

IOT TECHNOLOGY BASED NEW GENERATION SECURED ATM USING BIOMETRIC AND OTP

¹Mr. D. Anandakumar, ²K. Balamurugan, ³S. Buvanesh, ⁴A.E. Dharanesh, ⁵S. Kirubanithi

¹Assistant Professor, ^{2,3,4,5} UG Students
Department of ECE
Nandha Engineering College,
Erode 638 052, Tamil Nadu, India.

Abstract: Automated Teller Machines are extensively used currently by people. But It's hard to carry the ATM card all over, people may forget to have their ATM card or forget their PIN numbers. The ATM card may get damaged and users can have a situation where they can't get access to their money. In this proposition, Here, The Fingerprint and OTP preferred to high priority, as the combination of these two proved to be the best among the identification and verification ways. Since this project is card less and uses fingerprint and OTP for verification and transaction, there's no need for the user to carry their atm card. The primary step is to validate presently handed fingerprint with the fingerprint which is registered in the Bank's database at the time of account opening. If the two fingerprints get matched, also a message will be delivered directly to the user's mobile number which is the random 5 number pin number called as One Time Password (OTP). This OTP can be used only onetime; therefore, this avoids most problems associated with the present system. For every transaction, new OTP will be sent to account holder's mobile number, therefore there won't be fixed PIN number for every transaction. therefore, PIN number will vary during each transaction assuring security.

Keywords: IOT, Biometric, Secured ATM.

I. INTRODUCTION

Security has always been viewed upon as an outflow or afterthought by software designers. But in the case of banking and money transactions, the security should hold utmost precedence. Increase in daily attacks on ATM and banking security the designers getting on right track and putting security their important aspect in developing systems. The binary factor authentication is an approach to authentication which requires the donation of two authentication factors a knowledge factor, a possession factor. After present, each factor must be validated by the other party for authentication to happen. In present days the ATM holds only one thing to secure the money saved in the bank if we aren't considering the physical attacks. In our system we're going beyond this position of security to enhance security of the ATM. We introduce the conception of one-time password (OTP) in ATM banking. This system will give the alternate position of security using different factors to produce OTP. This will send over customer's mobile number stored in records. In secure ATM, user will have to register mobile and its IMEI number in bank system. When user puts swipes card into machine, user get request to Enter PIN (which is current way of ATM banking). In the proposed system user will use the fingerprint to get access and get OTP on mobile. The user uses his fingerprint and enters OTP to the system, he she will be having access to the machine differently no transaction can be made. In addition to the OTP for security the user will be having another option for security i.e. Biometric. Through biometric the problems can be resolved. So to enable this option the user have to register his/her biometric information at the time of opening the account or have to update the current information. At the ATM a scanner will be attached and that scanner will scan the fingerprint of the user which is compared with the database of the user.

II. EXISTING METHOD

In present days the ATM holds only one thing to secure the money saved in the bank and if user are not considering the physical attacks.

1. User enters the card to machine.
2. Card Reader reads the information on the magnetic strip on the card and sends the information to the bank server. If the card information is valid according to the bank, the ATM will ask for PIN.
3. User will enter PIN to the ATM machine.
4. If PIN entered by User is correct according to server, User will be allowed further to access for transactions.
5. This is process will only be applicable for one time, i.e. if user want to withdraw more money than user have to repeat the process again.

Advantages of using traditional system

- One can avoid a long waiting lines, filling the withdraw/ deposit forms in bank, and save time by using ATM
- as a go to option to withdraw cash, cash deposit, and check account balance.
- It's a 24X7, 365 days convenience (Though it's a non-working hour for banks, ATM serves all the time).
- It can be used anywhere in the globe.

- The use of the ATM Card is confined to only one person who's apprehensive of the PIN details of that particular card.
- Disadvantages of using traditional system
- Though there are numerous benefits of using an ATM Card in performing transactions, it does have implicit pitfalls. Then are the same
- The major disadvantage of using Card Present transaction is ATM Skimming. culprits can install unnoticeable spy cameras in the ATMs, and can steal the nonpublic details like account number, card number and PIN number, and further withdraw the money from the machine.
- An identity fraud might also occur, where the stealers steal your wallet which consists of you ATM card, and your identification cards like social security number, passport number etc., which can be used to change the PIN of the CARD.
- After performing the transaction and cash withdrawal, any robber might attack the card holder and threaten with any important weapon to snatch the money, as the ATM will be open and insulated utmost of the times, which helps the robber to enter.

