks like PIN tapping, hidden cameras, Card skimming and many more. Because The OTP is generated dynamically & sent to the user while performing the withdrawal transaction. So, even if the attacker has skimmed the card he/she only has the information which is present on the magnetic strip or any information on the card but the otp is different for all transactions and sent to the customer only on his/her registered phone number, hence the attacker cannot complete the transaction without the OTP and thus the attack/fraud can be stopped, avoided or eliminated.

2. LITERATURE SURVEY

Paper [1] IOT Based ATM Maintenance and Security System.

In this project, the maintenance of the ATM machine has been done by using various sensors like PIR sensor, accelerometer light sensor, smoke sensor & temperature sensor are used to give input to the system and the relay circuit used as an output device which help to ON and OFF the external devices. The Raspberry pi Microprocessor was used to control all input and output devices. All the data

given from the sensor is sent to the maintenance server by using IOT server.

Disadvantages:

- This requires many sensors and excessive hardware requirement is involved.
- Additional maintenance is maintained which causes more load onto the system.

Paper [2] ATM Security using fingerprint authentication and OTP.

In this project, with the help of Biometric Authentication & GSM technology we can overcome various ATM flaws in the current ATM system. Bankers have to collect the fingerprint of account holder as well as the nominee at the beginning process of opening the account. While doing the transaction at ATM system, first the currently provided fingerprint is verified with the registered fingerprint. If each of the fingerprints get matched, then the OTP message can be dispatched to random 10-digit number. OTP is only for one time, it will avoid various frauds related to ATM system.

Disadvantages:

- OTP is used for every transaction so it can be wasted.
- It is time consuming as it first verifies the fingerprint & then the OTP is sent to 10-digit random number.

Paper [3] ATM Security.

In this, an intuitive approach is to introduce biometric authentication technique in ATM systems, i.e., face recognition technique from 3 different angles using high resolution camera. Although various biometric technique like-fingerprint, eye recognition, retina, etc. have been devised as an authentication method for ATM machines, to minimize frauds associated with use of ATM system. ATM simulator based on face recognition from 3 different angles in order to minimize frauds associated with use of ATM system.

Disadvantages:

- The 3 different images stored in the database can vary at the time of transaction depending on the environment etc., which will not allow the customer to carry out any type of transaction.
- The 3 different image capturing and processing as well as authentication will be time consuming.

Paper [4] Enhanced security for ATM.

People can get right of entry to their financial institution account thru stability for balance inquiry, withdraw cash, switch fund etc. with the help of ATM.

It makes all these transactions paperless. To avail these facilities, the bank provides a plastic card to customers. But the plastic card has a few disadvantages. It may be lost, damaged, expired or skimmed. To overcome these disadvantages, we have proposed a new model for the card less transaction which uses BPIN and OTP for secure authentication. The BPIN is used to identify issuer institution; customer type and category of facilities are enrolled for that the transactions are cardless and paperless.

Disadvantages:

- The time required by the customers to get used to it is more.
- The BPIN is static which is provided by the bank or any financial institution.

Paper [5] Improving Atm Security via Face Recognition.

Proposed paper makes use of face reputation approach for verification in ATM system. For face recognition, there are two types of comparisons process. The first is verification, in this the system compares the given individual with who that individual says they are and gives a decision i.e. "Yes or No". The next one is identification, here the system compares the given individual to all the other individuals in the database and gives a ranked list of matches

Disadvantages:

- The time taken to process and verify the face recognition is more comparatively.
- The system has equal error rate.

3. METHODOLOGY

In our model, we have used a mechanism of two way authentication which provides more security and ensures safe transactions. It includes the use of PIN (Personal Identification Number) which is already provided by the bank and it is fixed for a specific user. Once the PIN gets verified the OTP (One Time password) is generated, which is a randomly generated unique one-time-number (4-6 digit) which is used for providing second factor authentication service which reduces the vulnerabilities of biometric information. The generated OTP cannot be used more than as its validity period is for a specific time period. After a specific time period it becomes invalid whether we use it or not. So it can be used for strong authentication purpose. The user or person than have to enter the received OTP to further carry on withdraws transaction required by him /her.

