

# ATM SECURITY SYSTEM USING FINGERPRINT AND GSM MODULE

P.PRASHANTH KUMAR REDDY, N.SHASHANK, P.SRI CHARAN REDDY, Department of Electronics & Communication Engineering, B.V.Raju Institute of Technology, Narsapur, Medak, Telangana – 502313.

Ms. P. KAVITHA REDDY, Assistant Professor, Department of Electronics & Communication Engineering, B.V.Raju Institute of Technology, Narsapur, Medak, Telangana – 502313.

## ABSTRACT

The aim of this project is that it is used for ATM access cash withdrawal with more security. We use biometric system for highly secure transaction. We use fingerprint system and One Time Password (OTP) is sent to the user registration mobile number through GSM Module system. After that, user will be able to complete the transaction securely.

We proposed a multifactor (OTP and fingerprint) based authentication security arrangements and to enhance the security and safety of ATM and its users. Automated Teller Machine (ATM)'s now a day are extensively used all over the world for the withdrawal of cash. But there is a number of disadvantages to these machines. Frauds attacking the automated teller machine has increased over the decade which has motivated us to use the biometrics for personal identification to procure high level of security and accuracy. To achieve this we are using CC3200 microcontroller to read the fingerprint which are allocated to respective customers by the banks and we have GSM modem which will send the sms updates when the transaction is done at the ATMS. This project describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint scanner. Moreover, the feature of the one-time password (OTP) imparts privacy to the users and emancipates him/her from recalling PINs. One

Time Password (OTP) is sent to the user registration mobile number through GSM Module system. After that, the user will be able to complete the transaction securely.

## 1. INTRODUCTION

Now-a-days, in the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. ATM (Automatic Teller Machine) which provide the customers with the easily accessible bank note trading is quite common. However, the financial crime cases are rising repeatedly in recent years, many criminals tamper with the ATM terminal and rob the user's credit card and password illegally. Once user's bank ATM card is lost and the password is stolen, the criminal will withdraw all the cash with in the shortest time, which will lead to enormous financial losses to customer. How to carry on the valid identity of the customer becomes the main focus in present financial circle. Traditional ATM systems authenticate basically by using the credit card and the password, this method has some defects. Using the credit card and password cannot verify the user's identity exactly. In recent years, the algorithm that the fingerprint recognition consistently updated and sending the four digit code through the controller which has offered new verification method for us, the original password authentication method joined with the

biometric identification method verify the clients' identity much better and achieve the purpose that using of the ATM machines improves the safety effectively

## OBJECTIVE

Our main objective is to create a high security ATM system where the users will be more relieved as their accounts cannot be accessed by others and can maintain secrecy which will definitely not allow any criminal to use the password for any kind of frauds

## MOTIVATION

- They considered the numerous security challenges encountered by Automated Teller Machines (ATM) and; given that the existing security in the ATM system has not been able to address these challenges, they saw the need to enhance the ATM security system to overcome these challenges.
- The financial crime case rises repeatedly in recent years; many criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer.

## 2. LITERATURE SURVEY

At present there are various techniques which are being successfully used for security of ATM Machine. An example is using CCTV camera for successfully recording the video footage of all the transactions activity in the ATM but such simple security methods weren't enough to provide much security. Thus GSM technology intervened. The information related to the attack or the threat occurring in the ATM is initially sensed and simultaneously the information is encoded and sent off to the receiver using radio frequency signals. These radio frequency signals have wide range of transmission and thus can be placed at any distance. Door is closed and thus the thief can't escape. Toxic

gas generation unit is activated at the same time, the thief becomes unconscious thus the internal activities that again occur in the ATM is prohibited. Power saving mode saves a lot of power. Alarm generation unit alerts the surrounding people about the irregular activity within the ATM. GSM provide a pathway for the delivery of the messages to 2 different people in case of holidays. The bistable can finally be only reset by the head of the bank. Thus the security features were enhanced largely for the stability and reliability of owner recognition. The method of protecting the ATM machine can be said as a method having no disadvantages. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use. [1]

