# Authenticated Access of ATM Cards

**Poornima D[1], Preethi Mariam Oommen P[1], Nirmala Devi K[2]**

[1]Student, [2]Associate professor

[1,2]Department of Electronics and Communication, KCG College of Technology, Chennai, India

## ABSTRACT

Due to the rise and rapid growth of E commerce the use ATM cards has drastically increased which caused an explosion in the ATM card frauds. In real life fraudulent transaction are scattered with genuine transactions Hence simple pattern matching techniques, for instance Personal Identification Number(PIN) are not enough to detect these frauds accurately. Implementation of efficient fraud detection system has become imperative to reduce people loss. Our project aims to prevent the use of ATM cards without the authorization of owner or card holder. At present the card can be accessed if the PIN is known. The amount withdrawn or transferred is notified by the card holder only after complete transaction .Hence the process can't be retrieved. But the project intimates the card owner before the transaction begins even if the PIN is known. This is limited only to card transaction and not to online mode. Hence the verification can be extended to online process.

## 1. INTRODUCTION

Day by day the usage of ATM cards has been increased in this modern world. The extent to which the card utilized properly is proportional to the misuse of cards. Since delinquent or offender is fully equipped with knowledge and well educated, illegal copies of ATM cards with magnetic strips has grown.

Consider a situation where our ATM card enclosed with PIN is lost. In such cases the amount is totally unsafe that is can be withdrawn or transferred in no time. Hence can't be retrieved easy. Yet we are in a position to give our ATM cards to our close friends, relatives though it is lawless. In those circumstances the card holder is surely unaware of the amount in process. Even the intimation from bank through Short Message Service is received only after complete transaction. Forthwith these messages are even blocked by the hackers without the knowledge of the card owner. To overcome these problems we have come up with a project which prevents the fraudulent transaction. No action such as transaction withdrawal can be done without card holder notice. Each and every action needs authentication from the possessor.

## 2. PROPOSED METHOD

To overcome the existing problem we have proposed Node-MCU based transaction process. In this process We are using RFID tag and reader. If the card gets authentication from the card holder, next process is possible or else the process is blocked. During the authentication process a pop up message displays like access granted or access denied. If the person is willing to continue the transaction process, he or she may continue by clicking allow option or else will select the block option. All the transaction process is display on LCD as well as updated on the user web page.
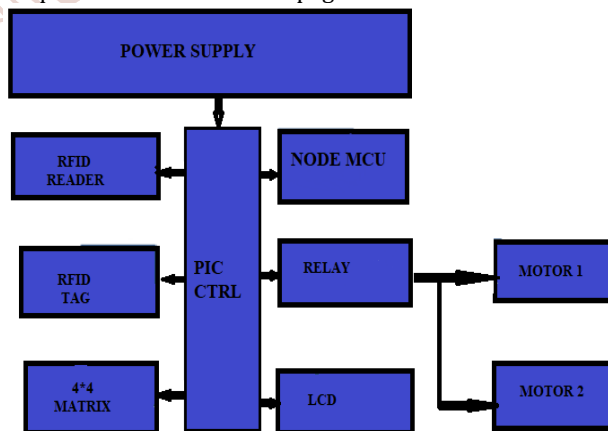


Fig1 BLOCK DIAGRAM

## 2.1 POWER SUPPLY UNIT

Power supply is a reference to a source of electrical power. A device or system that supplies electrical or other types of energy to an output load or group of loads is called a power supply unit or PSU.
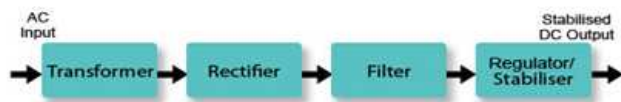
Fig 2 POWER SUPPLY UNIT

## 2.2 PIC16F877A MICROCONTROLLER

PIC microcontroller is the smallest microcontrollers that can be programmed to carry out a huge range of tasks. Every PIC microcontroller architecture consists of some registers and stack where registers function as Random Access Memory (RAM) and stack saves the return addresses. The main features of PIC microcontrollers are RAM, flash memory, Timers/Counters, EEPROM, I/O Ports, USART, CCP (Capture/Compare/PWM module), SSP, Comparator, ADC (analog to digital converter), PSP (parallel slave port), LCD and ICSP.

## 2.3 RFID

RFID signifies to tiny electronic gadgets that comprise of a small chip and an antenna. This small chip is competent of accumulating approximately 2000 bytes of data or information.