The system ensures two times more security compared to the system we are currently using and does not require any kind of physical changes to the ATM machines we use nowadays. We also have OTP features along with the traditional PIN system which will definitely does not allow

any criminal to use the ATM card for any kind of frauds as the OTP is valid only once and it is sent to the registered mobile number of the owner/customer. Thus, it becomes useless for the criminal even if he gets hold of the PIN as the OTP is varying for every transaction. For building the front-end we have used HTML and CSS and for the back-end development php is used. XAMPP is used for Apache server and MYSQL database is used for storing the data. TEXTLOCAL is used for sending messages (OTP) over the network.

OTP:
A one-time password, also known as a one-time PIN or dynamic password, is a password that is valid for only one login session or transaction.
The maximum critical gain that is addressed through OTPs is that, in comparison to static passwords, they are not liable to replay attacks. This means that a potential intruder who manage to record an OTP that was already used to login into a system to conduct any type of transaction will now no longer be able to abuse it, on the grounds that it's no longer be valid.

We are using TOTP algorithm for generation of OTP, Time-based One-time Password (TOTP) is a time-based OTP. The seed for TOTP is static, but the moving factor in a TOTP is time-based rather than counter-based. The amount of time in which each password is valid is called a time - step. As a rule, time – step tend to be 30 seconds or 60 seconds in length. If you haven't used your password within that window, it will no longer be valid, and you'll need to request a new one to gain access to your application.

4. MODELING AND ANALYSIS

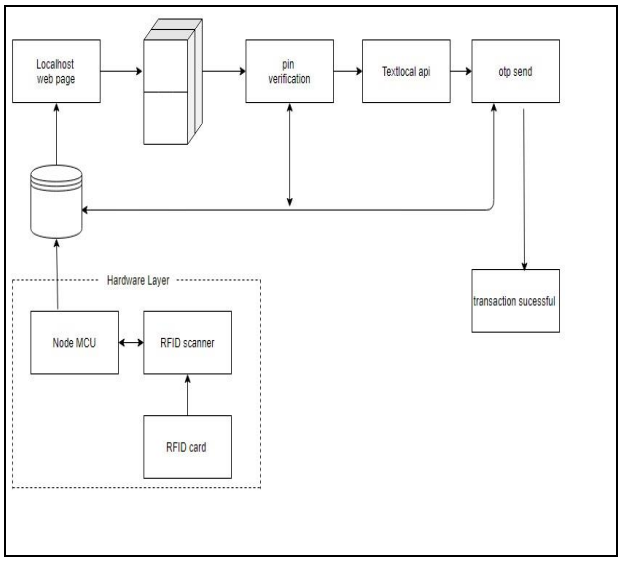

Figure 3.1: System Architecture.

System Architecture:
Hardware Layer:
This layer consists of Node MCD, RFID scanner and RFID Cards.

Node MCU: The Node MCU connects the RFID Scanner /Reader to the computer as well as the software. A System on a Chip or System on Chip (SoC) is an integrated circuit that integrates all components of a computer or other electronic system. Since Node MCU is open source platform, their hardware design is open for edit/modify /build. Node MCU Development Kit/board consist of ESP8266 Wi-Fi enabled chip. The ESP8266 is a low-cost Wi-Fi chip with TCP/IP protocol.

RFID Reader (MFRC522): It reads the data i.e. the card-id or card-number from the physical card when the card is brought close to the reader & it print's the scanned data into the card number field directly.

RFID Cards: It will act as an atm card for the proposed system. RFID is an automatic technology that helps machines or computers recognize objects, records, metadata and manage the target that has been set by an individual, with the help of radio waves is called a Radio Frequency Identification (RFID) system. A basic RFID system consists of tags. This tag is basically a microchip that is connected to an antenna, and further this antenna is attached with an object in the form of an identifier of the object. With the help of radio waves, an RFID reader and an RFID tag communicate with each other.

Database: The hardware connects to the database and inserts the data into the specified database which from which further the data is retrieved on to the webpage, automatically.

