Enhancing ATM Functionality with a Single Card Solution for Multiple Bank Accounts

Pramila priscilla p(piscillapramila5@gmail.com) ,
Dr. T. Selvin Ratna Raj M.E.,Ph.D.,
Florina J (florinanibu@gmail.com),
Jepa Stepy L(jepastepy2627@gmail.com),
Assistant Professor, Department Of ECE,
DMI College of Engineering, Chennai, Tamil Nadu.
DMI College of Engineering, Chennai, Tamil Nadu.

ABSTRACT

This project seeks to modernize traditional magnetic strip ATM cards by transitioning to RFID-based cards, each possessing a unique identifier. The data processing component is managed by an Arduino Mega microcontroller, which interfaces with various sensors to facilitate financial transactions. User authentication is accomplished through a fingerprint module for biometric verification, augmented by the implementation of a One-Time Password (OTP) transmitted to the registered mobile phone to enhance security.

The system is designed to allow users to link multiple bank accounts to their RFID card, thereby enabling a range of transactions, including withdrawals. To ensure the integrity of financial operations, a servo motor activates upon successful user identification, confirming the completion of transactions. Additionally, the system incorporates Python-based facial recognition technology to provide an extra layer of security. Upon successful identification via facial recognition, pertinent data is securely transmitted to the hardware for transaction processing, thereby offering robust protection against unauthorized access and fraudulent activities.

Keywords *——— RFID-based ATM, biometric authentication, Arduino Mega, OTP security, facial recognition, transaction protection, multi-account linking*

1. INTRODUCTION

Modern ATMs are implemented with high-security protection measures. They work under complex systems and networks to perform transactions. The data processed by ATM’s are usually encrypted, but hackers can employ discreet hacking devices to hack accounts and withdraw the account's balance. Hence, to avoid such unauthorized transactions and to protect the confidentiality of the user, we raised the bars by introducing an additional security measure such as the biometrics.

In the proposed method, the magnetic strip-based ATM card is replaced with RFID based card which have a unique number. The Arduino MEGA microcontroller is used to process the data from the sensor. The fingerprint module is used to authenticate the user. The user can register the bank details and also withdraw the amount from the registered bank details. Hence this system provides more secure and multiple bank account using single ATM card.

2. LITERATURE SURVEY

The works related to ATM security monitoring using GSM, MEMS Sensor and tracking unauthorized user using IoT devices and physical security is described in this section.

(a) The model discussed by Venka Reddy Maram, Mirza Sajid Ali Baig, Narsappa Reddy is Advanced Security Management System for ATM's using GSM and MEMS. The theft movement is observed by the MEMS sensor and sends a request to the microcontroller which will automatically lock the door, represented with the help of DC motor and send a message through GSM. A buzzer sound is produced to alert the security. The door will be unlocked with the switch which is present outside the room.

(b) The model discussed by Moturi Phalguna Satishi, Bala Kishore is Implementation of bank security system using GSM and IOT. Here, when any disturbance takes place for the ATM then data is sent through IoT and door is automatically closed. Then an alert is sent to the surrounding area using buzzer, at the same time total data will be uploaded in web page using IoT and puts alert message to the concerned person.

(c) The model presented by Vijay Sharma examines the seamless integration and coexistence of Chipless RFID within a comprehensive Internet of Things (IoT) framework. Radio Frequency Identification (RFID) technology has permeated various applications that are likely to be encompassed by the broader IoT landscape. Nonetheless, the commercial adoption of RFID in IoT-centric applications continues to encounter numerous technical challenges, primarily attributable to its elevated cost. Chipless RFID offers a significant advantage in this context due to its substantially reduced costs and simplified tag complexity.

(d) The model presented by Wen Liu addresses low-cost methodologies for the construction of indoor wireless fingerprint location databases. Fingerprint positioning has demonstrated considerable success in indoor localization applications; however, it often relies on a substantial quantity of fingerprint data to establish a reliable database. The quantity and diversity of this data significantly influence the effectiveness of the positioning system.

(e) The paper of Shinde S.P, Chingale R.R, Dhane D.C, Vader P.B discusses ATM machine security sensor using GSM and

MEMS sensor. Here when the movement of machine and the vibration is sensed using vibration and MEMS sensor, the buzzer produces a beep sound. DC Motor is used for closing the door. Smoke detector is used here to sense the gaseous or smoke near ATM machine.

