International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177*
*Volume 7 Issue V, May 2019- Available at www.ijraset.com*

# Implementation of Secured ATM by Wireless Password Transfer and Keypad Shuffling

Mohammad Sameer Sheikh[1], Kunal Pawar[2], Pooja Bhondave[3], Sanyogita Borade[4], Prof. K.U. Jadhav[5]
*Computer Department, Savitribai Phule Pune University*

***Abstract:** In this world of technology, atm (automatic teller machine) card is the essential part of life. To commit transaction atm pin code is compulsory and it must be secure. Use of atm is helpful for money transaction. But this system is unsafe to use because anyone can access the system. The atm pin is hack by many hackers using shoulder surfing attack. It is efficiently possible to avoid shoulder surfing attacks by keypad shuffling and wireless password transfer using arduino ide compiler. Shuffling keypad confuses the person who is standing near you.*
***Keywords:** shoulder surfing, wireless password transfer, arduino, shuffling keypad, transaction.*

## I. INTRODUCTION

Now-a-days many people can use ATM card for the transaction and other activities like shopping, paying bills etc. Carrying cash in a pocket, ATM is the best option instead. Automated Teller Machine is the automatic systems being used since 1967 by many of us. ATM was invented by John Shepherd-Barron on June 1967 at United Kingdom on June 1967. It emerged in India in 1968.

ATM is activated by inserting the card, then entering the ATM pin number of the particular card.

In today's world as the ATM has become a blessing to many but at the same time it has proved to be a curse due to many evolving hacking methods. One of the very well- known technique is Shoulder Surfing, the thief can guess the PIN by observing the movement of the shoulder. Sometimes a Spy Camera can be fitted above the keypad where you enter your pin, in this way your PIN will be known to the thief.

To avoid such problems, a technique is being implemented in which, as the users enters the ATM counter he/she can connect the ATM machines Bluetooth via their mobiles Bluetooth. After the authentication the user inside the ATM counter can enter the PIN through their mobile phones. In this way they can avoid the password guessing from the thief. The other well-known technique is keypad shuffling where after every user in ATM counter the keypad will be shuffled.

## II. TYPES OF ATM's FRAUD

According to the reports, in last few years there have been hacking into the electronic ATM systems which caused losses of billions of dollars in the global banking industry. Due tothe Cloning of cards and Hacking of PIN code the fraud occurred.
Some popular ATM frauds/attacks are explained below.

### *A. Skimming Attacks*

The most popular attack in ATM transaction is skimming attack. Lawbreakers are taking advantage of technology to make counterfeit ATM cards by using a skimmer (a card swipe device that reads the information on ATM card). When removed from the ATM, a skimmer allows the download of personal data belonging to everybody who used it to swipe an ATM card. A single skimmer can retain information from more than 200 ATM cards before being re-used.

### *B. Card Trapping*

In Card Trapping a device is placed directly over or into the ATM card reader slot. A card is physically captured by the trapping device inside the ATM in this type of attack. When the user forgot the ATM without their card, the card is taken by thieves/criminals.

### *C. ATM Malware*

Malware attacks involves an insider, such as an ATM technician who has a key to the machine, to install the malware on the ATM. Once that has been done, the attackers can insert a control card into the machine's card reader to trigger the malware and give them control of the machine through a custom interface and the ATM 's keypad. The malware allows criminals to take over the ATM to stole data, PINs and cash. The malware catches magnetic stripe data and PIN codes from the private memory space of transaction processing applications installed on a compromised ATM.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177*
*Volume 7 Issue V, May 2019- Available at www.ijraset.com*

*D. ATM Hacking*

In this hacking technique, attackers use sophisticated programming techniques to break into websites which reside on a financial institution's network. In this they can access the bank's systems to locate the ATM database and hence collect card information which can be used later to create a clone card. Hacking is also used to describe attacks against card processors and other components of the transaction processing network. Most of the ATM Hackings take place due to the use of non-secure ATM software.

## III.PROBLEM STATEMENT

"Analyse current ATM model implementation, and suggest improvements such as Keypad Shuffling technique and Wireless password transfer (Encrypted and decrypted format data) to secure the transaction process at ATM modules".

## IV.DETAILED STUDY

Security levels of ATM system are increasing day by day at various ways. Some of the authentication techniques added in password protection are as listed below.

*A. Fingerprints*

In this technique customer will require to enter his login ID and authenticate his fingerprint and both will be sent to bank server for every transaction. Transaction will be processed further after fingerprint verification.

*B. Face Recognition*

Person can be identified by his facial image. This can be done by capturing an image of the face in the visible spectrum using an optical camera. Some of benefits of facial recognition are that it is non-intrusive, hands-free and continuously accepted by most users.