Local Host Web Page: This is the webpage created in php and hosted on the localhost. On this page the card-number is automatically retrieved, and the ATM user has to enter the static and predefined PIN into the specified input field. The system will then fetch the verification details from database on the server. Once the PIN is verified the next window opens up

Text Local API: It is the Middleware or the third-party application we are using to send our OTP message over the network. This also needs an active DLT registered.

OTP verification: It is the 2nd and the newly proposed authentication mechanism which the user has to go through successfully in order to withdraw money from the ATM.
The user has to enter the correct OTP received to him/her on the registered phone number. If the otp is correctly entered then the further "traditional" withdrawal transaction takes place. Else the transaction is terminated then and there.

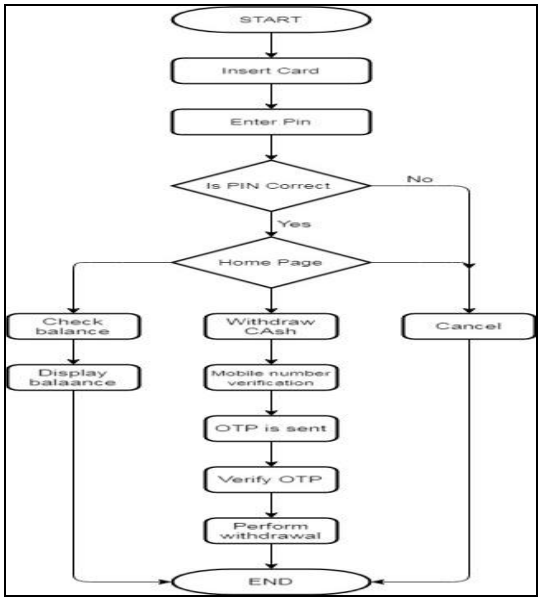

Figure 3.2: System Flow Diagram

Flow Diagram:
This diagram shows us the flow of the system and also gives information about the loops, conditions, etc. involved in the proposed system. As shown in the above figure 2 it specifies the conditions as-well-as the options through which the system will execute all the transactions involved. It involves all the processes from the start to end of the system. It is read the start to from end manner all the conditions or cases are connected to each other through arrows which point to the next. Here the 2 way authentication can be easily seen in the above flow diagram.

5. RESULTS AND DISCUSSION

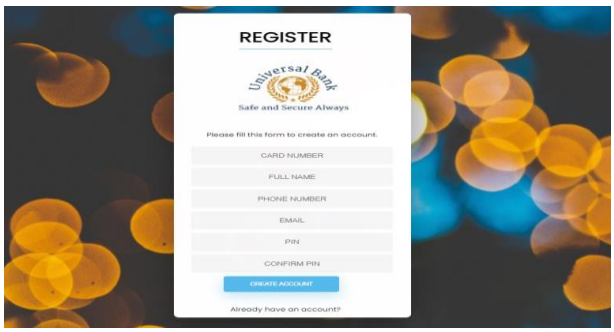

Figure 4.1: ATM Registration (For Backend use)

Registration Form: This Form is used to insert data into the database. It is used by the backend operator or bank personnel. It can be used as registration form for new debit card request etc. This form has fields like Name, Phone number, Email, PIN, etc., as seen in figure 4.1. All the fields are compulsory fill.

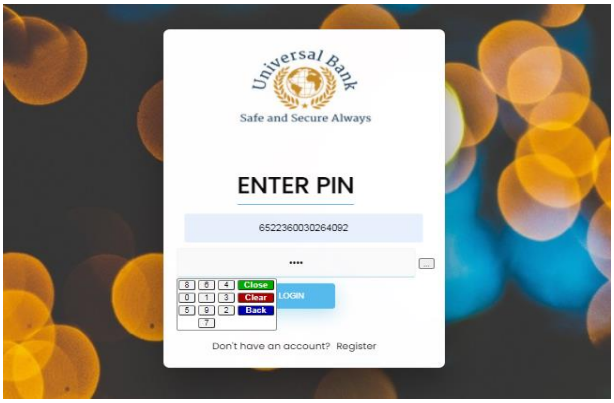

Figure 4.2: PIN Verification

Pin Verification: Here the Pin Verification is done. The card-number is automatically displayed into the card-number field when the RFID card is placed near the RFID Reader. In the PIN field the user has to enter the 4-dight PIN provided by the bank. The Pin input field has an onscreen randomized numeric keypad which will eliminate the risk of Pin tapping, etc.

