



INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 5, Issue 2)

Available online at: www.ijariit.com

Enhanced fingerprint recognition and OTP to improve ATM Security

Shivam Kumar Rajput

rshivam069@gmail.com

K.C. College of Engineering and Management Studies
and Research, Thane, Maharashtra

Aniket R. Patne

aniketpatne25@gmail.com

K.C. College of Engineering and Management Studies
and Research, Thane, Maharashtra

Amit Varma

amitvarma14313@gmail.com

K.C. College of Engineering and Management Studies
and Research, Thane, Maharashtra

Girish Vishe

girishvishe5@gmail.com

K.C. College of Engineering and Management Studies
and Research, Thane, Maharashtra

ABSTRACT

In the previous few years' robberies of ATM is increasing and becoming a problem for Banks. In the current system, we operating ATM using a PIN number which can be stolen or guessed and can be hacked during the transaction. That raises a question on the present security and demands something new in the system which can provide the second level of security. So for that in this paper, there is added some extra security to the current ATM Systems. We use the fingerprint system and One Time Password (OTP) which is sent to the user registration mobile number through GSM Module system. After that, the user will be able to complete the transaction securely. 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 microcontroller [1]. The code received by the customer should be entered by pressing the keys on the keypad provided. This proposal will go a long way to resolve the problem of bank account safety and transaction.

Keywords— ATM, OTP, Biometric, Security, Fingerprint, GSM

1. INTRODUCTION

In today's fast life nobody wants to wait in long queues for banking activities, they don't want to wait for the too long time that's why many of us are using ATM machine. A 24x7 self-banking service has made the ATM the heart of the banking system. With the help of ATM, the user can perform several banking activities like cash withdrawal, credit card/debit card payment, and money transfer from one account to another, paying various home usages bills like electricity, water, and phone bills. ATM (Automatic Teller Machine) has proved to be

an easy and convenient way to carry out all our banking tasks in just a few minutes [3]. As the use of ATMs has been increasing day by day the number of fraudulent attacks on the ATMs also increasing.

The existing ATM model uses a card (ATM/debit card or credit or credit card) and a PIN which gives rise to an increase in attacks in the form of stolen cards, or due to statically assigned PINs, the duplicity of cards and various other threats [4]. An ATM card or debit card authenticates person after verification of card number, Expiry date, card owner name, and the PIN [5]. But what if the card is stolen, or PIN is known to an unauthorized person. For this, we require a higher level of security which coined up an idea of adding Biometric and one-time password (OTP) to the current technology.

Biometric authentication can be Fingerprint scanning, facial recognition, Retina recognition, Iris scanning, etc. The biometric measures used generally include palm or finger vein print biometrics, although they may also include other functionalities such as iris recognition or face recognition. But here we are recommending a technology which works on the technology fingerprint recognition system. Biometric technology provides secure and irrefutable authentication.

Here at the start fingerprint of persons is registered in the database using fingerprint module. There are 4 switches we are used to registering the fingerprint of the persons. The then 16x2 LCD display is used to display whether person is authorized or not. Fingerprint module will recognize fingerprint of the persons and will transfer this data to Arduino, Arduino will further send a signal to the GSM module. When a person places his/her finger in the fingerprint scanner and comparison of the fingerprint of the person is made with the database. If the fingerprint detection matches with user's pre-saved fingerprint database then the user will get an OTP in his/her predefined or

register number through GSM module. The user will type the OTP using keypad. If OTP and the fingerprint of the person are matches with the database then only access will be granted to the user for the transaction. If OTP and fingerprint of the person do not match then access will not be granted and the transaction will be failed. And also buzzer will get ON which give alert and the message will be displayed on the LCD that person is unauthorized.

2. PROPOSED SYSTEM

Our project brings forward the idea of using fingerprint and OTP in ATMs as a password instead of the traditional pin number. OTP feature along with the fingerprint authentication which will surely not allow any criminal to use the password for frauds as the OTP is valid only for one time [8]. Our project has two levels of security: 1.) Using fingerprint, 2.) OTP.

