Advanced Smart ATM Authentication System

N. Ganitha Aarthi[1],

Assistant Professor, Department of Computer Science and Design, SNS College of Engineering(Autonomous), Coimbatore, India. arthi.ganitha@gmail.com

Bharathi.V [2], Hemavathy.K, [3], Ms. Reshmi S [4], Keerthana.A [5] , Joelin Rani.J

UG Students - Department of Computer Science and Design, SNS College of Engineering(Autonomous), Coimbatore, India.

Email ; bharathi.a.v.43@gmail.com , hemavathykamal08@gmail.com , Kuttykeerthi255@gmail.com , joelinrani44@gmail.com

Abstract Over the past few years, ATM robberies have increased and are starting to pose a threat to banks. The PIN number required to operate an ATM under the existing method can be stolen or during the transaction that can be surmised and compromised. This calls into question the current level of security and necessitates the addition of a new component to the system that can offer a second layer of protection. As a result, the present ATM Systems have some additional security included in this study. We make use of the fingerprint system and the One Time Password (OTP), which is transmitted via the GSM Module system to the user's registered mobile number. The user will then be able to safely finish the transaction. This ATM operates by automatically generating a unique 4-digit code whenever a consumer places his finger on the fingerprint module. As a message sent once a day to the approved customer's mobile device using a GSM modem that is linked to a microcontroller. The customer must input the code they got by tapping the keys on the supplied keypad. This plan will significantly help to address the issue of transaction security and bank account safety.

Keyword-ATM, OTP, Biometric, Security, Fingerprint, GSM.

I. INTRODUCTION

Nowadays, with everyone's life moving so quickly, nobody has time to stand in line for lengthy banking procedures. For this reason, a large number of people use ATMs. An ATM is now the central component of the banking system because to its 24/7 self-banking service. An ATM can be used to pay for a variety of household bills, such as those related to energy, water, and phone use, as well as to withdraw cash, pay with a credit or debit card, and transfer money between accounts. We may now complete all of our banking duties quickly and easily with the help of ATMs (Automatic Teller Machines). The number of fraudulent assaults against ATM has been rising daily in tandem with the growing use of these machines. The current ATM paradigm involves an ATM/debit card, credit card, or both, together with a PIN. This leads to a growth in assaults via stolen cards, PINs that are statically assigned, card duplication, and other risks. After the card number, expiration date, owner name, and PIN are verified, an ATM or debit card can be used to authenticate a person. But what happens if the card is lost or stolen, or if someone not authorized knows the PIN? We need a better level of security for this, which is why the idea to incorporate biometric and one-time password (OTP) into the current technology was developed. Biometric authentication methods include facial recognition, fingerprint recognition, retinal recognition, iris recognition, and more. Although they may also incorporate additional features like iris or face recognition, palm or finger vein print biometrics are the most commonly utilized biometric measurements. However, the technique that we are recommending here is based on the fingerprint recognition mechanism. Authentication with biometric technologies is safe and unchallengeable. People's fingerprints are initially recorded in the database using their mobile fingerprints here. There are four switches that we employ to record each person's fingerprint. It is shown on the 16x2 LCD display whether or not a person is permitted. The fingerprint module will identify each person's fingerprint and communicate this information to the Arduino, which will then send a signal to the GSM module. when a user inserts their finger into the fingerprint scanner and the fingerprint is compared to the

 DOI : 10.35291/2454-9150.2024.0078

database. The user will receive an OTP in his or her predetermined or registered number through the GSM module if the fingerprint detection matches the user's pre-saved fingerprint database. The OTP will be typed by the user on the keypad. Only the user will be able to access the transaction if their fingerprint and OTP match those in the database. Access won't be allowed and the transaction will fail if the user's fingerprint and OTP don't match. Additionally, an alert buzzer will sound, and an LCD message indicating that the person is not permitted will appear.

II. LITERATURE SURVEY

In [1], R. Ramani proposed a new approach for creating and implementing a GSM-based bank locker security system that could be set up in safe houses, workplaces, and banks. Through this technique, money from bank lockers may only be retrieved by genuine individuals. The passive tag's ID number is read by the RFID reader and sent to the microcontroller. If the ID number is valid, the microcontroller sends an SMS requesting the original password to open the bank locker to the verified person's mobile number. If the person responds with the password, the microcontroller verifies the passwords entered using the keypad and received from the verified mobile phone. The locker will unlock if the two passwords match; if not, it will stay closed.