III. PROPOSED METHOD

The main ideal of this project is to give additional security to the ATM system by using most trusted and easy way that's Biometric System and One Time Password (OTP).

1. When user wants to use OTP of the ATM System, the OTP should be produced at that time only with current time and user's available data in the present database system and OTP should be delivered on registered mobile of the user.
2. Though, system should get biometric If user selects biometric option on the screen. pattern information from stored database and should match the information with current examined fingerprint. Other Objective of this project is to introduce user friendly system for those people who are less familiar with newer technologies, with veritably many changes in the current system. That's fulfilled by using current technologies/ devices like Mobile, SMS, and ATM GUI etc.
3. This project demonstrates the execution of biometric and OTP for authentication rather of PIN and ATM card is encouraged. This system is powered by Arduino microcontroller, it consists of power force unit, keypad, fingerprint detector, GSM module, dc motor and driver. The GSM module, connected to the Arduino uno, sends OTP to the registered mobile number of the user and also the user will be asked to validate their fingerprint through the fingerprint scanner, and also the transaction can be done. The fingerprint of the user is stored in the database.

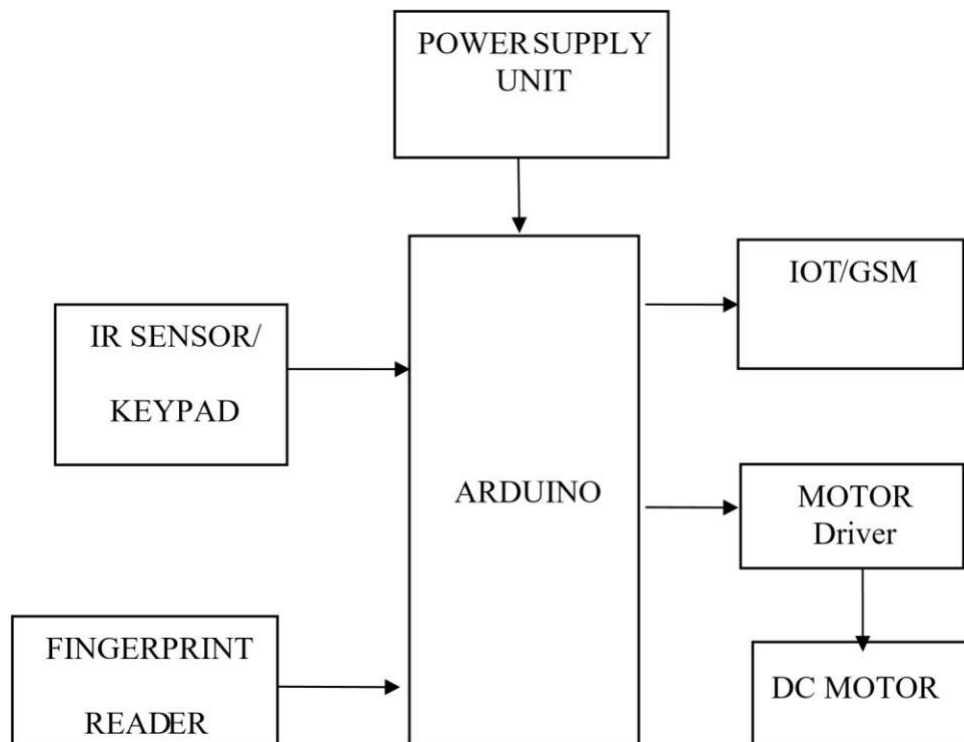


Fig 1. Block Diagram

IV. SOFTWARE DESCRIPTION 1.1 Arduino IDE

The Arduino IDE is an open- source software, which is used to write and upload code to the Arduino boards. The IDE operation is suitable for different operating systems similar as Windows, Mac OS X, and Linux. It supports the programming languages C and C++. Then, IDE stands for Integrated Development Environment. The program or code written

in the Arduino IDE is frequently called as sketching. We need to connect the Genuino and Arduino board with the IDE to upload the sketch written in the Arduino IDE software. The sketch is saved with the extension 'ino'.