RFID devices is used as a substitute of bar code or a magnetic strip which is noticed at the back of an ATM card or credit card, it gives a unique identification code to each item. And similar to the magnetic strip or bar code, RFID devices too have to be scanned to get the details (identifying information).
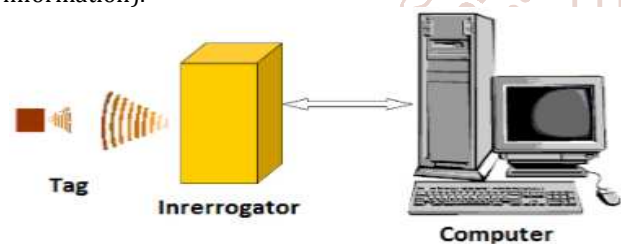


Fig 3 WORKING OF RFID

## 2.4 NODE MCU

Node MCU is an open source IoT platform. It uses the Lua scripting language. It is based on the eLua project, and built on the ESP8266 SDK 0.9.5. It uses many open source projects, such as lua-cjson, and spiffs. It includes firmware which runs on the ESP8266 Wi-Fi SoC, and hardware which is based on the ESP-12E module. Now, ESP-12E is widely applied to internet, communication in local area, intelligent home, industrial control, handed-devices, and etc.ESP-12E Dev Kit is used the design of on-board antenna and encapsulated by 2.54 direct insertion. It is very convenient to debug and install device.

## 2.5 MATRIX KEYPAD

Matrix keypad can be connected to the microcontroller by making the columns as input and the rows as output. So, in order to detect the key pressed from the keypad, the row lines have to be made low one by one and to read the columns. The status of each keys can be determined by a process called Scanning.
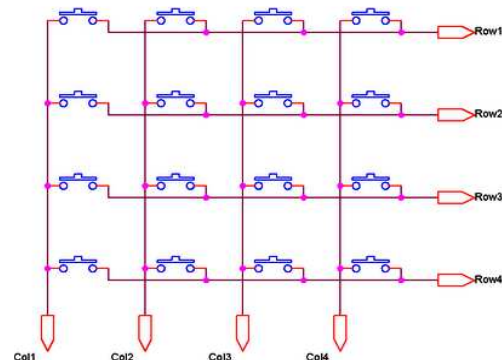


Fig 4 4*4 MATRIX

## 3. SOFTWARE USED
## 3.1 EMBEDDED C

Embedded C is a set of language extensions for the C Programming language by the C Standards committee to address commonality issues that exist between C extensions for different embedded systems. Embedded C uses most of the syntax and semantics of standard C, e.g., main() function, variable definition, datatype declaration, conditional statements (if, switch, case), loops (while, for), functions, arrays and strings, structures and union, bit operations, macros, etc.

### EMBEDDED SYSTEMS PROGRAMMING

Embedded systems programming is different from developing applications on adesktop computers. Key characteristics of an embedded system, when compared to PCs, are as follows:

➢ Embedded devices have resource constraints(limited ROM, limited RAM, limited stack space, less processing power)

➢ Two salient features of Embedded Programming are code speed and code size. Code speed is governed by the processing power, timing constraints, whereas code size governed by available program memory and use of programming language. Goal of embedded system programming is to get maximum features in minimum space and minimum time.

## 3.2 PROTUES

Proteus (PROcessor for TExt Easy to USe) is a fully functional, procedural programming language created in 1998 by Simone Zanella. Proteus incorporates many functions derived from several other languages: C, BASIC, Assembly, Clipper. It is especially versatile in dealing with strings, having hundreds of dedicated functions; this makes it one of the richest languages for text manipulation.

### SYNOPSIS AND LICENSING

The main features of this language are:
➢ fully functional, procedural language;
➢ multi-language support: Proteus is available in several languages (keyword sand messages);
➢ no data types: all variables can be used as integer numbers, floating point numbers or strings; variables are interpreted according to the functions being applied – Proteus keeps different representations of their values between calls, to decrease execution time in case of frequent conversions betwcen one type and the other;
➢ no pre-allocated structures: all data used by Proteus are dynamically allocated at execution time; there are no limits on: recursion, maximum data size, number of variables, etc.;

- no operators: Proteus is a completely functional language – there are no operators; thus, there is no ambiguity when evaluating expressions and parenthesis are not needed;
- large library of predefined functions: Proteus is not a toy-language, it comes with hundreds of library functions ready to be used for working on strings, dates, numbers, for sorting, searching and so on;

## 3.3 ARDUINO SOFTWARE (IDE)
The Arduino Integrated Development Environment or Arduino Software (IDE)contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuino hardware to upload programs and communicate with them.

