ATM Smart PIN Security System

Ms. S.DHIVYA[1], M.DEVIPRIYA[2], V.P.ARUNARAJESWARI[3], E.CHARUMATHI[4]

[1]Assistant Professor, Dept. of ECE, Sri Ramakrishna Institute of Technology, India
[2-4]UG Student, Dept. of ECE, Sri Ramakrishna Institute of Technology, India

---

Abstract - *In today's world, people are chasing towards an active and relaxing way of life, ATMs provide a convenient way for them, than to waste time in the bank for long durations. Despite the presence of CCTV cameras in ATMs, numerous thefts happen. Card cloning and ATM PIN leak are the examples of security issues, as Automated Teller Machine security concerns to protect against physical and virtual robbery. This challenge has given rise to a novel solution in the form of an Automated Teller Machine that shows scrambled text on the display, making it difficult for the person standing behind to find out the passcode. The random word generator concept will help us combat password guessing utilising the shoulder surfing approach. In this technique, the Random word generator is given a security alphabet with the passcode, and the keywords for the specified alphabetic letter are replaced for each transaction. The random word for every user changes constantly for every transaction. In addition, a GSM application is connected to an Automated Teller Machine for interaction over a wireless channel, when someone tries to use hacking skills to enter the old password, the cardholder will get a warning via SMS to the registered mobile phone number.*

***Key Words*: ATM PIN Security, Shoulder Surfing, Rand Word, GSM, Security Alphabet, ATM Card, Card Cloning,** are some of the terms used in this paper.

1. INTRODUCTION

An ATM (Automated Teller Machine) is a technology that lets account holders make money transfers without using external intervention. Customers validate their credentials in an ATM system by swiping a card reader with a chip. The magnetic card stripe holds customer data and each user has a unique PIN. Customers utilize ATMs to deposit cash and other operations such as withdrawing of cash, balance enquiries, and payment transfers to and from mobile phones. Customers swipe an ATM card into the machine, and authentication is done by entering a PIN that must match with the PIN recorded in the card's chip or in the database of the bank. ATM cards have several disadvantages, such card breakage, loss, theft, missing PINs, overlooking PINs, and so on. As a result of these worries, there is a considerable probability of cheating. The ATM framework gives clients 24 x 7 services for accomplishing transparent exchanges; yet, as ATM utilisation grows in a similar proportion, so do fraudulent intrusions on the ATM framework. When it comes to ATM machines, the primary concern is physical security, which focuses on ensuring access limitation, acknowledgment, and validation.

2. EXISTING SYSTEM

The process of withdrawing the cash in an ATM is by inserting an ATM card and then entering the security code to withdraw the cash. But when users enter into big ATMs, they have multiple ATM machines, due to this, inside the ATM there will be more than one person and there is a chance of peeking into the security PIN which is a drawback in the ATM machine technology.

Fig -1: Existing ATM Machine

3. PROPOSED SYSTEM

To overcome the existing system, an idea of the Alphabet Technique is introduced. Where a unique security alphabet is received along with the security code in the welcome kit offered by the bank during the account opening. Each time when a user accesses an ATM card, the user will be generated with various alphabetical keywords to enter security PINs to protect the account. If the hacker tries to access the account, a notification is sent to the user as a SMS in mobile.

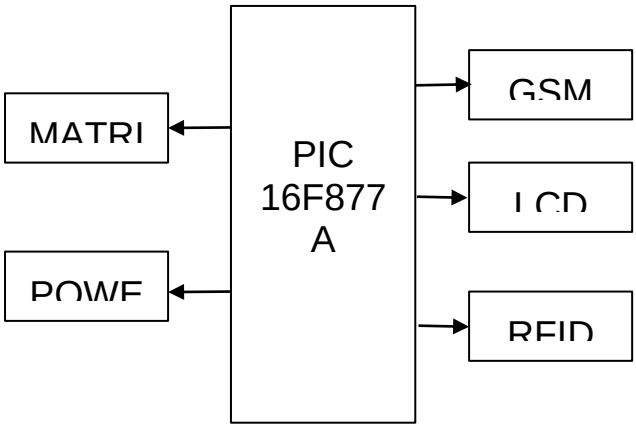

Fig -2: Block Diagram

In this model, when the user goes to the bank to withdraw the cash, these steps are followed- The user swipes the ATM card. Then the names with the different alphabet are displayed on the monitor and the user clicks the security letter. The security alphabet is the first letter of the keyword and then the security PIN is entered with a new security PIN generated. After this process, the user has to calculate the passcode by adding the count of the secured keyword to the last digit of the original security pin. If the user enters the correct password, it is navigated to enter the amount and then the balance amount is sent as an SMS to the mobile phone via the GSM module.

