CARD-LESS ATM SYSTEM.

Rushikesh Kulkarni(B.E.) , Muzammil Madki(B.E.), and Tejas Mapari(B.E.)

***Abstract*: - The current ATM system uses ATM card and PIN (Pin Identification Number) for authentication purpose. This system is susceptible to many security issues such as theft of ATM card, Lebanese loop, skimming etc. Hence in this paper we propose an embedded system that uses fingerprint authentication (not ATM cards) for accessing user account along with Pin Identification Number (PIN). In this system, Bankers will collect customer finger-prints, mobile number, e-mail and name while opening the account. If two or more persons need to access the account then fingerprints of all of them can be taken. Even multiple fingerprints of a same person are taken to make access easy. All this information is stored in bank's database. Account number and Pin Identification number are given to the user. The customer needs to validate his fingerprint first and need to enter PIN. This information is sent to server for authentication. If server validates this information then customer can access his account. This makes developed system secure rather than current system which uses only PIN for authentication.**

***Index Terms*: - ATM, card less, Fingerprint, PIN, unauthorized access**

I. INTRODUCTION

During 1960 as computers had already automated many things people started thinking that whether machines could replace tellers and bank clerks. Hence first ATM was established in New York City around 1960. The machine was able to deposit cash and a receipt of transaction was given to customer. In 1967 Barclays introduced first ever cash dispenser machine in London. First ATM that stored PIN on card was invented in United Kingdom in 1965 and modem and networked ATM was developed in Dallas, Texas, in 1968. But early ATMs were not sophisticated. Security problem soon appeared. After that ATM started developing. Today's ATM technology is such a complicated technology that it is not developed by single person instead it is mixture of many similar technologies. Today Automated Teller Machine, or ATM can transfer money from one account to another account, withdraw or deposit customers cash, can make bill payments and it can also give information about account balance. So these machines are very sophisticated and they can do almost everything that a human bank teller can do.

II. WORKING OF EXISTING ATM:

ATM which we see in many places consists of screen, ATM card slot, keypad, camera above the screen, on board vault which carries cash and counting machine. Machine is connected to main banks server why telephone network. Working of ATM can be described as follows: When ATM card is inserted into card slot the information present on the magnetic strip is read by two card readers present in the card slot. One card reader looks for special code which confirms that card is real. Second card reader grabs account number and password to check against what you entered. If authentication is successful then ATM connects with bank server through telephone network. Now user can perform bank transactions and when transaction is completed card comes out through ATM slot and user automatically logs out. Counting machine is present to count number of notes and receipt comes through printer which gives you information about transaction completed.

III. ATM FRAUDS:

In ATM, authentication is performed through ATM card given to the customer and a Pin Identification Number known to user. If this information is known then anyone can withdraw cash from customers account. There are several techniques by which criminals can get this information from user. Some techniques are mentioned below.

1) **Skimming:** This is most common type of fraud. In this information present in card is copied into duplicate card. Criminals install a skimming devise at the entry of card slot. When card is inserted information present on the card is read by the device. Small pinhole camera is fixed above the keypad to know the pin number which customer is entering. Once this information is known then duplicate cards are made and criminals can access customer's account.
2) **Lebanese loop:** In this method, fraudsters install one device in card slot because of which once card is inserted it gets locked inside and only those who have put a device in card slot to lock a card know how to draw a card. Small camera is installed on keypad to know the PIN. When customer inserts a card it gets locked inside slot because of Lebanese loop. When transaction completes machine tries to push card out but as it is locked it cannot come out. Machine shows error in such situation and cancels transaction. If user moves away from machine to make a complaint then criminal who is observing this can come and by taking out card (he knows how to take it out) he can withdraw cash from customers account.
3) **Lost Or Stolen Cards:** Many people carry ATM cards and other personnel cards in wallet. If in case ATM card is lost or it is stolen by criminal then through that your bank account can be accessed.
4) **Credit Card Not Present Transaction Fraud:** In credit card not present transaction, users do not need a credit card to make a purchase. Credit card customers can authenticate themselves by making signature which also authenticates transaction. Debit card customers authenticate themselves by providing PIN or by providing signature. To confirm this type of transaction merchant needs account number, expiry date, CVV, PIN, billing address of card holder. If this information is stolen by criminals then they can access account.