## UPLOADING
Before uploading your sketch, you need to select the correct items from the Tools > Board and Tools > Port menus. Once you've selected the correct serial port and board, press the upload button in the toolbar or select the Upload item from the File menu. Current Arduino boards will reset automatically and begin the upload. With older boards (pre-Diecimila) that lack auto-reset, you'll need to press the reset button on the board just before starting the upload. On most boards, you'll see the RX and TX LEDs blink as the sketch is uploaded. The Arduino Software (IDE) will display a message when the upload is complete, or show an error. When you upload a sketch, you're using the Arduino boot loader, a small program that has been loaded on to the microcontroller on your board. It allows you to upload code without using any additional hardware. The boot loader is active for a few seconds when the board resets; then it starts whichever sketch was most recently uploaded to the microcontroller. The boot loader will blink the on-board (pin 13) LED when it starts (i.e. when the board resets).

## LIBRARIES
Libraries provide extra functionality for use in sketches, e.g. working with hardware or manipulating data. To use a library in a sketch, select it from the Sketch > Import Library menu. This will insert one or more #include statements at the top of the sketch and compile the library with your sketch. Because libraries are uploaded to the board with your sketch, they increase the amount of space it takes up. If a sketch no longer needs a library, simply delete its #include statements from the top of your code. There is a list of libraries in the reference. Some libraries are included with the Arduino software. Others can be downloaded from a variety of sources or through the Library Manager. Starting with version 1.0.5 of the IDE, you do can import a library from a zip file and use it in an open sketch. See these instructions for installing a third-party library.

## 4. FLOW OF PROCESS
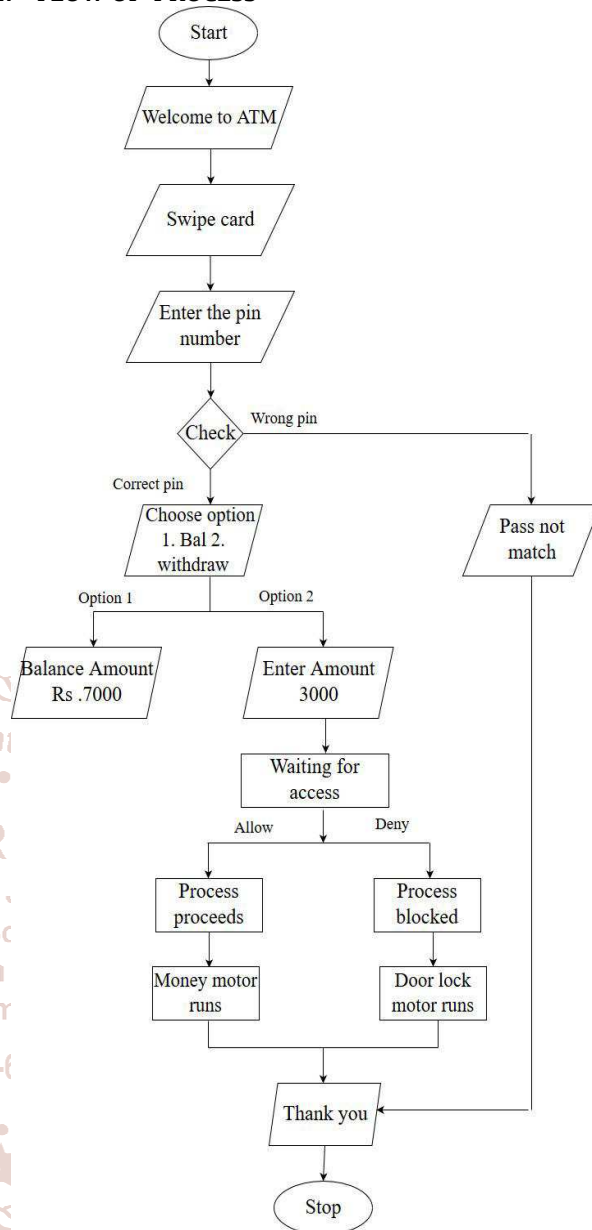


## 5. IMPLEMENTATION AND RESULTS
### SET UP
Connect the kit to a socket and on the power supply. Through the mobile, on the hotspot so that the device gets connected (hot spot name: credit card &password: password@123) to the kit. Once the connection is established between mobile hotspot and the kit, the node MCU will blink automatically. This is for identification.
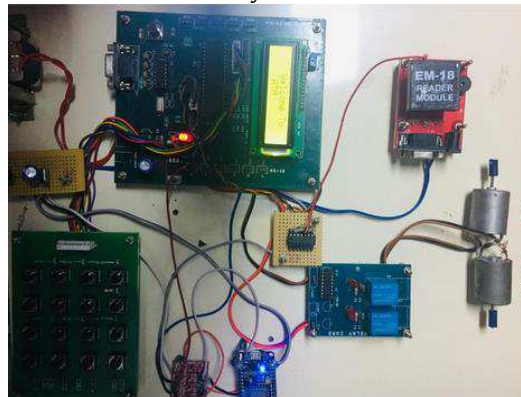


**Fig 3** COMPLETE SET OF THE PROJECT

**RESULT**
Once the kit is ready, the LCD will display "welcome to ATM" and a few seconds later "Swipe card" will be displayed.

