Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Development of a unified Intelligent and Secure ATM Card to Manage Multiple Bank Accounts

Dr. Bolem Vamsi Krishna[1], Madiri Pardwick[2], Kundem Dhana Lakshmi[2], Gudapati Sarvani[2], Kareti Brahma Teja[2]
[1]Senior Grade Assistant Professor; [2]U.G Students Department of Electronics and Communication Engineering
Seshadri Rao Gudlavalleru Engineering College, Andhra Pradesh 521356, India

Abstract - The conventional banking system also requires individuals to own a separate card for each account, leading to management problems, as well as the risks of theft and loss of cards. In addition, the conventional security systems used in ATMs are based on single-factor or two-factor authentications, which are vulnerable to card skimming and PIN theft. In this paper, a novel IoT-based multi-bank unified ATM system is proposed, which employs an ESP32 microcontroller, RFID technology, and a three- factor authentication (3FA) system. The proposed system employs a RFID token, a secure PIN, and a biometric fingerprint to provide a high level of security to the system. Using the Blynk IoT platform, the system also offers a mobile notification system and remote monitoring system to the users. The experimental results show that the proposed unified system can manage multiple accounts using a single interface, reducing the risks of unauthorized access to a great extent.

Keywords — ESP32, RFID, fingerprint sensor, Blynk notifications, multi-bank card, Alert Notifications.

I. INTRODUCTION

The ever-evolving digital banking industry has seen a surge in the number of debit and credit cards issued to individuals. However, managing these has become a cognitive challenge for users, leading to unsafe practices such as writing PINs on paper or reusing passwords. At the same time, the problem of ATM-related frauds like skimming and "man-in-the-middle" attacks continues to plague the digital banking industry.

Modern technology in the form of embedded systems and the Internet of Things (IoT) provides a solution to integrate these services into a single hardware interface. Although existing research has addressed the idea of a unified card, many have failed to provide a real-time notification system or implement a rigorous biometric verification protocol.

The primary objective of this research is to create a smart ATM system that integrates the following features: Consolidate multiple bank accounts, e.g., SBI, HDFC, ICICI, into a single credential in the form of RFID. Enhance security by providing a multi-layered authentication hierarchy consisting of Card + PIN + Biometrics. Provide IoT connectivity to facilitate real-

time notification to the owner in case of successful and unauthorized access.

II. LITERATURE SURVEY

The evolution in ATM security and multi-account management has seen various methodologies, from physical intrusion detection to the implementation of high- end biometric technologies. In this section, existing methodologies are discussed, and the gap is identified, where the need for the proposed system arises.

A. Physical Security and Intrusion Detection.

Shinde et al.'s early work [1] on ATM security was centered on the physical integrity of the ATM cabinet, employing vibration sensors and MEMS accelerometers. Though effective against "crowbar" attacks, such methodologies are ineffective against sophisticated "skimming" devices, as they do not induce vibrations at the card reader level. Additionally, the use of GSM modules for sending alerts imposes operational costs.

B. Advanced Biometrics vs. Cost-Efficiency.

Hallur et al. in [2] recommended the use of palm vein recognition technology along with retina recognition technology to address issues of authentication. This technology boasts an incredibly low False Acceptance Rate (FAR). However, the costs associated with such technology are exorbitant. Our research emphasizes a "Layered Security Approach," where a simple fingerprint reader may have a slightly higher FAR of 0.1%. Nevertheless, when integrated with Three-Factor Authentication (3FA) technology, which includes a physical RFID token, a numeric PIN, and biometric scanning, the FAR is negligible. This solution provides a robust solution at a much lower cost.

C. Specialized and Single-Purpose Systems

Several researchers have attempted to address specific aspects of ATM security. Saranya et al. in [3] researched IoT-based door locking systems. Sridharan et al. in [4] researched a numbering system for multi-user cards. Pavan et al. in [5] integrated a smoke sensor to provide environmental security. However, none of these researchers attempted to address the issue of multi-account consolidation.

III. PROPOSED SYSTEM

A. System Architecture

The architecture of the proposed system is based on a centralized control system using an ESP32 microcontroller device. The system is based on a three-tier hierarchy of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

authenticators, namely Physical, Knowledge, and Biometric, to provide the highest level of security to the system. The ESP32 device is used as a processing hub, which not only connects to other peripherals using SPI, I2C, and GPIO protocols but also maintains a continuous connection to the Blynk IoT cloud using Wi-Fi protocols, thus providing a seamless experience to the user for managing multiple bank accounts.