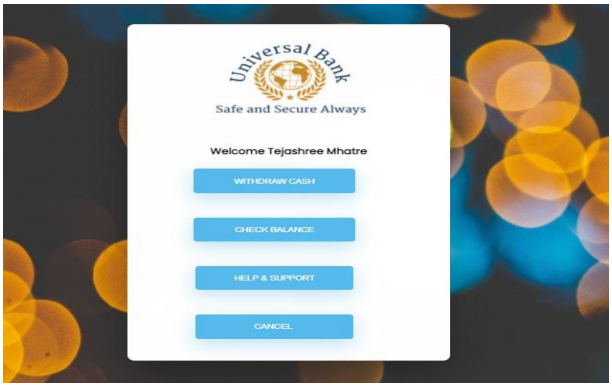

Figure 4.3: Home Page/Screen

Home Page/Screen: Once the PIN is verification is successful the Home Page opens Up which has options like, Withdraw, Check Balance, Help support & Cancel. The Cancel button terminates the transaction.

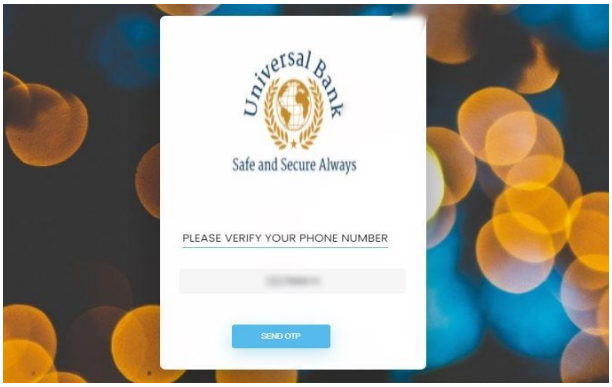

Figure 4.4: Mobile Number Verification

Mobile Number Verification: This page opens up when the withdraw option is selected. Here the users mobile number is displayed which is registered with the bank account. The user has to verify the mobile number because the OTP is sent on it respectively. Once the user clicks on SendOTP button the OTP is instantly sent to the user on his / her mobile number.

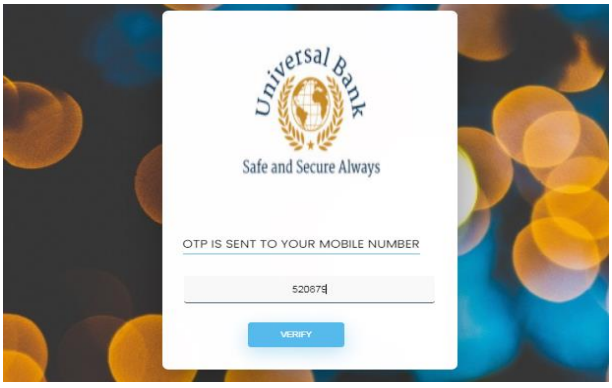

Figure 4.5: Enter OTP

Enter OTP: An OTP is sent to the user on the mobile number which was verified earlier. The user has to enter the 6-digit OTP sent to him/her. The OTP is time- based i.e. It is valid for 3 minutes after which it will expire.