The card with RF ID will be read and the LCD would display as "Enter password"

If the entered password is right it will proceed to next screen or else will display as "pass not match"

In this, the process has to be chosen. If option 1 is selected then the LCD willdisplay the balance amount or else will display "Enter amount".

Now the node MCU will wait for the access that is the authentication which will be through the mobile app.
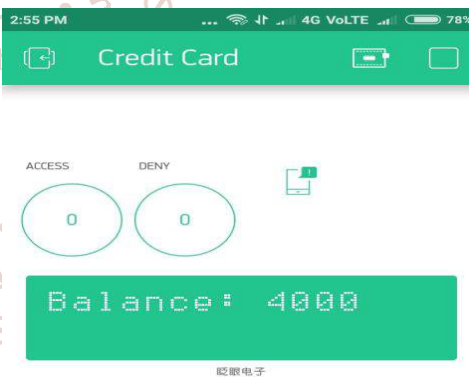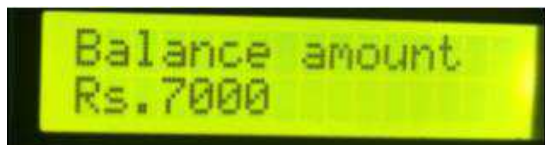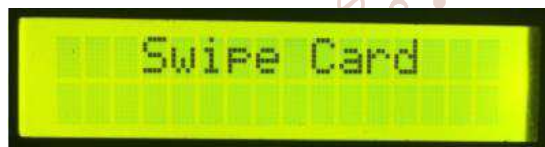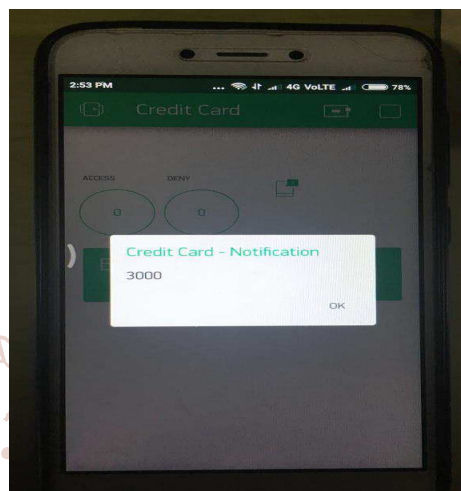
There will be two options allow and deny. The user can choose option 'allow' if he or she is aware of the transaction or else will choose 'deny' option.

Money motor will run if allow option is chosen and in the latter case door lock motor will run.

The balance amount will also be notified in the mobile app itself.
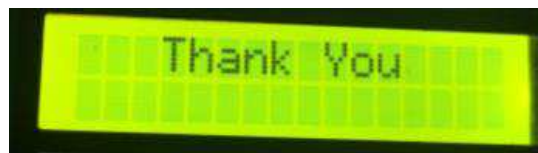




**Fig 4** LCD IMAGE DURING THE PROCESS





**Fig 5** MOBILE IMAGE DURING THE PROCESS

**Fig 6** RELAY INDICATION DURING THE ALLOW AND DENY PROCESS

## 6. CONCLUSION

The overall implementation of the outputs gives us a secured and authentic transaction achievement. The only investment is in the RFID & Node MCU system with less maintenance. This proposed system is suitable for several practical applications which are used in financial transactions for application of user identity and prevention from ATM frauds. Hence, our innovation ensures to solve the aspect of ATM security to a large extent.

## 7. FUTURE SCOPE

The future scope of the project is to extend this authentication method even in online mode that is online transaction of money. The method of authentication can use many parameters like fingerprint, face recognition.

## REFERENCES

[1] KuldeepRandhawa, Chu Kiong, ManjeevanSeera, CheePeng Lim, AsokeK.Nandi (2018) 'Credit card fraud detection using AdaBoost and majority voting', IEEE Journals.

[2] LutaoZheng, Guanjun Liu, Chungang Yan and Changjun Jiang (2018) 'Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity', IEEE Journals .

[3] Mohammad Sultan Mahmud, PhayungMeesad, SunanthaSodsee(2016)'An Evaluation of Computational Intelligence in Credit Card Fraud Detection', IEEE conference.

[4] S. Sharma, D. Shah(2016)'Analysis on Credit Card Fraud Detection Methods',IEEE conference.

[5] Wen-Fang YU, Na Wang (2017) 'Research on Credit Card Fraud Detection Model Based on Distance Sum', IEEE conference.

[6] Zahra Kazemi, HoumanZarrabi(2017)'Using deep networks for fraud detection in the credit card transaction', IEEE conference.