3. PROPOSED SYSTEM

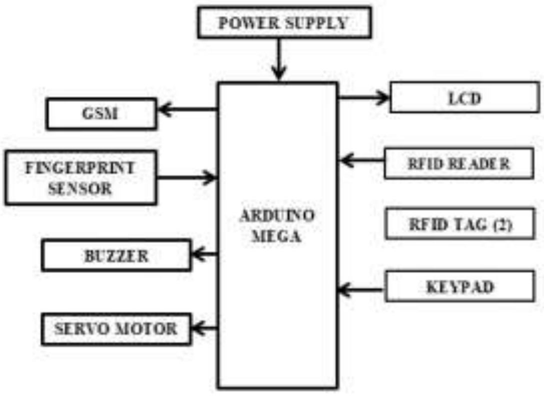


Fig. 1: Block Diagram

In the proposed method, the magnetic strip-based ATM card is replaced with RFID based card which have a unique number. The Arduino MEGA microcontroller is used to process the data from the sensor. The user can register the bank details and also withdraw the amount from the registered bank details. Hence this system provides more secure and multiple bank account using single ATM card.

A power supply of +5V is given to the circuit as an input. Arduino mega acts as a microcontroller that simultaneously stores data given to it. The ATM card consist of a magnetic strip containing a unique 12-digit number which acts as an RFID tag. This tag is read by a passive RFID reader (here EM-18 module) which is connected to the microcontroller through serial communication (UART). A 4x4 keypad is connected to the microcontroller that acts as an input to enter the 4-digit pin. Once the authenticity of the pin is confirmed the finger print of the user is verified using an optical fingerprint reader. The money is deposited or withdrew through servo motor that rotates 180 degree if the finger print matches the biometric data. On the other hand, if the finger print does not match, the buzzer starts ringing. Finally, irrespective of success or failure of the transaction a message or call is sent to the user through GSM module (SIM800L) which is 2G based network that uses AT commands.

4. RESULTS AND DISSCUSSIONS

The proposed scheme of MAASC (Multiple Account Access using Single ATM Card) provides the individual, the comfort of accessing users multiple accounts of different banks using a single card. Also, it provides the user one level higher convenience than the existing system.

Advantages of proposed system:

(a) Single ATM card provides more convince of using multiple bank transactions

(b) Higher security based on the biometric module

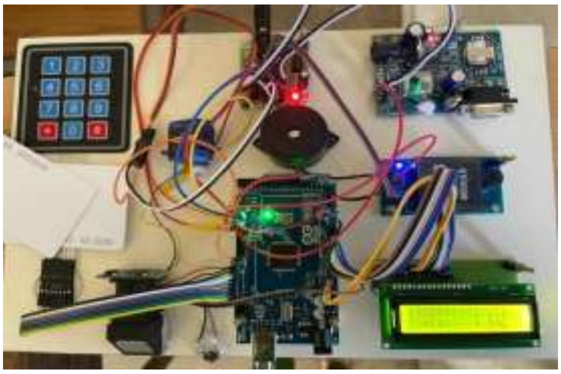


Figure 2: Hardware Implementation for multiple bank accounts using single ATM card

The below 9 figures shows the final outcome of proposed system which consist of Arduino Mega, RFID tag, RFID reader, GSM module, 16x2 LCD display, servo motor, keypad, buzzer and finger print sensor.

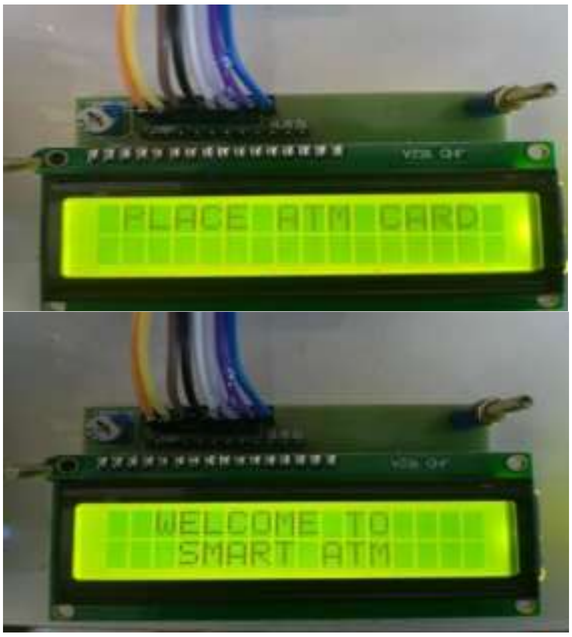
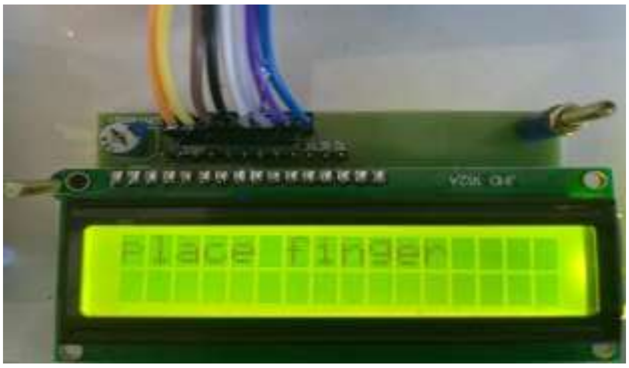