In [2], Using biometrics and hybridization, Pramila D. Kamble created a fingerprint verification system for an ATM security system. Fingerprint recognition is one of the most dependable and promising biometric technologies. These are the fingerprints that are the most used biometric characteristic for identifying individuals and confirmation. However, He suggested in this paper that ATM (Automatic Teller Machine) fingerprint verification biometric security system with hybridization. The fingerprint characteristic is selected due to its accessibility.

In [3], Professor S.B. Patel gave a presentation on GSM and Biometric Locker Security. We shall create GSM and biometric (finger or face) technology for bank lockers in this review article. Because only authorized individuals can retrieve money and papers from the lockers under this system, the bank will gather each person's biometric information to grant access to the lockers.

In [4], A smart banking security system using Pattern Analyzer was proposed by K. Amsawali. Pattern flows are first gathered and stored on bank agent servers as datasets. The device has a camera to record the user's pattern of movement, which is then transferred for processing so that the logic's features can be compared and the user where acknowledged. A password is required for an additional layer of protection. In the future this kind of authentication option can be used by banks for banking.

III. METHODOLOGY

3.1. Proposed Methodology

In place of the conventional pin number, our project proposes the use of fingerprint and OTP as an ATM password. fingerprint authentication in addition to the OTP functionality which ensures that no criminal will be able to use the password for fraudulent purposes because the OTP is only good for one time. We have two security tiers for our project. 1. Employing a fingerprint, 2. Using an OTP. The first step of our proposed method involves sending an SMS to the phone that says "GSM Test Ok," indicating that everything is operating as it should. And we will scan our finger in the following phase via the module for fingerprints. A notification indicating "MATCH FOUND" will then appear on the LCD screen if the fingerprint matches the database. Additionally, an OTP consisting of a four-digit random number, such as1234, will be sent to the user's mobile number or account holder when it has been received. Through the 4x4 Keypad, which is directly connected to the Arduino Uno Controller, the additional user will enter the password.

3.2 Block Diagram

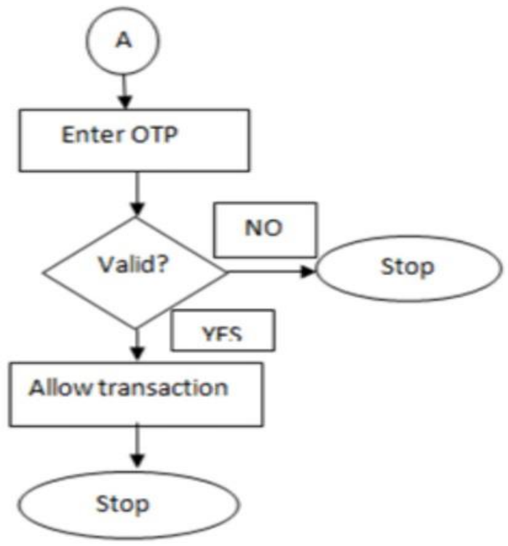

Fig 1 ; Proposed system block diagram

3.3 Biometric Fingerprint

An essential part of ATM security is a biometric scanner, which is used to confirm a user's identification using their distinct physiological or behavioral traits. The biometric scanner used for fingerprint authentication at ATMs is made to recognize and analyze the unique patterns seen in each fingerprint. Capacitive or optical sensors are frequently used in biometric scanners. While optical sensors use light to capture the fingerprint image, capacitive sensors identify differences in electrical current in the ridges and valleys of the fingerprint. The user's fingerprint is captured by the scanner, which produces a

 DOI : 10.35291/2454-9150.2024.0078

ISSN : 2454-9150 Vol-09, Issue-12, Mar 2024

high-resolution image that highlights fine details like ridge patterns, bifurcations, and ends. This comprehensive data creates an individual's distinct biometric template.