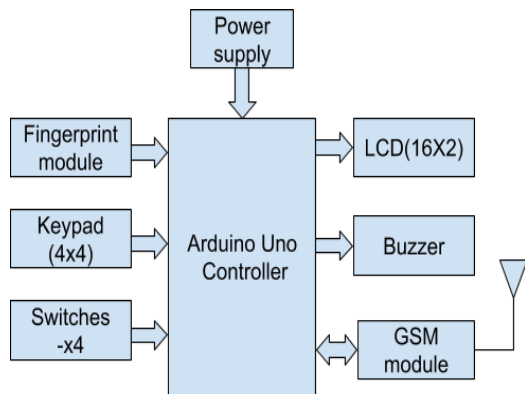


Fig. 1: A proposed system block diagram

In our suggested system at the initial stage, an SMS is sent to the mobile i.e. “GSM Test Ok” which indicates our system is working properly. And in the next step, we will scan our finger through the fingerprint module. Then if the fingerprint is matching with the database, then a message will be displayed on the LCD screen that is “MATCH FOUND”. And after OTP will be sent to the user account holder or user mobile number, OTP consists of 4 digits random number for e.g. 1234. The further user will enter the password through 4x4 Keypad which is directly connected to the Arduino Uno Controller. If the password is matched, then on the LCD screen a message will be displayed i.e. “PASSWORD CORRECT” and then the user can complete their transaction. But, in case if the user will enter the wrong password then the message will be displayed on the LCD screen i.e. “WRONG PASSWORD”. And if the user has the chance to reenter the password, after this if the user entered the wrong password more than three times, then an alert SMS is sent to the user number or account holder which will be like “THEFT ALERT”. And in this way, the transaction process is terminated. It means some other person is trying to access their account. And through this process, this our system works.

2.1 Hardware description

- **Fingerprint module-R305:** This is a fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 or USB-Serial adapter
- **Arduino Uno controller:** The Arduino Uno is a microcontroller board based on the ATmega328 microcontroller.
- **LCD (16X2) Module:** A 16x2 LCD means it can display 16 characters per line and there are 2 such lines and each character is displayed in the 5x7 pixel matrix.
- **GSM module:** A GSM modem is used to send the OTP to the registered mobile number.

- **Buzzer:** The buzzer will alert the user if any unauthorized accessed is taking place.
- **Keypad-(4x4):** It is of numeric type to input numeric values and alphabets from A to D which can be used for other purposes.

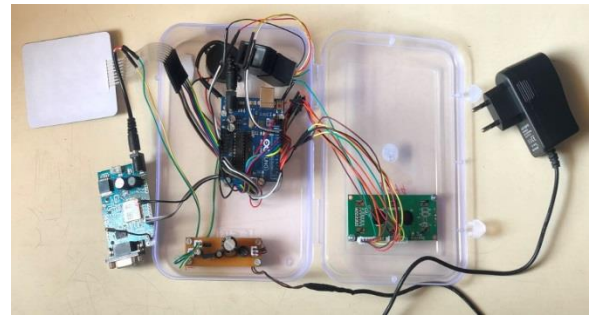


Fig. 2: Constructed hardware

2.2 Software model

The software design includes two stages. First of all the first module of code will be designed for user interface with ATM machine and another module of code will be for scanning and matching of the fingerprint. The overall flow diagram of software design is given in figure 3.

At the start, there will be the initialization of all the components and then start the procedure by registering and scanning of the fingerprint. After that OTP will be sent to the registered mobile number of the user. The OTP will be entered by the user and if the OTP is correct, the user is allowed to do the transaction. Otherwise, transaction ends and we need to start it again.