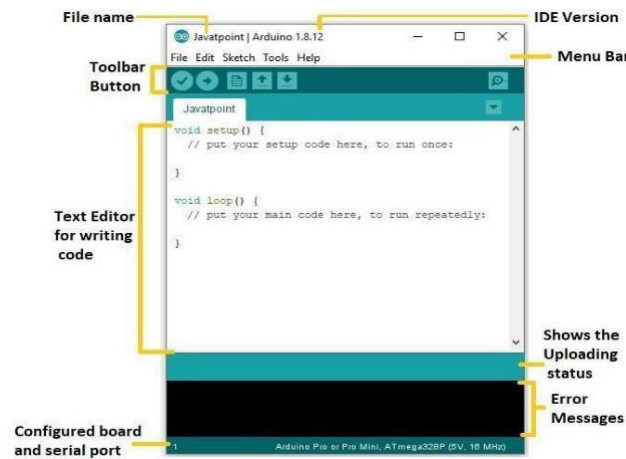


Fig 2. Arduino IDE

V. HARDWARE DESCRIPTION 5.1 Arduino UNO

The Arduino Uno is an open-source microcontroller board based on the Microchip ATmega328P microcontroller and developed by Arduino.cc and initially released in 2010. The board has 14 digital I/O pins (six capable of PWM output), 6 analog I/O pins, and is programmable with the Arduino IDE (Integrated Development Environment), via a type B USB cable. The ATmega328 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). An ATmega16U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer.



Fig 3. Arduino UNO

5.2 Fingerprint Sensor

Fingerprint sensor is the major part in the project. As fingerprint plays an important role in identification, yet face recognize Yet Face recognition is also used to identify an individual. Consider a case involving twins, Face image gets collapsed due to the same face, there fingerprint ID helps to identify the account. It is impossible for two persons to have the same fingerprint since the fingerprints are generated based on different factors. The Victorian scientist Francis Galton published a book on the forensic science of fingerprints and claimed that the chance of two people has same fingerprint is almost impossible, that the probability numbers to 1/64 million.



Fig 4. Fingerprint Sensor

5.3 Power Supply Unit

This section describes how to generate +5V DC power supply. The power supply section is the important one. It should deliver constant output regulated power supply for successful working of the project. A 0-12V/1 mA transformer is used for this purpose. The primary of this transformer is connected in to main supply through on/off switch& fuse for protecting from overload and short circuit protection. The secondary is connected to the diodes to convert 12V AC to 12V DC voltage and filtered by the capacitors, which is further regulated to +5v, by using IC 7805.

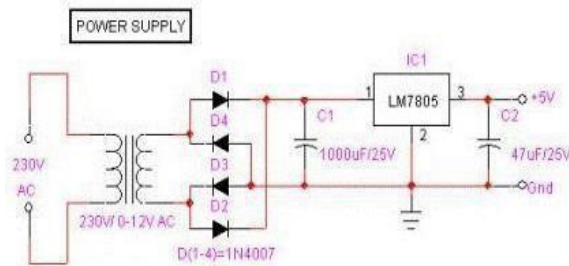


Fig 5. Power Supply Unit

5.4 SIMCOM GSM/GPRS MODEM

SIMCOM Wireless Solutions is a subsidiary of SIM Technology Group Ltd (stock code: 2000. H.K). It is a fast-growing wireless M2M company, designing and offering a variety of wireless modules based on GSM/GPRS/EDGE, WCDMA/HSDPA and TD-SCDMA technical platforms. By partnering with third parties, SIMCOM Wireless provides customized design solutions in M2M, WLL, Mobile Computing, GPS and other applications. SIMCOM Wireless also provides ODM services for customers. According to ABI Insight report, SIMCOM Cellular Module was number two provider of wireless modules worldwide in 2008 with 20% acquisition of global market share.



Fig 6.GSM Modem

VI. EXPERIMENTAL RESULT



Fig 7. Actual System Module of the Proposed method

The figure 7 represents the Actual system module for the proposed System. This system comprises a set of sensors, including a fingerprint sensor is used to verify the fingerprint of the user, GSM module is used to send OTP to the user. The information collected by the sensors is then transmitted to an Arduino board, which analyses the data and it leads to the further transaction.