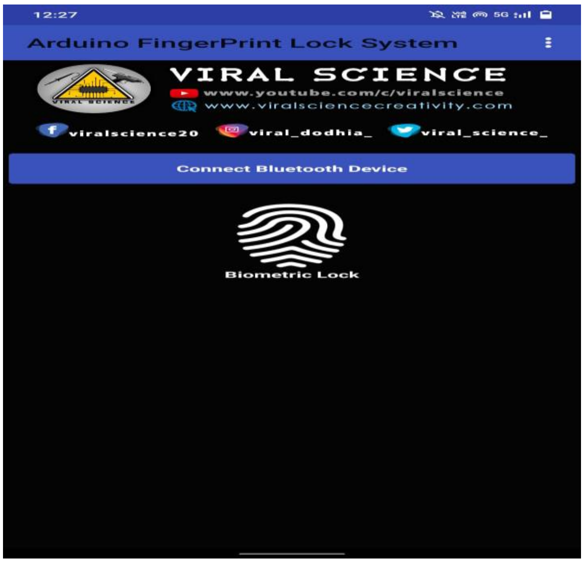

Fig 2: Biometric Fingerprint

Biometric scanners ought to function reliably in a range of circumstances, taking into consideration changes in skin tone, hygienic conditions, and external elements. A security of the biometric system is improved by countermeasures against spoofing attempts, like the use of phony fingerprints or photos. A thorough understanding of the biometric scanner's workings will help one recognize how important it is to the overall security of financial transactions to provide secure and reliable user authentication at ATMs.

3.4 GSM Module

Mobile voice and data services are sent over the open, digital cellular technology known as GSM (global standard for mobile communications). The primary uses of GSM, a global mobile communication technology, are the transmission and receiving of voice and message data. This security system relies heavily on GSM service. SMS (short messaging service) transmission is supported by GSM, along with phone conversations and data transfers up to 9.6 kbit/s. A type of wireless MODEM device called GSM MODEM is intended to facilitate computer connection with GPRS and GSM networks. Similar to cell phones, it needs a SIM (Subscriber Identity Module) card in order to initiate contact with the network.

3.4.1 AT Commands

MODEMs are operated using AT commands. The following data and services can be accessed via AT commands with a GSM MODEM or mobile phone: SMS, MMS, Fax, and data and voice link over mobile network.

SMS messages can be sent and received using GSM modules. Alert systems, control systems, and remote monitoring systems frequently make use of this feature.

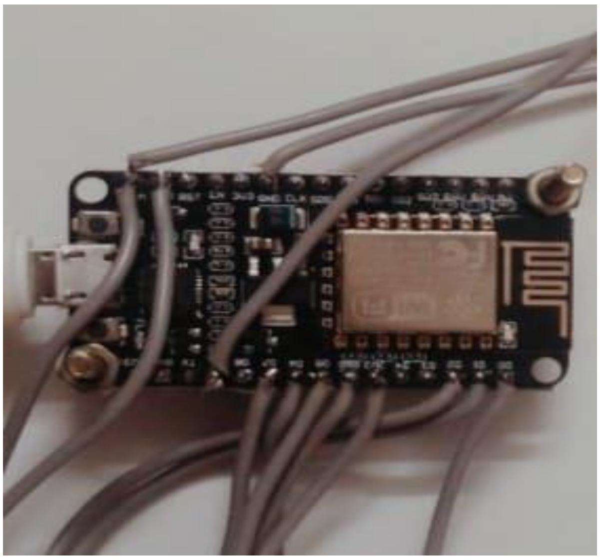

Fig 3 GSM Module

3.5. Ubidots Website

The main focus of Ubidots' cloud-based Internet of Things technology is data visualization, analytics, and monitoring for linked devices. It is not specifically designed with ATM security utilizing OTP and fingerprint authentication in mind. I can, however, offer a speculative scenario in which an ATM system with biometric authentication might benefit from the use of Ubidots or a comparable IoT platform to increase security. Collaboration with security specialists, adherence to pertinent regulations, and regular updates based on growing security standards are all necessary for the actual deployment of such a system. Furthermore, after my previous update, Ubidots or comparable platforms might have included new features or improvements, so it's best to consult their most recent documentation for the most up-to-date details.