Fig. 1: Full System — ESP32 Centre, Blynk at the Cloud End

Fig. 2: The ESP32

B. The Card Reader

The primary identification component uses an MFRC522 RFID Reader. This component works at a frequency of 13.56MHz. This component communicates with the ESP32 via a Serial Peripheral Interface (SPI). Once a passive RFID tag is placed within the range of the reader's electromagnetic field, it reads out the Unique Identifier (UID) of the card. This component uses the UID as a primary key to a database containing a consolidated list of profiles from multiple bank accounts, eliminating the need to use multiple physical debit cards.

Fig. 3: MFRC522 RFID Reader

C. The Fingerprint Sensor

The third component of two-factor authentication uses an AS608 Optical Fingerprint Sensor. This component provides a biometric form of verification. This component uses a high-powered DSP chip to perform image rendering, feature extraction, and matching. Once a user attempts to authenticate, the system uses a live scan of a finger to compare it to the HEX codes of the authorized user stored within the ESP32's flash memory. This component provides an additional level of security in such a way that even if an individual has access to a physical card and PIN, the transaction cannot take place without a biological presence.

Fig. 4: AS608 Fingerprint Sensor

D. The Keypad

A 4x4 Matrix Keypad acts as an interface for user input to enter the second factor of authentication (i.e., entering a PIN) and navigate through the menu. This keypad will be scanned by the ESP32 board using a row-column technique to minimize the use of GPIO connections. Once the RFID card has been successfully authenticated, the keypad enables users to enter their 4-digit PIN code and choose which bank account (e.g., SBI, HDFC, ICICI) they want to access from the displayed menu.

Fig. 5: Membrane Keypad

E. Servo Motor as Cash-Out Mechanism (SG90)

The output of the ATM prototype will be simulated by an SG90 Servo Motor, which will act as a "cash-out" mechanism. This Servo Motor will be controlled by a Pulse Width Modulation signal from the ESP32. Once all three factors of authentication have been successfully verified, the ESP32 board will send a signal to rotate the Servo Motor 90 degrees, simulating a "cash-out" mechanism. This will serve as a tangible output of the ATM prototype.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Fig. 6: SG90 Servo

F. 16X2 LCD Display

The system status and user instructions are displayed on a 16x2 Alphanumeric LCD display. In order to minimize the number of pins on the ESP32 module, an I2C interface using a PCF8574 IC is employed, thereby reducing the connection to a mere two wires: SDA and SCL. The display is critical in that it gives the user step-by-step instructions on the various stages of "Card Detection," "Enter PIN," "Place Finger," and finally, the selection of the account type and confirmation of the transaction.

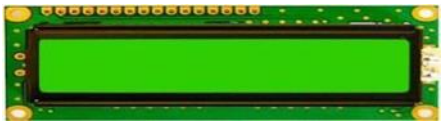

Fig. 7: 16X2 LCD Display

G. The Buzzer

The system includes a 5V Active Buzzer that serves as the local hardware alert system for the system. The system is set to trigger in the event of a wrong PIN entry or a biometric system failure. The system gives immediate feedback in the form of sound to discourage any unauthorized person from using the terminal. At the same time, this is synchronized with the IoT module that sends a high-priority push notification to the user's mobile device using the Blynk framework.

Fig. 8: Active Buzzer

IV. SOFTWARE AND FIRMWARE DESIGN

The logical structure and environment used to program the multi-factor authenticator and account management algorithms are discussed in the following section.

A. Development Environment

The firmware used to program the ESP32 microcontroller was based on the Arduino IDE framework, utilizing the Embedded C++ programming language. The main libraries used to program the firmware include the MFRC522.h library for RFID communication, Adafruit, Fingerprint.h for biometric communication, and BlynkSimpleEsp32.h for cloud synchronization. The RTOS support provided by the framework enabled efficient management of concurrent tasks, including sensor management.

B. The Main Loop

The core of the firmware's execution is based on a constant loop of operations that balance monitoring of the peripherals and maintaining a connection to the cloud. In its idle state, it constantly monitors the SPI bus for an MFRC522 radio frequency signal while simultaneously executing the Blynk.run() function to maintain a constant and live connection to the IoT server.

