ATM SECURITY USING FINGERPRINT IDENTIFIER

Mr.N.NARESH [1] ,K. KARUNIKA[2], K.GREESHMA REDDY[3], G.SAI SHARANYA[4] ,G.RAHUL[5]

[1] Assistant Professor, Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College(An Autonomous Institution), Medbowli, Meerpet, Saroornagar, Hyderabad-500097

[2,3,4,5]Students, Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College(An Autonomous Institution), Medbowli, Meerpet, Saroornagar, Hyderabad-500097

ABSTARCT

With the growing number of ATM-related crimes, there is an urgent need to enhance the security of ATM transactions. Traditional PIN-based authentication systems are increasingly proving to be vulnerable, as PINs can be easily guessed, stolen, or hacked. To address these issues, this project proposes a dual-layer ATM security system that integrates biometric fingerprint recognition with One-Time Password (OTP) verification. The system is designed to ensure that only the rightful account holder can access their funds. When a user initiates a transaction, the system first verifies their identity through a fingerprint scan using a biometric module. If the fingerprint matches the stored record in the database, the system confirms successful identification with a "MATCH FOUND" message on the LCD. Following this, a unique 4-digit OTP is automatically generated and sent to the user's registered mobile number via a GSM module. The user must then enter this OTP using a 4x4 keypad connected to an Arduino Uno microcontroller. If the entered OTP is correct, the transaction proceeds, and a confirmation message "PASSWORD CORRECT" is displayed. However, if the OTP is entered incorrectly more than three times, a security mechanism is triggered, and an alert SMS stating "THEFT ALERT" is sent to the user's mobile number. The transaction is then blocked to prevent unauthorized access. This dual-factor authentication system significantly strengthens ATM security by combining biometric verification with dynamic OTP-based authentication, effectively minimizing the risks associated with PIN theft and fraud.

I.INTRODUCTION

Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has

impacted positively and negatively to banking activities and transactions is the advent of automated teller machine (ATM). With an ATM, a customer is able to conduct several banking activities such as cash

withdrawal, money transfer, paying phone and electricity bills beyond official hours and physical interaction with bank staff. In a nutshell, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. Personal identification number (PIN) or password is one important aspect in ATM security system. PIN or password is commonly used to secure and protect financial information of customers from unauthorized access [1]. An ATM (known by other names such as automated banking machine, cashpoint, cash machine or a hole in the wall) is a mechanical system that has its roots embedded in the accounts and records of a banking institution [1]-[2]. It is a computerized machine designed to dispense cash to bank customers without need of human interaction; it can transfer money between bank accounts and provide other basic financial services such as balance enquiries, mini statement, withdrawal and fast cash among others [3]. The paper is arranged as follows. Section II provided the background of ATM security and the need for biometrics. identifiers. Section IV described the materials and methods employed to conduct the survey. Section V presented the results obtained and the discussions on the results. Section VI concluded the paper.

II.LITERATURE SURVEY

1. Lee et al. (2011) discussed how ATM card skimming devices could easily intercept card data, compromising the security of the entire system.

2. Singh and Singh (2015) highlighted that PINs are often vulnerable to being stolen by onlookers or through malicious practices such as shoulder surfing.

3. Jain et al. (2007), fingerprint recognition was proposed as an ideal biometric method due to its accuracy and low possibility of forgery. This study demonstrated the efficiency of fingerprint sensors in real-world applications, making it a feasible solution for ATM security.

4. Diao et al. (2013) explored the integration of fingerprint recognition with ATMs, showing that biometric systems provided greater security by preventing unauthorized access through lost or stolen cards. However,

they also noted challenges like fingerprint spoofing and sensor malfunctions.

5. Bai et al. (2014) proposed the integration of biometric fingerprint recognition with PIN authentication, offering an additional layer of security. This approach reduced the risks associated with stolen or guessed PINs and was well-received in the academic and financial sectors.

6. Patel et al. (2017) introduced the concept of adding One-Time Password (OTP) systems to ATM security. OTPs, generated dynamically and sent via SMS, provide an additional layer of security against PIN-based vulnerabilities. The system was shown to be effective in preventing unauthorized access, even if the PIN is compromised.

7. Sahu et al. (2019) proposed the use of GSM modules for sending OTPs to registered mobile numbers. This approach ensures that an unauthorized individual cannot easily access the ATM even if they have the user's card and PIN. The OTP is unique for every transaction, and its short validity period makes it almost impossible for attackers to use it maliciously.