Figure 3: The RFID reader reads the ATM card having unique 12 digit



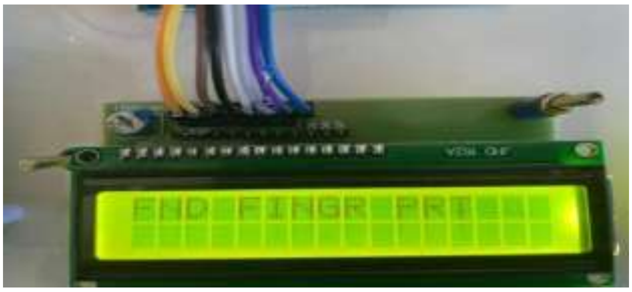


Figure 4: Finger print sensor is used to match with the database of the respective user

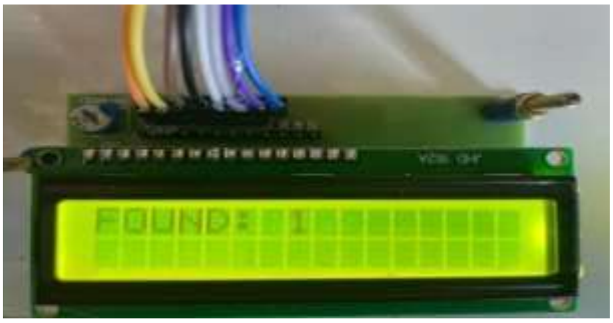


Figure 5: Account matched with the authorized user

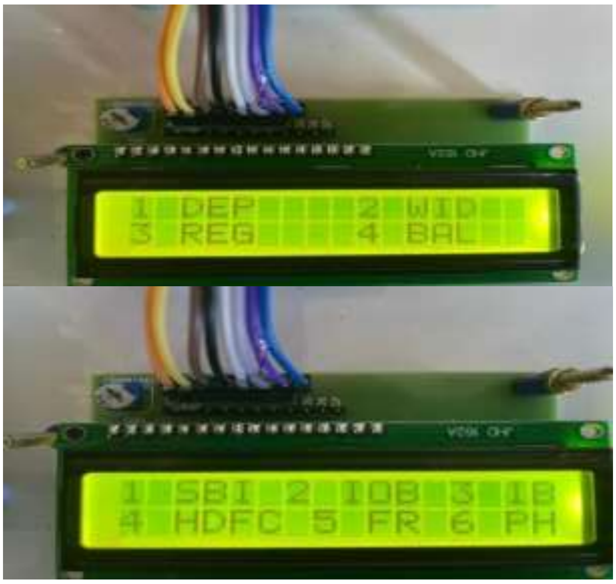