By many such techniques criminals can access your account. If biometrics is used for authentication then these frauds can be minimized. Hence we propose fingerprint authentication for ATM machine.

IV. BIOMETRICS:

Biometrics can be defined as science and technology of measuring and statistically analyzing biological data. In this technology unique features of human being such as fingerprints, face, iris image, voice etc. are captured and processed. Following are various types of biometrics:

1) Physiological technique: Include finger, hand and fingerprint.
2) Geometry technique: Include eye, retina, iris, wrist (vein).
3) Behavioural technique: Include voice, signature, typing and pointing.

Biometrics works well for authentication systems as no one can mimic biometric characteristics of others. Biometrics is used in many high precision authentication systems like airport, offices, attendance system etc. but it is not used in ATM so far.

V. DESIGN AND WORKING OF PROPOSED SYSTEM:

Block diagram:

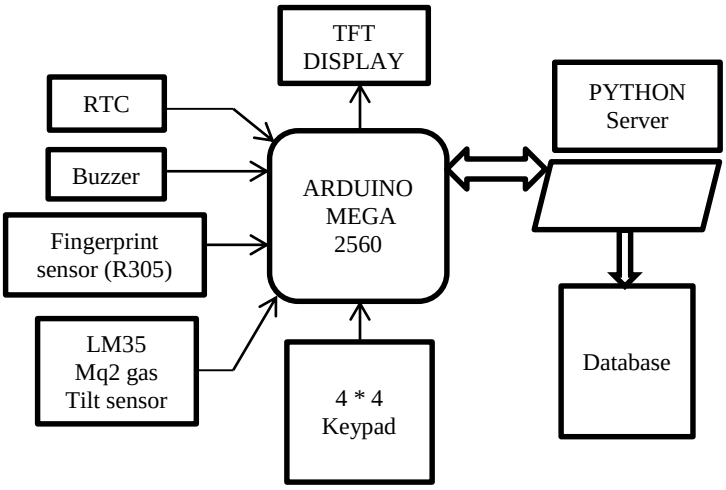

Fig1: Hardware components used in project and their dataflow indicated by arrow.

DESCRIPTION:

1) ARDUINO MAGE 2560:- This is used for controlling and processing of whole system. All sensors display and keypad are interfaced using this micro-controller. Micro-controller sends and receive information from server
2) TFT Display: - This is used for showing information on screen. It guides the user while performing transactions.
3) Keypad: - User input like password or type of transaction is taken from keypad.
4) R305 Fingerprint sensor: - This sensor is used to take fingerprint of user. It is an optical sensor which uses 5 security levels for matching fingerprints. Resolution of image created by this is 256*288 pixels. 1:N matching can be performed using this sensor.
5) Python server:- ATM machine sends data to python server through serial port. Python script processes this data verifies customer and sends response to ATM. Python is used for database management. It updates database and does required operations on database.
6) Database: SQLite3 database software maintains customer information like name, password, account number, balance etc.
7) RTC:- It is used for showing time on screen.
8) LM35 temperature sensor, MQ2 GAS sensor, tilt sensor are used for protecting ATM from physical attacks. For protecting cash present in cash cartages these sensors are used. If output from these sensors goes above threshold then buzzer is sound.

WORKING:-

This system maintains database of all ATM users at the back end which contains name, mobile number, e-mail, PIN, account balance, one unique id corresponding to a fingerprint. All this database is taken when user opens account in ATM. Fingerprints of all persons who wish to access account are taken.

When user enters welcome message is displayed on screen. Then system asks for valid fingerprint. If fingerprint is matched then user need to enter 5 digit password saved in database. Password is sent to server for verification. If both fingerprint and password are correct then user's account is accessed. When user enters into his account then transactions are displayed on the screen. User needs to choose one transaction by entering corresponding number on keypad. User can perform 4 transactions which are as follows:

1) Cash Transfer: - Transfer cash from your account to another account whose account number customer enters from keypad.
2) Cash Withdraw: - Amount entered by user through keypad is withdrawn from account and database is updated.
3) Balance enquiry: - Current balance in account is shown on screen.
4) Password change: - User can change password.