The project "ATM Security Using GSM and Fingerprint with Authorized Permission for Transaction" has been successfully designed and tested. The total features of all the hardware components that are used have developed it. Presence of each module has been reasoned out and placed properly and contributing to the best working of the unit. Using highly advanced IC's with the help of improving technology, the project has been implemented successfully [2]

These days a lot of criminals tries to steal the ATM passwords or tries to tamper with the ATM bank accounts. As only one level of security is provided by the bank i.e. the ATM password only so it gets easy for the criminals to attack on the bank accounts. In this paper, a design is presented so as to enhance the security system of the ATM (Automated Teller Machine). A second level of security is provided using the fingerprint module which matches the fingerprint template with the stored template then only allows the user to proceed for the transaction and if it does not matches then after three attempts a prior generated warning SMS along with the location is sent to the enrolled user's mobile phone as well as to the nearest police station. In this way a second level of security is provided and this will reduce the number of ATM frauds. In future, this security system can be brought to the higher levels by incorporating face

recognition methodology. Also, a lot of improvements can be done so as to enhance the speed of the security system. The robustness can also be increased by improving the modules which are used in this security system. This security system will definitely reduce the frauds related to the ATM (Automated Teller Machine) [3]

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both Biometric fingerprint strategy and GSM technology. We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking. The developed application has been found promising on the account of its sensitivity to the recognition of the cardholder's finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines. [4]

This type of ATM prototype can be efficiently used with fingerprint recognition. Since, password protection is not bypassed in our system, the fingerprint recognition done after it yielded fast response and is found to be of ease for use. Fingerprint images cannot be recreated from templates; hence no one can misuse the system. LPC2148 and FIM3030 provide low power consumption platform. Speed of execution can be enhanced with the use of more sophisticated microcontroller. The security options were increased for the most part for the stability and dependableness of owner recognition. The whole system was built on the technology of embedded system that makes the system additional safe, reliable and straightforward to use. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs [5].

### 3. OVERVIEW OF THE SYSTEM

#### 3.1 EXISTING SYSTEM

In the existing system firstly the user inserts his card and the PIN number. If the PIN number is correct, then the system allows the user to perform the transactions. If the PIN is not correct then the system will again ask the user for a PIN and it allows a maximum of three times to enter the PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM.

In an event where the user fails to authenticate to the bank system, the bank card will typically be blocked and also confiscated by the ATM. If the user were to be a fraudster, confiscating the bank card would prevent the fraudster from further guessing the correct PIN and subsequently withdrawing from the card owner's account via the ATM.

However, in a situation whereby the fraudster is in possession of both the bank card and correct PIN, there is no way of preventing such withdrawals via the existing ATM machine.

#### 3.2 PROPOSED SYSTEM

The proposal is to use fingerprints in ATMs as passwords involved with the PIN number. Fingerprint recognition will make users relax by preventing unauthorized account access and assuring security. Here, a fingerprint module generates 4-digit code as a message to the customer's assigned mobile number by placing finger on it and on the basis of validation of this code, customers are allowed for further access.

