INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 6)
Available online at: www.ijariit.com

ATM security using fingerprint and GSM module

Janhavi Rane
janhavi2326@gmail.com
Watumull Institute of Electronics Engineering and Computer Technology, Mumbai, Maharashtra

Hiten Mandaliya
hitenmandaliya562@gmail.com
Watumull Institute of Electronics Engineering and Computer Technology, Mumbai, Maharashtra

Kruti Harkhani
harkhanikruti@gmail.com
Watumull Institute of Electronics Engineering and Computer Technology, Mumbai, Maharashtra

Pooja Parmar
shreyaparmar200@gmail.com
Watumull Institute of Electronics Engineering and Computer Technology, Mumbai, Maharashtra

ABSTRACT

A wide variety of system needs reliable personal recognition system to either authorize or determine the identity of an individual demanding their services. The goal of such systems is to warrant that the rendered services are accessed only by a genuine user and no one else. In this paper, we proposed a multifactor (OTP and fingerprint) based authentication security arrangements and to enhance the security and safety of ATM and its users. Automated Teller Machine (ATM)'s now a day are extensively used all over the world for the withdrawal of cash. But there is a number of disadvantages to these machines. Frauds attacking the automated teller machine has increased over the decade which has motivated us to use the biometrics for personal identification to procure high level of security and accuracy. This project describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint scanner. Moreover, the feature of the one-time password (OTP) imparts privacy to the users and emancipates him/her from recalling PINs. One Time Password (OTP) is sent to the user registration mobile number through GSM Module system. After that, the user will be able to complete the transaction securely.

Keywords— *Fingerprint scanner, GSM module, OTP*

1. INTRODUCTION

In the modern era, the ATM system is a very essential part of our life. We know that over the past three decades, consumers have been largely depending on and trust Automatic Teller Machine, known as an ATM machine to conveniently run into their banking needs. It makes our transactions very easy which was very tedious in early time. Traditional ATM systems authenticate basically by using the debit card and the password, this method has some defects. Using the debit card and password cannot verify the user's identity exactly. A lot of criminals tamper with the ATM terminal and steal user's debit card and password by illegal means. Once the user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to the customer. How to carry on the valid identity to the customer becomes the focus in current financial circle.

In our project, we propose to add more security to the current ATM Systems. By using Biometric Authentication and GSM technology, we can overcome many of the flaws introduced by our current ATM system such as shoulder surfing, use of skimming device, etc.

The idea of using fingerprint and OTP in ATMs as a password instead of the traditional pin number is that the users will be more relieved as their accounts cannot be accessed by others and can maintain secrecy. We also have OTP feature along with the fingerprint authentication which will definitely not allow any criminal to use the password for any kind of frauds as the OTP is valid only once. Thus, it becomes useless for the next time even if any criminal gets hold of it.

2. EXISTING SYSTEM

An ATM is used by people for making transactions. The transaction can be cash deposits and withdrawal, transferring money, balance enquiry and many more. To use an Automatic Teller Machine (ATM), a plastic smart card is provided by the bank to the cardholder. This smart card contains a magnetic black stripe on the back of it which contains the specific information (unique card number and some other information) of the user. Along with the smart card, a PIN code is also provided to the cardholder by the bank to access the account. A PIN is a 4- digit number which is generated by the bank. Each cardholder has a unique PIN code. The PIN can easily be remembered by the user and if needed, it can also be changed by the cardholder. The PINs are 4 digit numbers and have a range from 0000-9999 resulting in 10000 possible numbers. The customer is identified by inserting a plastic ATM card and entering a personal identification number (PIN) for the customer. ATM allows customers to access their bank accounts and enable them to deposit and withdrawal processes as well as check their

account balances and enable them to use their mobile phones to buy prepaid credit. Also, an automatic teller machine allows a bank customer to conduct their banking transactions from almost every other ATM machine in the world. The number of entering the password is restricted to 3 only. In the existing system firstly the user inserts his card and the PIN number. If the PIN number is correct, then the system allows the user to perform the transactions. If the PIN is not correct then the system will again ask the user for a PIN and it allows a maximum of three times to enter the PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM. In an event where the user fails to authenticate to the bank system, the bank card will typically be blocked and also confiscated by the ATM. If the user were to be a fraudster, confiscating the bank card would prevent the fraudster from further guessing the correct PIN and subsequently withdrawing from the card owner's account via the ATM. However, in a situation whereby the fraudster is in possession of both the bank card and correct PIN, there is no way of preventing such withdrawals via the existing ATM machine.