*C. GSM*

Bank server will collect the customer 4-digit OTP (One Time Password) password through the GSM (Global System for Mobile Communications) after the card insertion. After validation of OTP the user moves for further processing.

*D. Voice or Speech Recognition*

The capability of a machine or program is to receive and interpret dictation to recognize and carry out spoken commands. Voice is also a physiological quality because every person has a different pitch level but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioural. The voice-based security fails many times at a person affected by fever or any vocal sound problem

## V. COMPONENT ANALYSIS

Implementation of the suggested improvements requires making modifications in the current architectural model of ATM's. Component analysis is performed in order to evaluate the pros and cons of system to be constructed.

*A. Arduino Uno*

Arduino Uno which is a CPU, does all the work via Bluetooth and Wi-Fi module. Both are connected to the board. All the code is written in the board. It has 18 input/output Pins. Of which 13 can be used as PWM output, 16-analog input, 4 UARTs. The Board is compatible with most shields designed for the Arduino Diecimila. The Arduino Uno can be power-driven through USB connection or with an external power supply. Power source is selected automatically. The Arduino Board can be programmed with Arduino Software.

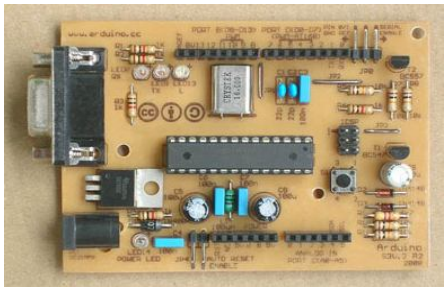


Fig.1Arduino Mega

*B. HC-05 Bluetooth Module*

Bluetooth HC-05 module having 6 pins. HC-05 module is easy to use Bluetooth SPP (Serial Port Protocol) module. It is for transparent wireless serial connection setup. It has frequency 2.4 GHz ISM band. Transfer rate is 1Mbps.Power supply requirement: +3.3V DC 50mA.

*C. 20*4 LCD Display*

LCD display is used for displaying process on to the screen. 80 characters can be printed at a time. Graphic 20*4 LCD displays are based on (monochrome) LCD technology, yet they offer interesting graphical capabilities because every pixel is individually addressable. 20×4 LCD displays so they offer good readability. They offer a selection of graphic functions, special characters and text fonts which makes the use of this kind of display extra attractive.

*D. Keypad*

The Keypad is an element that connects two points in a circuit when user press it. We connect keypad wires to the Arduino board.

## VI. WORKFLOW

*A.* Microcontroller is the core to all the processes. It initiates all the codes that are written for communication of Bluetooth Module, Wi-Fi module and LCD display which are directly connected to the Arduino Mega.

*B.* Shuffling Algorithm and OTP generation algorithm is also programmed on the mega chip.

*C.* Bluetooth module will be performing the Bluetooth pairing between ATM system and user application. After authentication generated OTP should be entered via keys.

*D.* Wi-Fi router provides Internet access to the microcontroller which enables communication with the bank database for verification of user details and writing transaction on it.

*E.* LCD display of size 20*4 is used for displaying process on the screen.

*F.* Again, the shuffled keypad is displayed on LCD. Press the corresponding keys on the keypad to enter the correct OTP. After OTP, user needs to enter the transactional password that was created at time of registration using mobile application.

## VII. METHODOLOGY

*A. Shuffling Keypad*

The random number is generated by using Fisher–Yates shuffle technique. It is one of the techniques for generating the shuffled numbers on a display. Its input bit is a linear function of its earlier state.

"In computing, random number generation technique, input bit is a linear function of its previous state." A shift register is a device whose identifying function is to shift its contents into adjacent positions within the register.

*1) Algorithm:* Fisher–Yates shuffle is an algorithm for generating a random permutation of a finite sequence (0-9).

Steps of Algorithm:

Write down the numbers from 1 through N.

Pick a random number k between one and the number of unstruck numbers remaining (inclusive).

Counting from the low end, strike out the kth number not yet struck out, and write it down at the end of a separate list.

Repeat from step 2 until all the numbers have been struck out.

The sequence of numbers written down in step 3 is now a random permutation of the original numbers.

*B. Wireless Password Transfer*

The mobile based security level is developed by creating the mobile application as Bluetooth which is used only by the ATM system. Similarly, the ATM machine has its Bluetooth which is used to exchange the data between the ATM database and user passwords. Connection establishment of Bluetooth between user and ATM system is done by the following procedure

User inserts the card into the given card slot.

System requests to switch on the Bluetooth and to display the pairing random number to pairing user and system devices. This may avoid the person who stands near user to pairing the device.

After authenticate system send 4-digit password through Bluetooth.

Transfer of password from mobile to system Bluetooth and verify it. Verify the password for further processing.