### 4. SYSTEM DESIGN

#### 4.1 BLOCK DIAGRAM

##### 4.1.1 TRANSMITTER

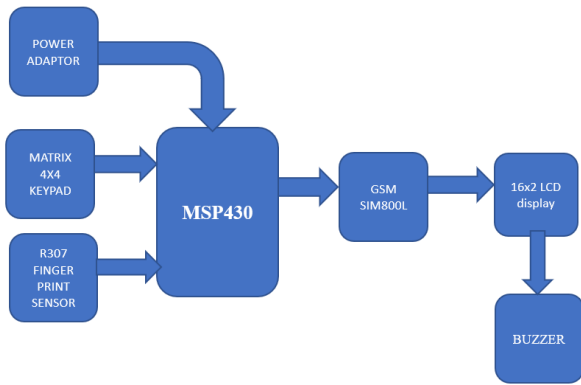


Fig 4.1.1 Transmitter Block Diagram

4.1.2 RECEIVER

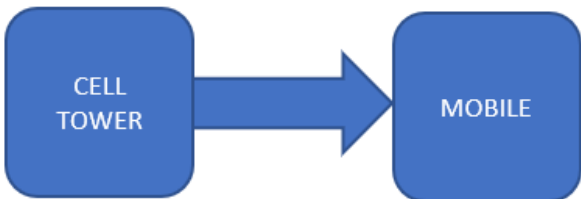


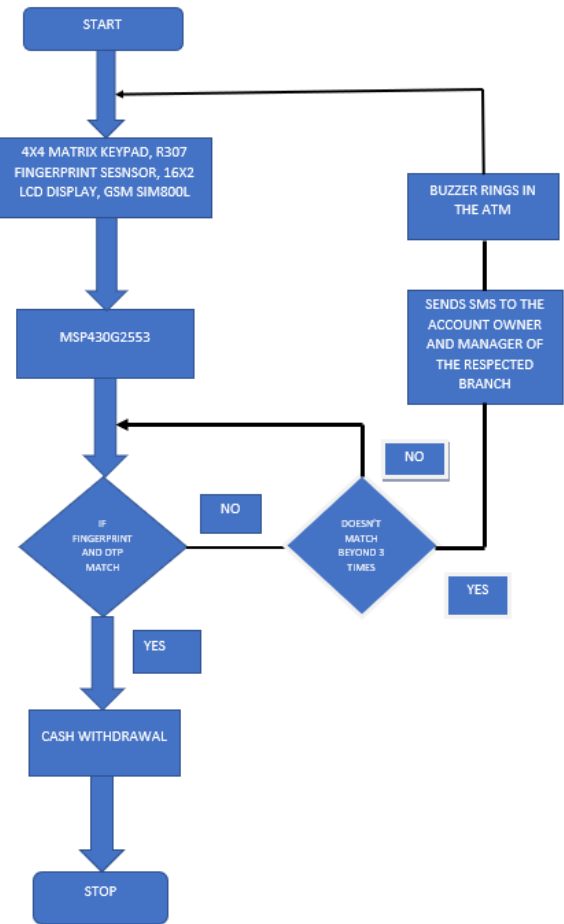
Fig 4.1.2 Receiver Block Diagram

4.2 BLOCK DIAGRAM FOR REGULATED POWER SUPPLY



Fig: 4.2 Power Supply

4.3 FLOW CHART



5. IMPLEMENTATION & RESULTS

The project is based upon providing a high security ATM system to the customers to reduce all the fraud activities. For this we use MSP430G2553 controller board and a matrix 4x4 keypad to enter the OTP in the bank ATM also we use a R307 Fingerprint sensor which senses the fingerprint which is enrolled in the Bank. We also use 16x2 LCD display which shows the details of the account and also we use a GSM SIM8001 which sends an SMS when any frauds try to enter into another bank account. We also use buzzer at the ATM which gets activated when any one try to access another account. By using these components the connections made are shown below GSM is an ultra, compact reliable wireless module. It provides 900/1800 MHz performance for voice, data, calls and Fax. We require an energia IDE to implement and test our code. The error free code is dumped into the MSP430 controller. First 9v is supplied to the circuit there a 7805voltage regulator stabilises

the voltage to constant 5v and that constant voltage is given to the splitter and that splitter splits the voltage to the keypad, fingerprint sensor, LCD display, GSM SIM800L. LM317 voltage regulator used in the GSM module as the GSM sim800l uses only 4v the LM317 compresses 9v to 4v. LM1117 voltage regulator is used near the power supply as we require only 3.3v for the msp430 microcontroller that voltage regulator compresses the 5v to the 3.3v.

The MSP430 and the sim800l communicates through the serial communication using UART pins. The boaderate for the MSP430 and SIM 800L is 9000 bits/sec. R307 Fingerprint module also communicates through serial communication using UART pins. Level shifter is used as the MSP430 output is low we require 5v input for the buzzer to activate so the level shifter shifts the low signal to the 5v which triggers the buzzer.