8. Chandran et al. (2020), have shown the effectiveness of combining biometric authentication and OTP for securing ATM transactions. This dual authentication system drastically reduces the chances of unauthorized access, as it combines something the user has (the mobile device) and something the user is (the fingerprint).

9. Kumar et al. (2018). Fingerprint spoofing using molds of fingerprints has been shown to bypass security in certain systems.

10.Tiwari and Soni (2016) noted that fingerprint sensors can sometimes fail due to dirt, moisture, or poor fingerprint quality, leading to false rejections or system malfunctions.

11. Rai et al. (2020) pointed out that while OTPs enhance security, they are still vulnerable to SIM swapping and interception through social engineering attacks.

12. Combining fingerprint recognition with other biometric features like facial recognition or iris scanning, as studied by Agarwal and Kumar (2021).

III.EXISTING SYSTEM

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 . An ATM

card or debit card authenticates person after verification of card number, Expiry date, card owner name, and the PIN . 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.

IV.PROPOSED SYSTEM

This project introduces a dual-security ATM system using fingerprint authentication and One-Time Password (OTP) verification to replace traditional PIN-based systems. The system operates Upon activation, an SMS ("GSM Test OK") confirms that the system is operational. The user scans their fingerprint using a fingerprint module. If a match is found in the database, the message "MATCH FOUND" is displayed on an LCD screen. A 4-digit OTP is then sent to the user's registered mobile number via GSM. The user enters the OTP through a 4x4 keypad connected to an Arduino Uno controller. If the OTP matches, the message "PASSWORD CORRECT" is displayed, allowing the transaction to proceed. If the OTP is entered incorrectly more than three times, an alert SMS ("THEFT ALERT") is sent to the user's registered mobile number, and the transaction is terminated to prevent unauthorized access.

V.SYSTEM ARCHITECTURE

The diagram you've provided clearly represents the architecture of your dual-authentication ATM security system. Below is a detailed elaboration of the system components and their interactions: This architecture is based on modular design, centered around the Arduino Uno microcontroller, which acts as the central processing unit. The system is composed of various input/output and communication modules, working together to implement a two-layered authentication process: Fingerprint Verification and OTP Authentication. The system architecture of the proposed enhanced ATM security system is designed to implement a dual-layered authentication mechanism, combining biometric verification with OTP-based validation. At the core of this architecture lies the Arduino Uno microcontroller, which serves as the central processing unit, orchestrating communication between various components and managing the overall logic of the system. The process begins when a user initiates a transaction by scanning their fingerprint using a fingerprint sensor module. This sensor captures the

fingerprint image and forwards the data to the Arduino Uno, which then cross-verifies it with pre-registered biometric templates stored in the system's memory. If the fingerprint matches, the microcontroller proceeds to the next stage of authentication. Upon successful fingerprint verification, the Arduino triggers the generation of a unique four-digit One-Time Password (OTP). This OTP is sent to the user's registered mobile number through a GSM communication module. The GSM module is interfaced with the Arduino, enabling real-time message transmission via cellular networks. Simultaneously, the system notifies the user through a 16x2 LCD display, which is also connected to the Arduino. The LCD serves as an interface that guides the user through each step of the transaction, providing messages such as "Match Found", "Enter OTP", or "Transaction Authorized". The user is then prompted to enter the received OTP using a 1×4 matrix keypad connected to the microcontroller. Once the OTP is entered, the Arduino compares it with the originally generated code. If the input matches the generated OTP, the system proceeds with the transaction, displaying a success message on the LCD. However, if the entered OTP is incorrect, the user is given up to three attempts to provide the correct code. If all three attempts fail, the system assumes a potential security breach. Consequently, it activates the alert mechanism and sends a “THEFT ALERT” message to the registered mobile number using the GSM module. This alert system is further supported by a buzzer that can emit a warning sound in the event of unauthorized access attempts. The entire architecture operates on a regulated power supply that ensures stable voltage levels to all components. The software components supporting this hardware setup include the Arduino IDE used for development and programming, written in Embedded C. This software environment allows for seamless integration of modules and effective management of security protocols. Overall, the system architecture integrates biometric identification, secure OTP delivery, and user-friendly interfaces in a synchronized manner, greatly improving ATM security while addressing the limitations of traditional PIN-based systems.