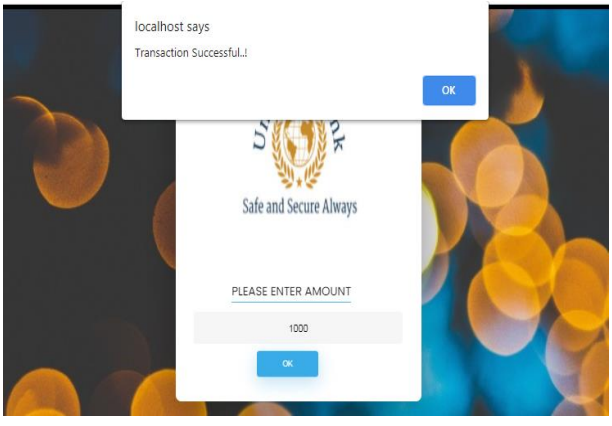

Figure 4.6: Withdraw Money

Withdraw Money: Once the correct OTP is verified the 2 way authentication process is completed and the user is prompted to enter the desired amounted which is to be withdrawn by the user.

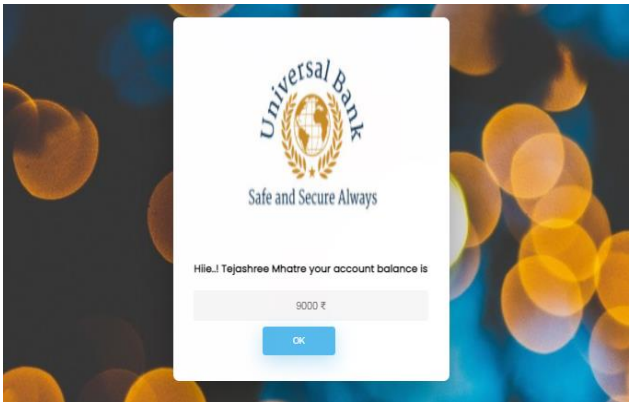

Figure 4.7: Check Balance

Check Balance: When the user clicks on the Check Balance button on the home Page the users account balance shown or displayed on the screen.

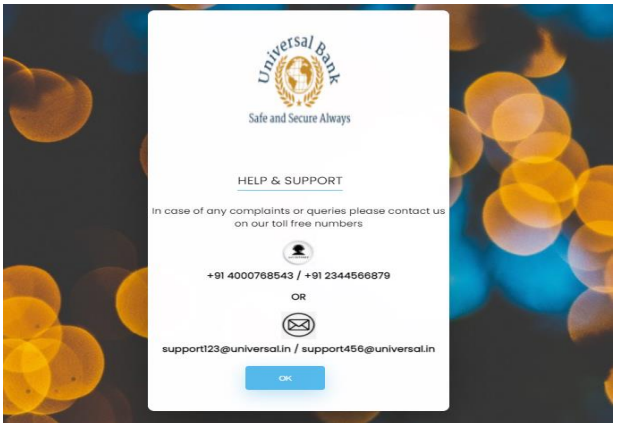

Figure 4.7: Help & Support

Help & Support: This window provides contact details of the bank. In case of any problem or transaction failure the user can contact the bank using the given details.

6. CONCLUSION

Therefore, the system ensures two-step verification and provides two- times more security compared to the system we are currently using. As well as it does not require any kind of physical additions or changes to the ATM machines we use nowadays. Hence, this paper focuses on security of

ATM system and even how to augment security for the ATM systems.

REFERENCES

[1] R. Aruna, V. Sudha, G. Shruthi, R. Usha Rani, V. Sushma, "ATM Security using Fingerprint Authentication and OTP", in International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) , Volume 5, Issue 5, May 2018.

[2] V. Prasanan, R. Sandeep Kumar, C. Deepak, R. Deepak Kummar, S. Navin Kumar, "Iot Based Atm Maintenance And Security System" in International Journal of Applied Engineering Research ISSN 0973-4562, Volume 14, Number 6, 2019 (Special Issue).

[3] Kavita Hooda, "ATM Security", in International Journal of Scientific and Research Publications, ISSN 2250-3153, Volume 6, Issue 4, April 2016.

[4] Archana et al., International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, October-2013.

[5] K John Peter, G.Gimini Sahaya Glory, G.Nagarajan, Sanjana Devi.V.V , K Sentamarai Kannan, S.Arguman, "Improving Atm Security via Face Recognition" in 978-1-4244-8679-3/11/$26.00 © IEEE, 2011.