The bank employees enrol the fingerprints of the customer and also a nominee fingerprint details will be linked to the respective personal bank accounts. When a customer wants to withdrawal the money he enter the ATM he need to place the finger in the ATM machine then it scans the finger and when it gets matched. We also have a unique one where after verifying your finger then it asks for you to select your bank everyone uses multiple banks so you need to select which bank you want to draw the cash then OTP is sent to the number which is linked to the account. The customer enters the OTP at the ATM and if it verifies then customer can withdrawal the money from the account. But if the fingerprint or the OTP doesn't match for the 3 times then the buzzer gets activated in the ATM to alert the guard at the ATM and also a SMS is sent to the customer and the bank manager of the ATM stating fraud transaction happened in the ATM it states the ATM name and also location of the ATM is sent through SMS. If the owner of the account is unable to withdrawal the cash the nominee can access his account for the cash withdrawal. This way we can secure our bank accounts using security system using fingerprint system this reduces all the fraud activities at the ATM.

## RESULTS:

To test the project we have used our fingerprint and my nominee fingerprint is our teammate so we linked our fingerprints then we placed our finger on the scanner the it scans the finger and then verifies and then after verifying OTP was sent to mobile which was kinked and then after we enter the OTP we can proceed with the cash withdrawal option and they can draw the cash.

In another case where if another person wants to access another account then if the fingerprint doesn't match for 3 times with the bank linked then buzzer gets activated in ATM to alert the guard present at the ATM. We also have an another case when he can access the fingerprint through any means but ne enters OTP wrong then also after 3 times of wrong OTP the buzzer gets activated

If any type of fraud happens with the account then the buzzer gets activated to alert security guard initially then a SMS with stating that a fraud wants to enter into your account and also it mentions the ATM name and address and also location is also shared via SMS to the account owner and the manager of the respected bank. This way we can reduce all the illegal transactions through this security using fingerprint no one will be scared of losing money. This way we can protect our bank accounts

## 6. CONCLUSION & FUTURE SCOPE:

### 6.1 CONCLUSION:

Automatic Teller Machines have become a mature technology which provides financial services to different area and different client in all over the countries. Thus it is very important to make the process more secure and reliable. Thus by implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additional, the system also contains the original verifying methods which were inputting owner's password which is send to client. When this system is fully deployed will definitely reduce the rate of fraudulent activities on

the ATM machines such that only the registered owner of a card and nominee, access to the bank account, and the nominee user also will do the transaction so it is more comfortable in case of emergency. Thus the systems become more safe, reliable and easy to use.

Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 6, June 2015.

## 6.2 FUTURE SCOPE:

- In our proposed system we are dealing with fingerprint technique for draw the cash by getting OTP. Future scope is by iris and Face recognition for draw the cash by ATM to provide more security.
- We can enhance the system by adding retina scan, Palm scanner and other devices of biometric credential. More sensors such as temperature sensor, anti-break glass door sensor, etc. can be added to the system to ensure safety of the ATM. Use the minutia approach for avoiding the database type attacks.

## REFERENCES

1. Sudhakar Hallur<sup>1</sup>, Manjunath Bajantri<sup>2</sup>, Sagar Santaji<sup>3</sup>, ATM SECURITY USING GSM TECHNOLOGY, International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 06 | June-2018
2. T.N.S.Pallavadhar<sup>1</sup>, V.Srinivas<sup>2</sup>, ATM Security using GSM and Fingerprint with Authorized Permission for Transaction, International Journal of Emerging Engineering Research and Technology Volume 3, Issue 11, November 2015,
3. Shivam Mishra, Aakarsh Jain, Shivam Kumar, Ankit Goyal, Enhanced ATM Security System using GSM, GPS and Biometrics, International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P) Volume-7, Issue-8, August 2017
4. [1] Aruna R, [2] Sudha V, [3] Shruthi G, [4] Usha Rani R, [5], 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. Avinash Kumar Ojha, ATM Security using Fingerprint Recognition, International Journal of