Once transaction is over user is automatically logged out from account. Screen displays message which tells user whether transaction is successful or not. If user enters wrong password more than three times then even if fingerprint is valid user automatically logs out and next time he has to authenticate fingerprint again. At any time output from sensors goes above threshold then buzzer is sound and all transactions are stopped.

Technical Details:

Database of all customers is maintained in SQLite3 database. This database is handled by Python server.

Python 2.7.8 is used for managing database. Arduino Mega 2560 controller is used at front end which collects data from all sensors and keypad. It sends PIN entered by user to server for verification. Server processes this data and sends command to controller. Communication used between controller and server is serial communication. Pyserial 2.7 software is used for connecting python with Arduino controller. Vpython software is also used for running python shell and displaying output.

Flowchart:-

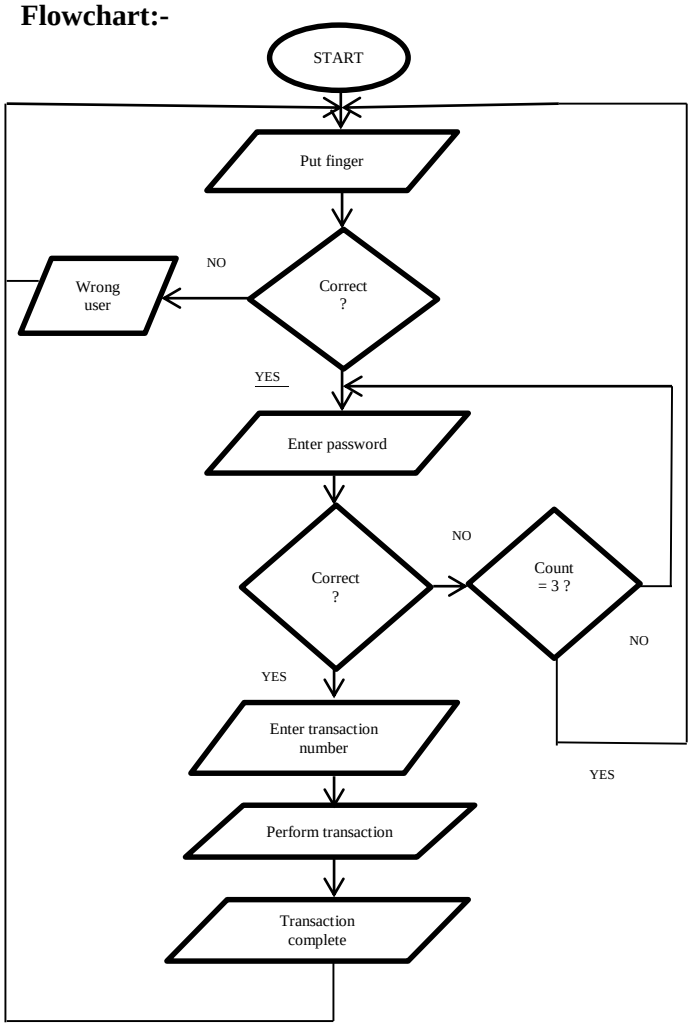

Fig2: Flowchart of whole system.

VI. WHY FINGERPRINT:-

The result of the survey conducted by the International Biometric Group (IBG) in 2012 on comparative analysis of fingerprint with other biometrics is presented in Figure. 2.