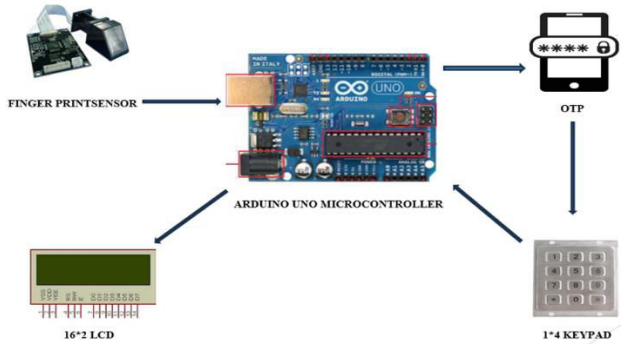

Figure 5.1 System Architecture

VI.OUTPUT SCREENSHOTS

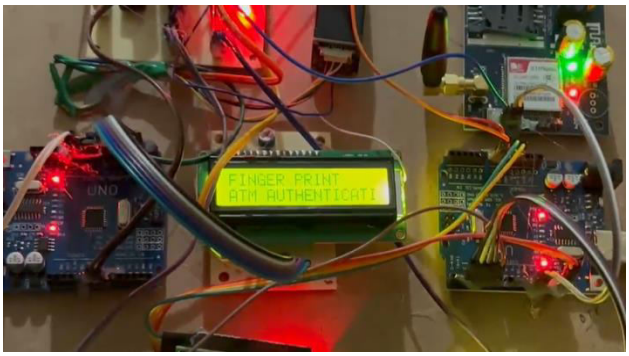

Fig no: 6.1

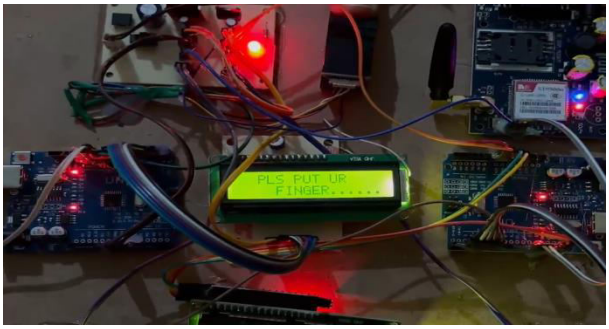

Fig no: 6.2

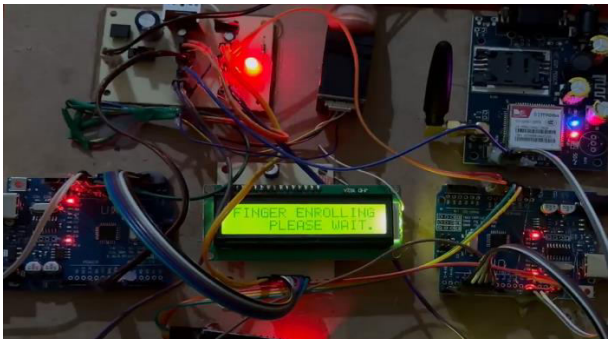

Fig no: 6.3

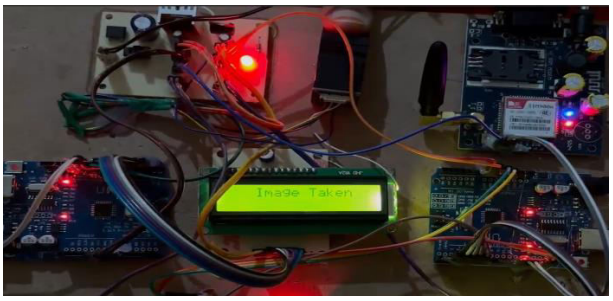

Fig no: 6.4

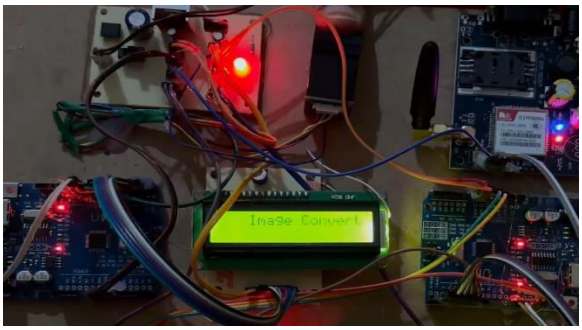

Fig no: 6.5

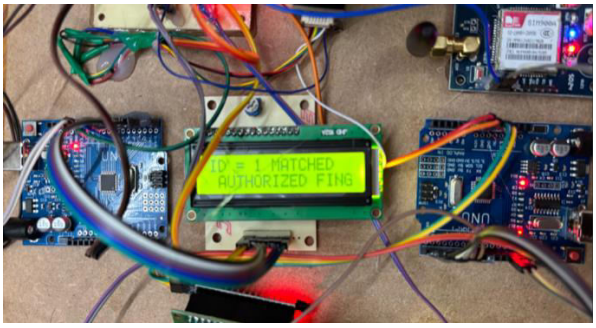

Fig no: 6.6

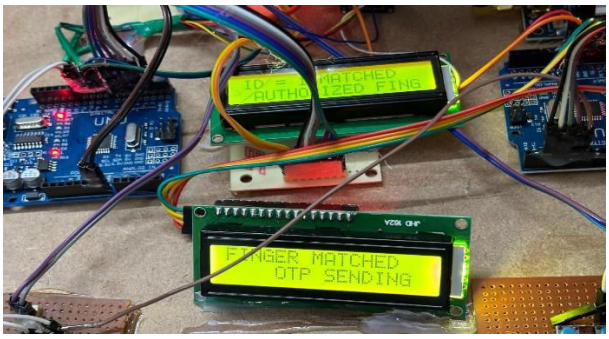

Fig no: 6.7

Fig no: 6.8

Fig no: 6.9

VII.CONCLUSION

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. It cannot be borrowed, stolen or easily forged. Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology using fingerprint identifier may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud and lead to user convenience by broadly providing the following three functionalities (a) positive identification (b) large scale identification and (c) screening.

VIII.FUTURE SCOPE

In the future, this dual-layer ATM security system can be further enhanced through the integration of more advanced biometric modalities such as facial recognition or iris

scanning, providing an additional layer of identity verification and reducing the risk of spoofing attacks. As biometric technologies continue to evolve, incorporating multi-modal authentication will make the system more robust and resistant to breaches. Additionally, cloud-based data storage and verification can be introduced to allow for centralized fingerprint data management, enabling users to access ATMs from any location without relying solely on local databases. This shift towards cloud infrastructure would also enhance scalability and make system updates more manageable across a network of ATMs. Machine learning algorithms can be implemented to monitor and analyse user behaviour, helping the system detect anomalies or suspicious transaction patterns in real-time. This intelligence can be used to automatically trigger alerts or temporarily lock accounts when potential fraud is detected, further tightening security. Moreover, the inclusion of end-to-end encryption for OTP transmission via GSM can protect against interception and enhance data privacy. For improved accessibility and user convenience, future versions of the system could