Figure 6 : Menus Displayed in LCD

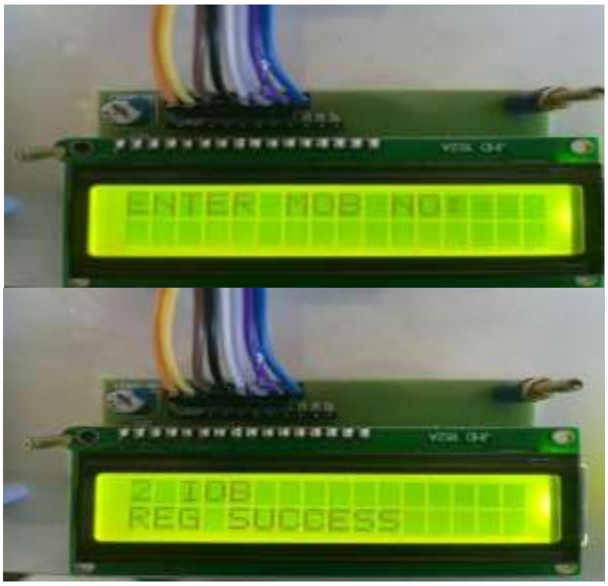


Figure 7 : Mobile Number is Successfully registered after the user login

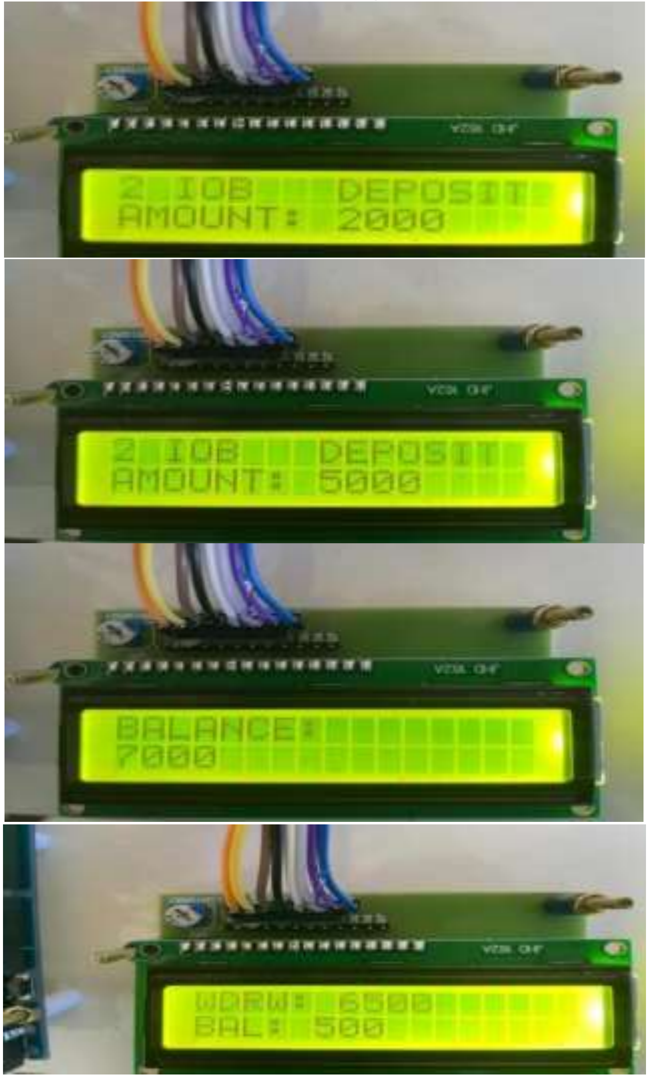


Figure 8 : Amount is deposited and withdrawn successfully

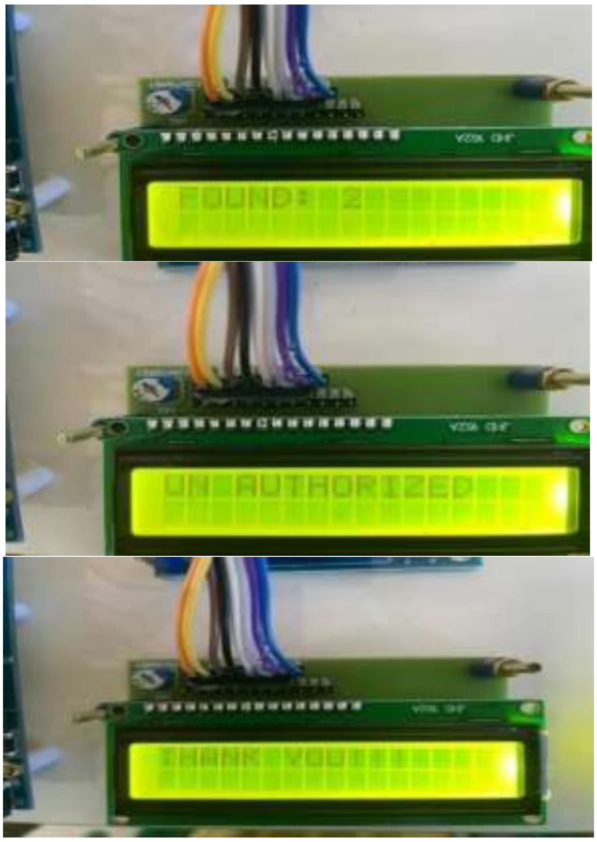
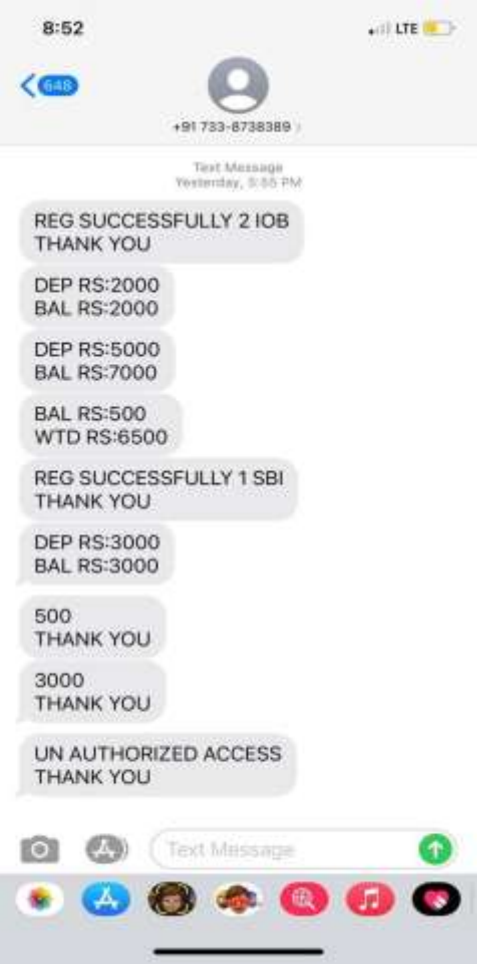