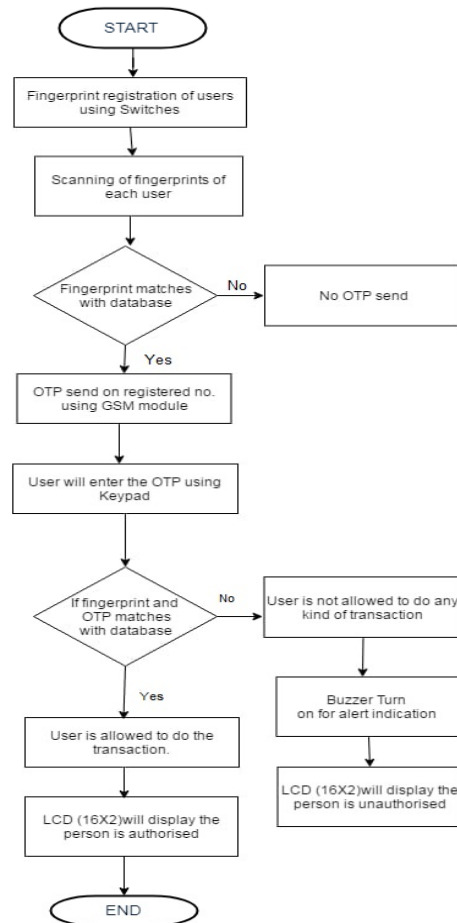


Fig. 3: Flow Chart of the proposed system

2.3 GSM technology

In order to send OTP, GSM (Global System for Mobile Communication) technology is used with the help of GSM

module. A GSM Modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages.



Fig. 4: SIM900A GSM Modem

2.4 Fingerprint technology overview

The unique nature of a fingerprint makes it ideal for use in automated recognition systems. A fingerprint is made of a series of ridges and grooves. Once a fingerprint is captured the system locates the minutia points. These minutia points occur where the lines of the ridges begin, end, branch off and merge with other ridgelines. These points are then mapped and a line is drawn between each point. This creates a map of how each point relates to the other points [12]. The map is then stored as a data stream called a minutia template in a database for future comparison with other presented fingerprints. It is important to note that during the entire process no fingerprint images are stored on the system and a fingerprint image cannot be recreated from the minutia template.

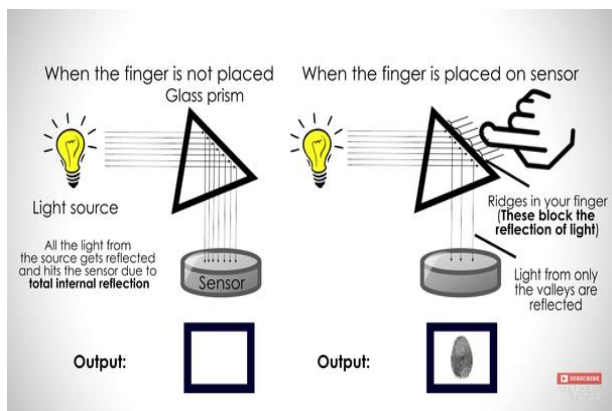


Fig. 5: Overview of Fingerprint Scanner

3. ADVANTAGES OF PROPOSED SYSTEM

- It will give foolproof authentication.
- It is very effective as compared to other methods.
- Biometric tokens are the safest means of preventing ATM frauds.
- The one-time password sends by GSM modem to the user changes every time so it provides good security.
- People are forced to remember many passwords. But biometric technology does not require the use of any Password or PIN.
- F. In some application, biometrics can replace or reestablish the existing technology.
- G. Biometric systems have less error rate and it is convenient to use.

4. APPLICATIONS OF BIOMETRIC SYSTEM

- The biometrics can be used mainly used for Security purposes such as Counterterrorism, Access control, comparing surveillance images to know terrorist.
- It can be used in schools to verify the identity of individuals picking up children from schools.
- It is also helpful for increasing the residential Security as it will alert the homeowners of approaching unknown persons.
- One of the applications of biometrics is in Voter verification, where eligible politicians are required to verify their identity during a voting process this is intended to stop voting where the vote may not go as expected.
- And one of the most vital applications of biometrics is in the field of the Banking system to verify the authorized person.