support biometric registration and updates via mobile applications or bank kiosks, reducing the need for physical branch visits. From a hardware perspective, future enhancements might include the use of more compact and power-efficient microcontrollers, enabling easier deployment and maintenance in rural or low-power areas. Integration with NFC or RFID-based identification systems could also provide alternative authentication methods for users with disabilities or those unable to use fingerprint sensors. Overall, these enhancements would not only bolster the security and reliability of ATM transactions but also contribute to building a smarter, more inclusive banking infrastructure.

IX.REFERENCES

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.https://doi.org/10.1109/TCSVT.2003.818349

[2] Chander, H., & Nidhi, M. (2017). Biometric ATM security system using fingerprint and GSM technology. International Journal of Advanced Research in Computer Science, 8(9), 379–382.

[3] Al-Hasan, A., & Al-Khafaji, F. (2019). OTP-based secure authentication system for ATM machines. International Journal of

Computer Applications, 178(24), 1–6. https://doi.org/10.5120/ijca2019918757.

[4] GSM Module Datasheet - SIM800L. (2022). SIMCom Wireless Solutions. Retrieved from: https://simcom.ee/documents/SIM800L/SIM800L_Hardware_Design_V1.00.pdf

[5] Lee, C. C., & Shih, W. K. (2008). A remote user authentication scheme using smart cards with forward secrecy and user anonymity. Future Generation Computer Systems, 24(8), 743–750.

[6] Ramesh, M., & Uma, B. (2021). Enhanced ATM authentication system using IoT and biometrics. In Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC), IEEE, 1587–1592.

[7] Mandal, A., & Saha, D. (2020). Design and Implementation of a Fingerprint Based ATM System Using Arduino. International Journal of Scientific Research and Engineering Development, 3(4), 258–263.

[8] Singh, M., & Arora, A. (2016). Review on ATM security using fingerprint and OTP. International Journal of Innovative Research in Computer and Communication Engineering, 4(7), 13965–13969.

[9] Sood, S. K. (2012). A novel multi-server authentication protocol based on biometrics and smart card with provable security. Computers & Electrical Engineering, 40(5), 1572–1585.