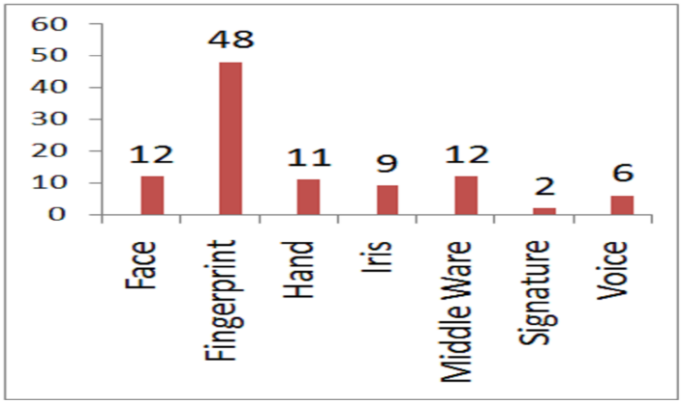

Fig.3. Comparative survey of fingerprint with other Biometrics Percentage of biometric method used on y-axis and type of biometric method on x-axis.

It shows percentage of biometric method used for identification on y-axis and different biometrics methods on x-axis. Substantial margin exists between fingerprint and other biometric methods. Fingerprints are widely used for identification.

ADVANTAGES:

1) These systems are easy to use and install.
2) Fingerprints remain same over a long period of time.
3) Unique.
4) Only 2 in 64 million people may have similar fingerprint.
5) Many image processing algorithms for fingerprint recognition are available.

VII. FUTURE SCOPE:

1) Through one ATM we can withdraw cash from account of another bank. Such interbank transactions can be implemented. For this one needs to maintain separate database of all banks and in ATM option of such all banks must be given to user. User will select one option and then all transactions from that account are performed.
2) Fingerprint image encryption can be developed and collected fingerprints can be stored in central database.
3) Similar system can be developed for online transactions instead of debit and credit card.
4) Portable cash payment machines can be developed.

VIII. SUMMARY:-

In this project we successfully interfaced fingerprint sensor with ATM and proved that biometric authentication must be used for increasing security of ATM. Taking into consideration ATM card frauds we developed a system which does not require ATM card for transaction. System is checked thoroughly by taking several fingerprints and all ATM transactions are successfully implemented. We also learnt working of current ATM system and added some sensors into ATM for physical security.

IX. CONCLUSION:-

ATM is widely used all over the world for cash withdrawal and for other bank transactions. Because of ATM card used for authentication there are some security issues related with this system. Instead the proposed embedded system uses fingerprints for authentication and hence it is highly secure. Fingerprints are unique and fingerprint detection is easy compared to other biometrics. By using proposed embedded system banks can increase security of ATM and cost of manufacturing ATM cards can be reduced. This embedded system is free from ATM card frauds such as card skimming, Lebanese loop, stolen cards and many others. If fingerprints of multiple users are stored, 1: N matching of fingerprints can be done and hence multiple persons can access account whenever required. Physical security to ATM is provided by interfacing sensors like temperature sensor, gas sensor which detects presence of hazardous gases used to cut cash cartages and steal money. Tilt sensors checks whether machine is tilted by burglars to take out cash. However issue of interbank transaction through ATM needs to be discussed in more detail as proposed system do not focus on that.

X. **REFERENCES:-**

1. Charles Bell, ”Beginning sensor networks with Arduino and Raspberry Pi”; Apress publications
2. Fingerprint Sensor R(305) Datasheet
3. Michael Roberts, “Beginning Arduino”; Technology in Action(TIA), pp259-290
4. Arduino Uno Atmega328 Datasheet.
5. Charles Severance, “Python for Informatics.”
6. http://www.toptechboy.com/using-python-with-arduino-lessons/
7. Gazal Betab, Ranjeet Kaur Sandhu ,Fingerprints in Automated Teller Machine-A Survey, International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014
8. PENNAM KRISHNAMURTHY, MR. M. MADDHUSUDHAN REDDDY, Implementation of ATM Security by Using Fingerprint recognition and GSM, International Journal of Electronics Communication and Computer Engineering, Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X
9. Mr. Mahesh A. Patil, Mr.Sachin P.Wanere , Mr.Rupesh P.Maighane, Mr.Aashay R.Tiwari, ATM Transaction Using Biometric Fingerprint Technology, International Journal of Electronics, Communication & Soft Computing Science and EngineeringISSN: 2277-9477, Volume 2, Issue 6