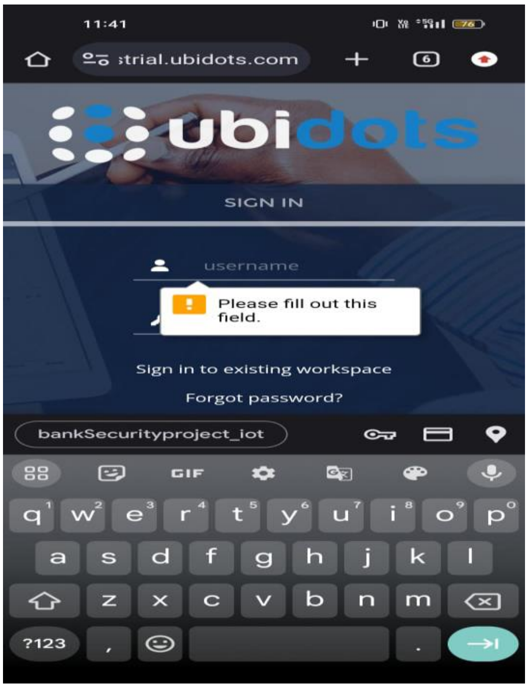

Fig 4: Ubidots Website

 DOI : 10.35291/2454-9150.2024.0078

3.6 LCD

Our board comes with a 16*2-character LCD display outside of the box. Access permitted and denied messages are shown on LCDs. There are sixteen and twenty characters per line by two lines, respectively, in LCDs. The timing of locker opening and closing. LCD displays can be used to show messages, open and close doors, prompt users to input passwords, and more.

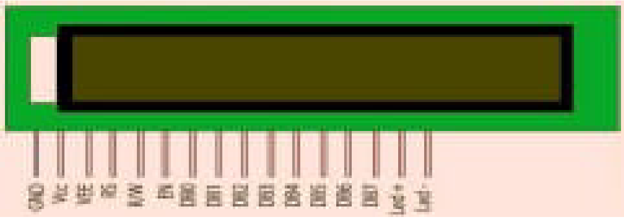

Fig 5: LCD Display

3.7 OTP Generator

An essential part of multi-factor authentication systems, the OTP (One-Time Password) generator provides an additional degree of protection for operations like ATM transactions. During the initial configuration, a unique secret key that is only known by the authentication server and the generator is generated. Comprehending the complexities of the OTP generator emphasizes how it strengthens security by adding a dynamic, time-sensitive component to the authentication procedure. This strengthens the defense against unwanted access considerably, particularly when combined with other authentication elements like biometrics.

IV. RESULT AND DISCUSSIONS

STEP 1: The first appears on the LCD when the board is powered on.

Fig 6: LCD Display

STEP 2: The welcome note scan fingerprint is displayed on the LCD.

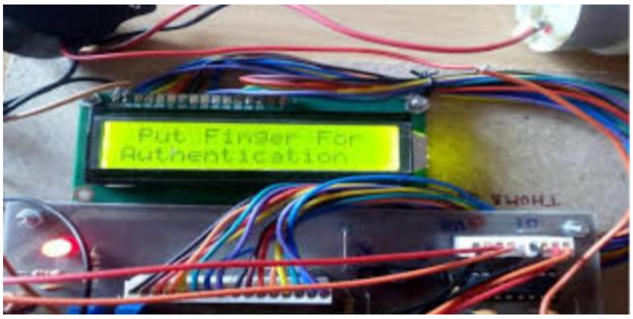

Fig 7: Indication to scan the finger.

STEP 3: It shows two possibilities if the fingerprints match.

STEP 4: Selecting option 1 (open door) will cause the LCD to display.

STEP 5: Option 2 (modify user) has been chosen; the LCD will display.

STEP 6: If the fingerprints don't match, the LCD will show this.

STEP 7: The buzzer will sound.

STEP 8: Step 3 requires us to input a working password.

STEP 9: Step 7 will cause the door to automatically open.

STEP 10: Once the task is finished, we must press any key to shut the locker door and return to step 1.

STEP 11: Four options are displayed when option 2 is selected. Choose the necessary option; for instance, if option 4, or the cancel option, is chosen, the process returns to step 1.