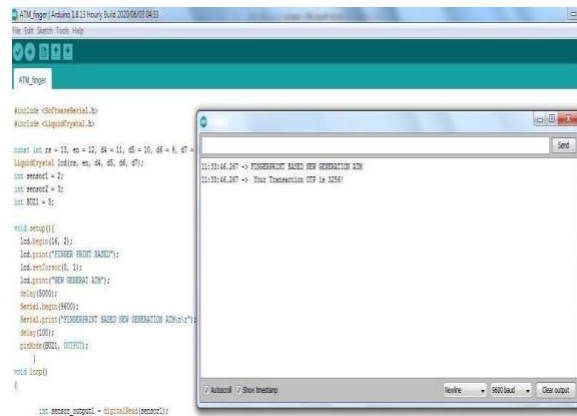


Fig 8. Arduino Interface

After the user successfully verified the fingerprint using fingerprint sensor the OTP is then send to the registered mobile number .The sent OTP can be viewed by seen by the end user. After entering the OTP the transaction can be successfully completed.



Fig 9.LCD Display of the Arduino Board

The user has to verify the fingerprint using fingerprint sensor ,the entered fingerprint will be compared and verified with the fingerprint stored in the database .After successful verification of the fingerprint the OTP will be sent to the Users mobile number.

VII. CONCLUSION

Automatic Teller Machines have become a sophisticated technology which provides financial services to different area, countries and different client all over the world. In today’s world ATM is getting less secure with arriving new ways to hack or crack ATM PIN or ATM card. Use of OTP and Biometric systems is the best and easy way to deal with these security threats friendly and non-invasively. Using this system the ATM system is secured from thief attacks. User 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 fingerprint as contained in the database. If this system when fully deployed it will undeniably reduce the rate of counterfeit activities on the ATM machines. There is a large enhancement in the security features which helps in stability and reliability of the owner’s recognition. This type of system can be used in various security systems.

REFERENCE:

1. Abdulmajeed, Alsufyani1, Alroobaea1, Ahmed, Roobaea, Detection of single-trial EEG of the neural correlates of familiar faces recognition using machine learning algorithms, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, November –
2. Aru, O.Ezeand I.Gozie, Facial Verification Technology for Use in ATM Transactions, in American Journal of Engineering Research (AJER), [Online]2020,pp.188-193.https://doi.org/10.30534/ijatcse/2020/28862020
3. H.R.Babaei, O.Molalapatana and A.A.Pandora, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKM, 3rdvol.45, November – December 2020, pp.211-216.
4. E.Derman, Y.K.Gecici and A.A.Salah, Short Term Face Recognition for Automatic TellerMachine(ATM)Users,inICECCO2019,Istanbul,Turkey,pp.111-114. https://dx.doi.org/10.21172/1.841.20

5. JinfangXu, Khan, Rasib and RasibHasan, SEPIA: Secure-PIN- authentication-as-ascriptive for ATM using Mobile and wearable devices, 3rdIEEE International Conference on Mobile Cloud Computing, Services, and Engineering IEEE, June 2019,pp. 41-50.
6. Marilou O. Espinal, Arnel C. Fajardo, Bobby D. Gerardo, RujiP. Medina, Multiple Level Information Security Using Image Steganography and Authentication, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, November – December 2019, pp.3297-3303.
7. M.Murugesan, R.Elankeerthana, Support vector machine the most fruitful algorithm for prognosticating heart disorder , International, Journal of Engineering and Technology, Volume 7, pp.48– 52, 2018.
8. M.Murugesan,S.Thilagamani, Overview Of Techniques For Face Recognition, International Journal Of Life Science and Pharma Reviews , pp.66 - 71 , 2019 , ISSN 2250 – 0480.
9. M.Murugesan, R.Elankeerthana, Pedestrian Re- Identification Using Deep Learning, International Journal Of Life Science and Pharma Reviews, pp.71 - 78 ,2019 , ISSN 2250 – 0480.
10. P.Pandiraja, N. Deepa, A Novel Data Privacy- Preserving Protocol for Multi-data Users By using genetic algorithm, Journal soft Computing Volume 23Issue 18, pp8539-8553, 2019.