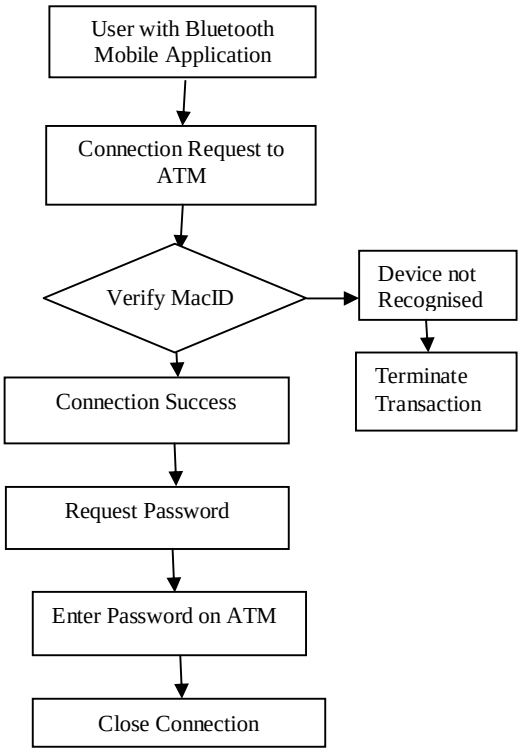
*1) Algorithm to generate OTP (One Time Password):*

Server generates the secret key

The server shares secret key with the service generating the OTP

A hash based message authentication code (HMAC) is generated using the obtained secret key and time. This is done using the cryptographic SHA-1 algorithm.
Since both the server and the device requesting the OTP, have access to time, which is obviously dynamic, it is taken as a parameter in the algorithm.
The code generated is 20 bytes long and is thus truncated to the desired length suitable for the user to enter. Here dynamic truncation is used
A counter is used to keep track of the time elapsed and generate a new code after a set interval of time
OTP generated is delivered to user by the methods described above.

*C. Flowchart for wireless password transfer*




## VIII. ADVANTAGES

*A.* Enhanced the security using keypad shuffling method and Bluetooth password transfer due to which our Password remains safe from the hacker.
*B.* Two – Way authentication is used to enhance the security. In which an additional layer of security the user must pass before being allowed to access an account.

## IX. FUTURE WORK AND CONCLUSION

This paper gives a model for the modification of existing ATM systems by virtual shuffling of keypad and wireless password communication offers an effective way of stopping PIN theft. The idea will confuse the Password guessing and password thieving in future from unauthorized person, Therefore, this is a kind of additional technique preventing pin theft in future. In future due to the advancement in hardware and software will remove its problem and make it more efficient.

## X. REFERENCES

[1] Enhancing the Security Features of Automated Teller Machines (ATMs)" A Ghanaian Perspective Nana Kwame Gyamfi Mustapha, Adamu Mohammed, February 2016.
[2] Securing ATM system with OTP and Biometric", Mohammed Hamid Khan, April 2015.
[3] "Implementation of Secure ATM by Wireless Password Transfer and Shuffling", Keypad Kumaresan S, Suresh Kumar K, Dinesh Kumar G , March 2015 - August 2015

[4] "Random Keypad and Face Recognition Authentication Mechanism" Shivani Shukla, Anjali Helonde, Sonam Raut, Shubhakirti Salode, Jitesh Zade, 2018.
[5] "The implementation of fisher yates shuffle on aljabar learning media based on hybrid application" by Iyon Maryono, Wildan Budiawan Zulfikar, and Rahayu Kariadinata.
[6] S. S. TS and A. H. Permana, Desain Handout Multimedia Menggunakan 3D Pageflip Professional untuk Media Pembelajaran pada Sistem Android, J. Penelit. Pengemb. Pendidik. Fis., vol. 2, no. 1, pp. 89– 96, Jun. (2016).

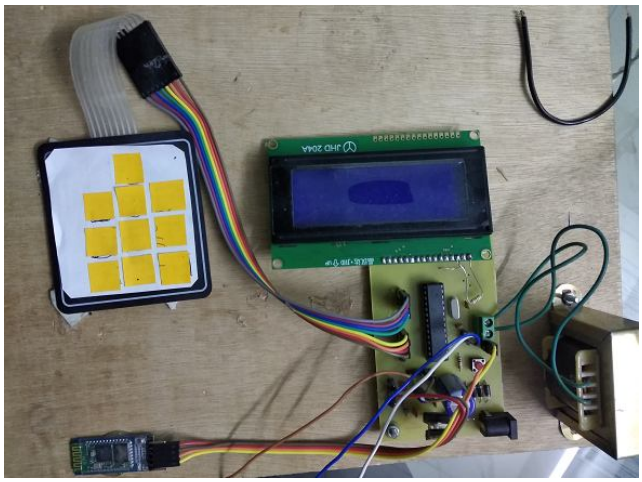


Fig 2 System