Figure 9 : If user is found unauthorised buzzer goes on..Finally, before logging out it shows "Thank you"


8:52

LTE

648

+91 733-8738389

Text Message
Yesterday, 5:55 PM

REG SUCCESSFULLY 2 IOB
THANK YOU

DEP RS:2000
BAL RS:2000

DEP RS:5000
BAL RS:7000

BAL RS:500
WTD RS:6500

REG SUCCESSFULLY 1 SBI
THANK YOU

DEP RS:3000
BAL RS:3000

500
THANK YOU

3000
THANK YOU

UN AUTHORIZED ACCESS
THANK YOU

Figure 10 : The GSM sends message to the registered mobile number

5. CONCLUSION

In this project, the user can manage his/her multiple accounts in various banks with the help of this single smart card ATM which provides easy access and reduces the complexity of managing more than one ATM card and their respective passwords. Here we provided the user with biometrics in order to create a viable method of identifying user's sufficient security level for the ATM system. The security features were enhanced largely for the stability and reliability of the owner's recognition. The whole system is built on the technology of embedded system which makes the system safe, reliable and easy to implement.
Hence the vulnerabilities of the ATM fraud are reduced.

6. REFERENCES

[1] S. Fox. (2013). 51% of US Adults Bank Online. Pew Research Center Washington, DC, USA. Accessed: Feb. 24, 2019. [Online]. Available: https://core.ac.uk/download/pdf/71362506.pdf

[2] S. Ahmad, "Demonetization-its impact on banking online transactions," Sumedha J. Manag., vol. 6, no. 3, pp. 4–15, 2017. [Online]. Available: http://search.proquest.com/openview/80b340c087f8285fb81ec91b55e13 64a/1?pq-origsite=gscholar&cbl=1936345

[3] H. A. Abdeljaber, "Automatic Arabic short answers scoring using longest common subsequence and Arabic WordNet," IEEE Access, vol. 9, pp. 76433–76445, 2021.

[4] N. A. Karim, Z. Shukur, and A. M. Al-Banna, "UIPA: User authentication method based on user interface preferences for account recovery process," J. Inf. Secur. Appl., vol. 52, Jun. 2020, Art. no. 102466

. [5] N. Harini and T. Padmanabhan, "2CAuth: A new two factor authentication scheme using QR-code," Int. J. Eng. Technol., vol. 5, no. 2, pp. 1087–1094, 2013. [Online]. Available: http://citeseerx.ist. psu.edu/viewdoc/download?doi=10.1.1.411.9555&rep=rep1&type=pdf

[6] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication:

A survey," Cryptography, vol. 2, no. 1, pp. 1–22, Jan. 2018.

[7] N. A. Karim, H. Kanaker, S. Almasadeh, and J. Zarqou, "A robust user authentication technique in online examination," Int. J. Comput., vol. 20, no. 4, pp. 535–542, Dec. 2021.

[8] N. A. Karim and Z. Shukur, "Using preferences as user identification in the online examination," Int. J. Adv. Sci., Eng. Inf. Technol., vol. 6, no. 6, p. 1026, Dec. 2016.

[9] M. K. Normalini and T. Ramayah, "A proposed biometrics technologies implementation in Malaysia internet banking services," in Proc. 13th Eurasia Bus. Econ. Soc. Conf., vol. 1, 2015, pp. 79–87. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-15880-8_7

[10] E. Pakulova, A. Ryndin, and O. Basov, "Multi-path multimodal authentication system for remote information system," in Proc. 12th Int. Conf. Secur. Inf. Netw., Sep. 2019, pp. 1–4, doi: 10.1145/3357613.3357640.