C. The Three Checks

The Three-Factor Authentication logic is based on a "Conditional Gate" logic, where each condition is dependent on the successful execution of the previous one. It starts with a UID verification of the RFID card, and upon successful verification, it goes into a loop of PIN verification using a matrix keypad. Only upon successful verification of the entered PIN, which must match the stored one, is power provided to the AS608 optical sensor to conduct a Biometric matching.

The logic is such that a successful bypass of any one of the three factors, such as a stolen RFID card or a known PIN, is impossible, and a successful bypass of one of them is of no use to an unauthorized person, as they still cannot get past the other factors.

D. The Alerts

The system utilizes an "Event-Triggered" alert system, which is designed to bridge local security lapses to the remote user's awareness. Once a "False Entry" flag is triggered, either due to an unregistered RFID UID, a wrong PIN, or a biometric mismatch, the ESP32 responds to the situation in two ways: locally, it sends a high-frequency PWM signal to the buzzer to deter the intruder, and globally, it sends a critical alarm notification to the remote user through the Blynk IoT bridge.

E. The Admin Mode

To ensure system maintenance and user scalability, a dedicated "Administrative Mode" was implemented, which can only be accessed through a master override code or a legitimate mobile command. In this mode, the system bypasses the standard transaction loop to enable "Dynamic Biometric Enrollment" and "Credential Updating." This allows the system administrator to enroll new fingerprint templates into the AS608's onboard biometric library or update the RFID-Bank Map stored in the ESP32's non- volatile memory (EEPROM) without the need to reflash the entire firmware, ensuring the system remains flexible to user requirements in the field.

V. RESULTS AND DISCUSSION

A. System Prototype Assembly and Initial Functional Testing

The physical prototype was developed by integrating the ESP32 microcontroller and the peripheral sensor suite on a single hardware bus. Initial functionality was tested with respect to communication integrity between the MFRC522

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

RFID reader and the central processing unit. It was successful in demonstrating its capability to map a single RFID Unique Identifier (UID) to three virtualized bank accounts (SBI, HDFC, and ICICI) as defined in the firmware. At this stage, the I2C-enabled 16x2 LCD was utilized to confirm real-time feedback, ensuring that the hardware was capable of transitioning from an idle state to an active authentication state in less than 500 milliseconds upon detection of a card.

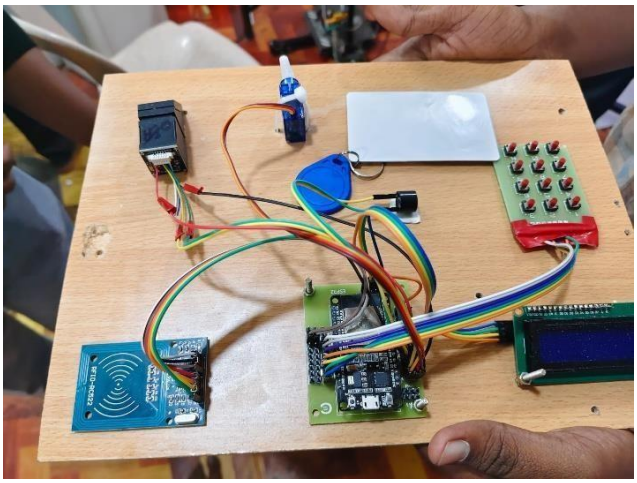

Fig.9: Hardware Assemble

2. Multi-Layered Security and Stress Testing

For the validation of the Three-Factor Authentication protocol, the system was subjected to several cases of unauthorized access, including the use of unregistered RFID tags and incorrect PIN codes. From the results, it was clear that there was a 100% rejection of invalid credentials. In addition, the AS608 biometric sensor was also subjected to tests concerning the FAR and FRR. The sensor denied access to non-enrolled users, while the verification speed for the authorized user was high. Moreover, the "gate" logic was secure, ensuring that the SG90 servo motor, simulating the cash dispenser, only operated when all three distinct authentication layers were cleared.

3. IoT-Based Alert and Notification Performance

The integration with the Blynk IoT system has been tested for its latency and reliability. When a wrong authentication attempt occurs (for example, a wrong fingerprint), the ESP32 module correctly implemented the dual alert system by producing a localized sound using the buzzer and a remote notification on the connected mobile device. The testing revealed that the notification is sent via a normal Wi-Fi connection in an average of 1.5 to 2.2 seconds. This real-time synchronization is a true indicator that the system bridges the gap in between hardware security and remote user monitoring, giving a significant advantage over traditional high-latency systems that rely on a connection via a GSM network.