5. CONCLUSION

Automatic Teller Machines have become a sophisticated technology which provides financial services to different area, countries and different client all over the world. In today's world ATM is getting less secure with arriving new ways to hack or crack ATM PIN or ATM card. Use of OTP and Biometric systems is the best and easy way to deal with these security threats friendly and non-invasively. Using this system the ATM system is secured from thief attacks. We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking [7]. The developed application has been found promising on the account of its sensitivity to the recognition of the cardholder's fingerprint as contained in the database [7]. If this system when fully deployed it will undeniably reduce the rate of counterfeit activities on the ATM machines. There is a large enhancement in the security features which helps in stability and reliability of the owner's recognition. This type of system can be used in various security systems.

6. FUTURE SCOPE

In future, we can add face recognition feature in this current system using image processing in which we can use open CV software using python language, which gives higher accuracy in face recognition and some other algorithms.

Also, we can add some sensors like a tilt sensor which is used to alert about the robbery of cash from the ATM. As in the current system, we are entering the less no. of the fingerprint of persons but in future, we can increase this count.

7. ACKNOWLEDGMENTS

As the authors of this paper, we would like to acknowledge our Project guide Ms Rupinder Kaur and Head of EXTC Department Dr Baban Rindhe of K.C. College of Engineering and Management Studies & Research for giving their support and help for the development and research of this paper.

8. REFERENCES

- [1] T.N.S.Pallavadar and V.Srinivas, "ATM Security using GSM and Fingerprint with Authorized Permission for Transaction", International Journal of Emerging Engineering Research and Technology Vol. 3, Issue 11, November 2015, pp. 86-91.
- [2] Moses Oketchukwu Onyesolu and Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study", International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012, pp. 68-72.
- [3] S.Naga Gowri, R.Durga Devi and P.Gowshalya, "A Biometric based ATM Security System using RFID &

- GSM Technology”, International Journal for Modern Trends in Science and Technology, Vol. 03, Issue 04, April 2017, pp. 169-176.
- [4] Chaitali Bhosale, Pooja Dere, Chaitali Jadhav, "ATM security using face and fingerprint recognition", International Journal of Research in Engineering, Technology and Science, Vol. VII, Special Issue, Feb 2017.
- [5] Archana A. Talikoti, Deepa Modi, Laxmi Talikoti, "SECURITY OF ATM SYSTEM USING RFID AND OTP", Visvesvaraya Technological University, Belagavi, 2018.
- [6] <https://www.scribd.com/doc/249699706/Biometrics-and-Banking-Special-Report>
- [7] M.Padmavathi, B.Rajeshkumar, R.Ganesh Kishore, "Bio-Matric Intelligent ATM System", International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-4248, Vol. 4, Issue 3, March 2018, pp. 573 – 577.
- [8] Rathishala Rajendran, Kavita Anandraj, Edwina Jacob and Chhaya Narvekar, "ATM Security using Fingerprint Authentication and OTP", Vol.5, No.2, April 2015.
- [9] [9] <http://itatec.co.za/sagem-biometrics-fingerprint-reader>.
- [10] G.Sambasiva Rao, C. Nagaraju, L. S. S. Reddy and E. V. Prasad, "A Novel Fingerprints Identification System Based on the Edge Detection”, International Journal of Computer Science and Network Security, vol. 8, pp. 394-397, (2008).
- [11] N.Selvaraj & G.Sekar, "A method to improve the security level of ATM banking systems using AES algorithm”, International Journal of Computer Applications (0975-8887), Vol.3, No.6, June 2010.
- [12] <http://itatec.co.za/sagem-biometrics-fingerprint-reader/>