4. EXPERIMENTAL SETUP

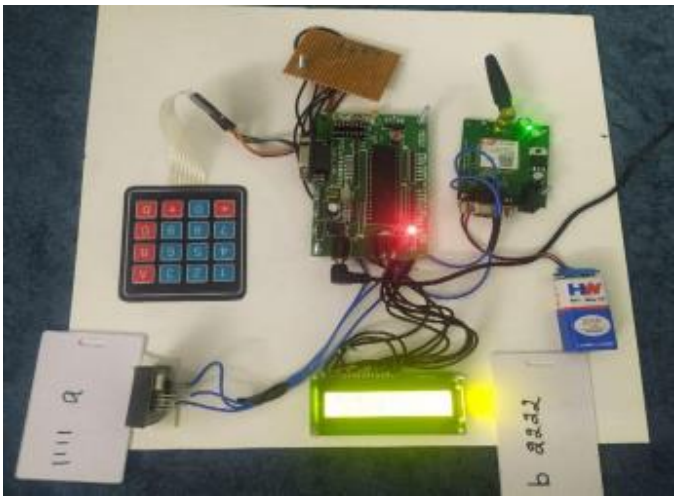

Fig -3: External Structure Model

In this model, a PIC microcontroller (Pic-16f877a) is used for controlling the entire module connected to a power supply. Here the RFID tag is used as an ATM card and RFID reader is used for scanning the tag to enter the passcode. After scanning, rand keywords are generated in the LCD as a display, then the user has to recognize the security alphabet and then count the letters of the secured alphabet keyword. Matrix Keypad is used to enter the security PIN for transaction. The ATM module is connected to GSM for wireless communication between the module and mobile phone for receiving the payment transaction messages.

5. RESULTS AND DISCUSSION

In this paper, an ATM Module is attached with GSM for wireless communication and rand words are generated for secured transactions to avoid shoulder surfing and hacking of password. In the below figure, the message of the remaining balance and unauthorized entry has been sent as a warning through GSM to the mobile phone.

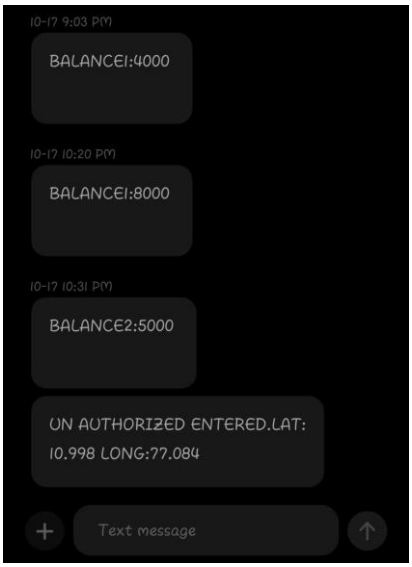

Fig -4: Balance and Alert Message

6. CONCLUSION

The progress of science and technology is a never-ending process and is always being developed. As technology progresses, we might witness a future in which humans live in any environment. The PIC16F877A based system suggested is proven to be compact, less complex and equipped for performing a wide range of tedious and repetitive tasks. Though it was created with the requirement for security in mind, it has now been expanded to include industrial and scientific uses. The proposed approach of random word generation may be used to provide overall robust security. As a result, it assists us in overcoming the major limitations of abusing highly verified security, such as a fingerprint, as well as reducing the usage of a skimmer.

REFERENCES

[1] Prashant Kumar Yadav, Akhtar Husain, Surjeet Kumar, "Enhanced ATM Security with OTP Based Authentication", International Journal of Advanced Science and Technology, 29(3), 7987 - 7993,2020.

[2] Raja, G. & Bavithra, M, "ATM Shoulder-Surfing Resistant Pin Entry Using Based Pin and Base Text.",

International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 01-05. 10.32628/CSEIT2064115,2020

[3] Raj G, Ram, "Growth and Development of ATM in India.", Asian Journal of Research in Banking and Finance. 8. 64. 10.5958/2249-7323.2018.00007.X,2018

[4] ApurvaTaralekar, GopalsinghChouhan, RutujaTangade, NikhilkumarShardoor, "One Touch Multi-Banking Transaction ATM System using Biometric and GSM Authentication", International Conference on Big Data, IoT and Data Science (BID), Vishwakarma Institute of Technology, Pune, pp.61-68, Dec 20-22,2017.

[5] Taekyoung Kwon, Sarang Na, "SteganoPIN: Two-Faced HumanMachine Interface for Practical Enforcement of PIN Entry Security", IEEE Transactions On Human Machine Systems, vol. 46, pp. 314-317, September2016

[6] Sweta Singh, Akhilesh Singh, Rakesh Kumar "A Constraint-based Biometric Scheme on ATM and Swiping Machine", In International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), pp. 45-49, September 2016.

[7] Shweta Sankhwar, "A Safeguard Against ATM Fraud", IEEE 6th International Conference on Advanced Computing, pp. 23-27, May 2016.

[8] Kavitha V, Dr.G. Umarani Srikanth," Moving ATM Applications to Smartphones with a Secured Pin-Entry Methods", IOSR Journal of Computer Engineering (IOSRJCE), Volume 17, Issue 1, pp. 58-65, Ver. II (Jan–Feb.2015).