V. CONCLUSION

Automated Teller Machines (ATMs) have developed into sophisticated technological tools that offer financial services to a wide range of clients, regions, and nations worldwide. In the current ATM security is decreasing due to emerging methods of hacking or cracking ATM PINs or cards. The most effective and simple method of countering these security risks in a non-intrusive and courteous manner is to use biometric and OTP systems. By using this technique, the ATM is protected against hacker attempts. As a biometric measure, we have been able to create a fingerprint mechanism that improves the ATM's security characteristics for efficient banking. The created program has shown promise due to its sensitivity in identifying the cardholder's fingerprint from the database. In case Without a doubt, when this technology is fully implemented, the number of fraudulent transactions on ATMs will drop. The consistency and dependability of the owner's recognition are aided by a significant improvement in the security features. A variety of security systems can employ this kind of technology.

 DOI : 10.35291/2454-9150.2024.0078

ISSN : 2454-9150 Vol-09, Issue-12, Mar 2024

REFERENCES

[1] A.Aditya Shankar, P.R.K.Sastry, A.L.Vishnu ram.A.Vamsidhar Fingerprint Based Door Locking System International Journal of Engineering and Computer Sciences ISSN:2319-7242, Volume 4 Issue 3 March 2015.

[2] Kanak Chopra, garvit Jain Door Opening System Based on Fingerprint Scanning International Journal of Engineering Research Management Technology, March 2015, Volume 2, Issue-2.

[3] Pavithra.B.C, Myna.B.C, Kavyashree.M Fingerprint Based Bank Locker System Using Microcontroller Proceedings of IRF International Conference, 5 April-2014, Pondicherry, India, ISBN: 978-93-82702-71-9.

[4]M.Gayathri, P.Selvakumari, R.Brindha Fingerprint and GSM based Security System International Journal of Engineering Sciences Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.

[5] Sagar S. Palsodkar, Prof S.B Patil Biometric and GSM Based Security for lockers International Journal of Engineering Research and Application ISSN: 2248-9622, Vol.4, December 2014.

[6] Raghu Ram.Gangi, Subhramanya Sarma.Gollapudi Locker Opening and Closing System Using RFID, Fingerprint, Password and GSM International Journal of Emerging Trends Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March April 2013.

[7] R.Ramani,S.Valarmathy, S. Selvaraju, P.Niranjan Bank Locker Security System based on RFID and GSM Technology International Journal of Computer Applications (09758887) Volume 57 No.18, November 2012 .

[8] Pramila D Kamble and Dr. Bharti W. Gawali Fingerprint Verification of ATM Security System by Using Biometric and Hybridization International Journal of Science and Research Publications, Volume 2, Issue 11, November 2012.

[9] Gyanendra K Verma, Pawan Tripathi, A Digital Security System with Door Lock System Using RFID Technology, International Journal of Computer Applications (IJCA) (0975 8887), Volume 5 No.11, August 2010.

[10] Mary Lourde R and Dushyant Khosla Fingerprint Identi_cation in Biometric Security Systems International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October,2010.

[11] Sagar S. Palsodkar*, Prof S.B. Patil , "Review: Biometric and GSM Security for Lockers" Int. Journal of Engineering Research and Applications , Vol. 4, Issue 12(Part 6), December 2014.

[12] R.Ramani , S. Selvaraju , S.Valarmathy, P.Niranjan , "Bank Locker Security System based on RFID and GSM Technology '', International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012.

[13] Vaijanath R. Shintre, Mukesh D. Patil, "Banking Security System Using PSoC". International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 7, July 2015.

[14] Tarief.M. F. Elshafiey, "Design and Implementation of a museum and bank security system using antenna as IR proximity sensor and PSoC Technology", IEEE symposium on wireless technology and applications, September 25-28 Malaysia 2011.

[15] Bhalekar S.D., Kulkarni R.R., Lawande A.K., Patil V.V., "Online Ration card System by using RFID and Biometrics", International journal of Advanced Research in Computer Science & Software engineering., Vol. 5, Issue 10, October 2015.

 DOI : 10.35291/2454-9150.2024.0078