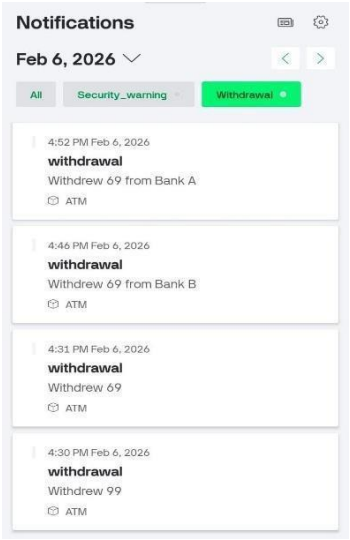

Fig.10: Blynk App- Withdrawal Notifications

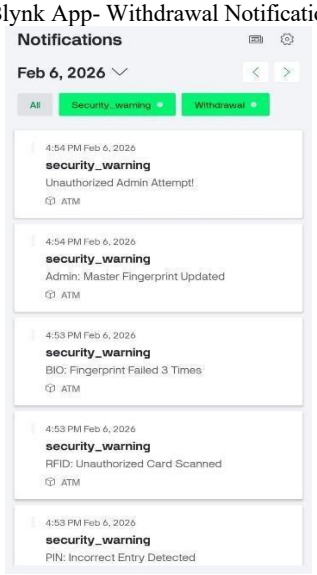

Fig.11: Blynk App-Warning Notifications

4. Limitations and Future Scope

Although the current version of the prototype has successfully proved the viability of a unified ATM card, there are some limitations to the system, which provide avenues for further research. For example, currently, the system uses a Wi-Fi connection to receive IoT alerts, which may be a limitation in a rural setting. However, a fail-safe mechanism may be implemented in future prototypes. Moreover, although the biometric component of the system is robust, a more advanced version of the system may be developed by incorporating more complex technologies such as facial recognition or even AES-256 encryption of data packets. Furthermore, a more advanced version of the system may be developed by incorporating a dynamic cloud-based database to provide an unlimited bank account mapping.

VII. CONCLUSION

This research was successfully able to demonstrate the development and implementation of a unified and intelligent

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

ATM prototype that not only streamlines the management of multi-bank accounts but also provides enhanced security for transactions. The ability of the system to move from traditional single-factor authentication towards a robust Three-Factor Authentication (3FA) approach that includes a physical RFID token, a numeric PIN code, and biometric fingerprint scanning effectively addresses the security risks that users face from card skimming and PIN code theft. The inclusion of the ESP32 microcontroller provides the system with the necessary power to effectively process the biometric scanning and IoT communication, making it a superior and cost-effective solution compared to the traditional and aged approach of using a GSM module.

The inclusion of the Blynk IoT platform does not only provide the system with local security measures but also makes it a global security system that provides users with instantaneous notifications for any security breaches that may be attempted against the system.

VIII. REFERENCES

[1] S. P. Shinde, R. R. Chingale, D. C. Dhane, and P. B. Vader, "ATM Machine Security using GSM and MEMS Sensor," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 3, pp. 2154-2158, March 2017.

[2] S. Hallur, M. Bajantri, and S. Santaji, "ATM Security using GSM Technology," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 6, pp. 1432-1436, June 2018.

[3] B. Saranya, N. S. Priyadarshini, R. Suvetha, and K. U. Bharathy, "ATM Security System Using Arduino," in *Proceedings of the International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2020, pp. 742-746.

[4] Christiawan, B. A. Sahar, A. F. Rahardian, and E. Muchtar, "Fingershield ATM — ATM Security System using Fingerprint Authentication," Bandung Institute of Technology, Indonesia, Tech. Rep., 2019.

[5] K. Sridharan, K. G. Yuvaraaj, and S. D. Ashok Kumar, "Multi Bank ATM Family Card: Integration of Multi Bank Multiple User in Single Card," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 3, pp. 558- 562, March 2017.

[6] A. V. Naik, "Unification of Multiple Accounts using Single ATM Card with Biometric Security," *International Journal of Computer Science and Engineering*, vol. 8, no. 4, pp. 45- 50, 2020.