3. PROPOSED SYSTEM

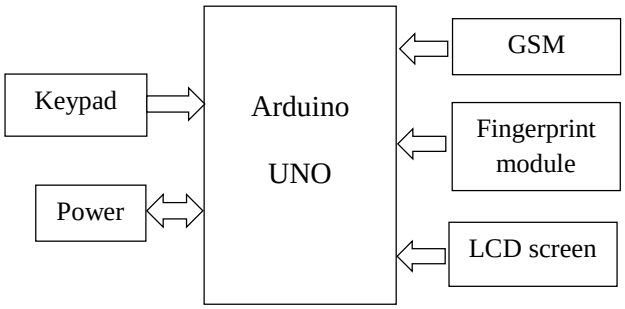

Fig. 1: Block diagram

In this system, we are using Arduino UNO as our main hardware as it has a large assortment of included libraries and built-in pinouts. External circuits required in Arduino are less compared to microcontroller ARM 7 and ARM 9. Development time is less and architecture is less complex.

We can change the code as and when required. The proposal is to use fingerprints in ATMs as passwords involved with the PIN number. Fingerprint recognition will make users relax by preventing unauthorized account access and assuring security.

The Fingerprint and the user-id of all users are stored in the database. Fingerprints are used to identify whether the Person is genuine.

A Fingerprint scanner is used to acquire the fingerprint of the individual, after which the system requests for the PIN (Personal Identification Number).

In this system, Bankers will collect the fingerprints of the customers and their mobile number while creating the accounts then customer only can access ATM machine.

The working of this ATM machine is when the customer places his finger on the fingerprint module when access it automatically generates different 4-digit code as a message every time to the mobile of the authorized customer through GSM modem which is connected to the Arduino Uno.

The code that received by the customer should be entered by pressing the keys on the keypad provided. After entering it checks whether it is a valid one or not.

If the OTP is valid then the customer can proceed with the further bank transactions. If the customer enters the wrong OTP then the customer gets 3 chances to enter the correct OTP. If still not valid then the process terminates and the customer has to scan the fingerprint again.

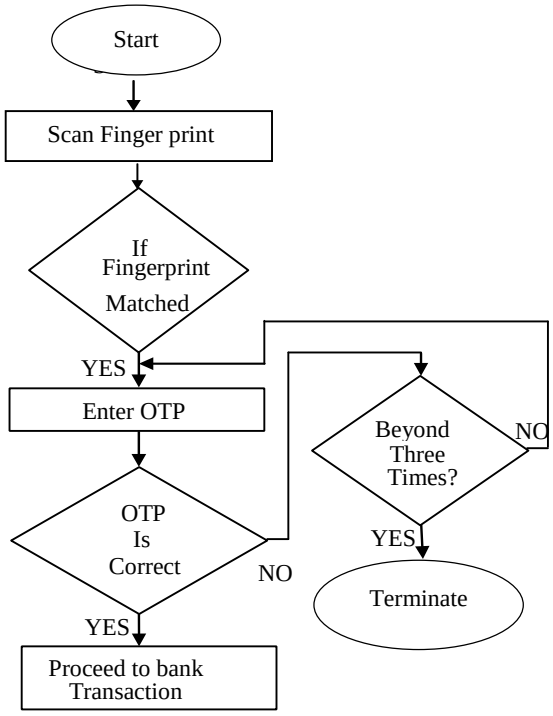

Fig. 2: Flow chart

4. CONCLUSION

The proposed system based on Arduino microcontroller is found to be more compact, user-friendly and less complex, which can readily be used in order to perform several tedious and repetitive tasks. The implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. This approach has enabled us to achieve the target of controlling the device remotely using an SMS-based system satisfying user needs and requirements. The system is implemented with high reliability and security. The system is extendible and further additions can be done. Hence, we can conclude that the required goals and objectives have been achieved.

5. FUTURE SCOPE

1. Future, we can expand this project by adding a GPS module which sends the alert message to authority telling that at which the ATM is tried to be theft.
2. Today IOT is been implemented everywhere, so IOT can be also used for security purpose.
3. Sensors like Eye Sensor can be used to make the system more reliable.

6. ACKNOWLEDGEMENT

The authors gratefully acknowledge Prof. Vrushali Purandare from Watumull Institute of Electronics and Computer Technology, for her guidance in the project and providing encouragement for this work.

7. REFERENCES

[1] (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012
[2] International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA 2nd National Conference on

Innovative Paradigms in Engineering & Technology (NCIPET 2013) – www.ijais.org
[3] International Journal of Engineering and Technical Research (IJETR)
[4] http://www.svskits.in/index.php/advanced-projects/atm-security-system-using-gsm-and-finger-module-detail.html
[5] International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014.
[6] International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.
[7] International Journal of Control, Automation, Communication and Systems (IJCACS), Vol.1, No.2, April 2016.

