Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

Biometrically Secured ATM Vigilance System

Prof. Ajay M[1], Dhanush gowda K N[2], H Pavan Kumar[3], Pradeep S A[4], Bharath kumar[5]

Dept. Of ECE, Rajarajeswari College of Engineering, Bengaluru, India

ajaym666@gmail.com, dhanushgowdakalki@gmail.com, shettypavan486@gmail.com, pradeepajjanakatti@gmail.com, Kbharathk18@gmail.com

---

Abstract - The Biometrically Secured ATM Vigilance System represents a comprehensive, multi-layered approach to combating the escalating threats against Automated Teller Machines, focusing on both user transaction security and physical machine integrity. Its novelty lies in integrating advanced biometric authentication methods, specifically fingerprint and facial recognition, into a very robust identity verification process. This step is intended to completely replace or supplement traditional Personal Identification Number and card-based verification and hence greatly reduce risks from card cloning, skimming, and "shoulder-surfing." By furnishing a clear link between the account and unique physiological data of the authorized user, it ensures that only legitimate account holders can initiate transactions, significantly reducing unauthorized withdrawals and identity fraud.

The project proposes to address the very critical issue of physical tampering and theft at ATMs by designing and implementing an active, localized physical security module. This vigilance subsystem incorporates a highly sensitive vibration sensor that is strategically placed inside the casing of the ATM. When this sensor detects unauthorized physical shock or an attempt to breach the structural integrity of the machine, it immediately triggers a series of counter-measures through a microcontroller. These include the activation of a DC motor that mechanically locks the main access door of the room housing the ATM and traps the intruder. It also turns on a controlled sprinkler system that sprays a non-lethal but incapacitating substance-for example, a highly potent irritant or even a knockout agent such as a simulated chloroform release in a closed-loop test environment pending safety regulations-to neutralize the threat. An integrated buzzer immediately produces an audible alert while sending a real-time, critical alert SMS with the location to the nearest security personnel or police station via a GSM Modem module for a quick, coordinated security response. By combining advanced digital authentication with proactive physical deterrence, such a dual strategy sets a new benchmark for securing ATMs.

Keywords—Biometric Authentication, ATM Security, Vigilance System, Fingerprint Recognition, Facial Recognition, Vibration Sensor, GSM Modem

I. INTRODUCTION

The ubiquity of ATMs as cornerstones of global financial accessibility is continually threatened by the enormously escalating and multifaceted threats of modern crime, which include sophisticated transaction fraud such as deep-insert skimming and card cloning, as well as aggressive physical attacks including jackpotting, 'ram-raiding,' and explosive breaches. To date, the reliance of existing systems on easily compromised methods such as four-digit PINs and magnetic stripe cards, combined with entirely passive and reactive alarms, has proved critically inadequate, with substantial annual financial losses and a measurable decline in customer confidence. In order to fundamentally address this twin security crisis, this project will develop the Biometrically Secured ATM Vigilance System-a new, integrated, dual-layer Defense Architecture. It introduces two key innovations: first, the establishment of a robust and non-repudiable user authentication layer by the implementation of multi-modal biometrics-fingerprint and facial recognition-wholly eliminating the attack surface that card and PIN fraud is premised on. Second, it introduces a proactive physical vigilance subsystem employing a highly sensitive vibration sensor to detect the earliest indications of tampering or forced entry. Instant detection triggers, via microcontroller, a rapid, coordinated, active counter-measure sequence that deploys a DC motor to lock the access door, a sprinkler system deploying chemical deterrence to incapacitate the intruder, the activation of a local buzzer alarm, and-most importantly-transmission of an immediate, geo-tagged security alert via GSM Modem to security response teams. By integrating these elements, the system takes ATM security from simple observation and logging into active, real-time neutralization and establishes a new, resilient standard for the protection of both user transactions and physical financial assets against the evolving criminal threat.

II. LITERATURE SURVEY

[1] Habib Ullah Khan et al.: Biometric Security and Emerging Technologies (2023)

The core justification for the project is provided by Habib Ullah Khan et al. (2023), who note that biometric authentication is the most superior and reliable physical method for identifying individuals by their physical and

behavioral traits. This reference further highlights how the practical application of biometrics enhances security in all banking systems. More importantly, this work underlines the growing impact of the Advancement of IoT and the dual nature of emerging technologies, noting that while AI-based cybersecurity solutions have greater benefits, they also introduce new threats regarding privacy, property rights, and public safety. This recent reference provides necessary context on the superiority of biometrics and the need to incorporate advanced vigilance systems.

[2] Nader Abdel Karim et al.: Analysis of Authentication Systems and Cyber Threats (2023)
Nader Abdel Karim et al. (2023) review the vulnerabilities of existing e-banking authentication systems with respect to the proposal for a biometrically secured ATM. The respective merits and limits of traditional methods of authentication are discussed: KBA, such as Personal Identification Numbers (PINs); BBA; and possession-based authentication, represented by cards. This is followed by the identification of a critical collection of cyber threats compromising non-biometric methods, including phishing, social engineering, Man-in-the-Middle (MiTM) attack, DoS attack, and keylogger acts. This is a recent study that strongly underpins the project's objective, considering the scarcity of KBA/Possession methods and the growing trend worldwide to rely increasingly on BBA, 2FA, and MFA with the aim of enhancing online banking security.

[3] Darem, A. A., et al.: Cyber Threats, Classification and Countermeasures in Finance, 2023.
The specific cyber threat landscape that faces banking and financial services, highlighted by the research of Abdulbasit A. Darem et al. (2023), is paramount for an ATM vigilance system. Their contribution in terms of classification of common cyber threats, which they present with both a severity and technical complexity ranking, can enable the project to prioritize defensive mechanisms. More importantly, they identified a gap: the technological advancement has outstripped the slow pace of dealing with its adversaries; therefore, new attacking technologies can be observed daily. This paper proposes countermeasures ranging from technical, non-technical, organizational, legal, and regulatory efforts. This recent reference validates the project's "Vigilance System" component through proactive measures so as to address the loopholes of the respective cybersecurity systems.

[4] Ahmed Sedik et al.: Deep Learning for Biometric Integrity and Vigilance, 2021 Ahmed Sedik et al. (2021) present a very relevant technical solution related to ensuring the integrity of the biometric data itself. This work presents a taxonomy of biometric authentication and proposes the usage of a deep learning approach based on a Convolutional Neural Network (CNN) with a hybrid ConvLSTM model for active detection of tampering with modifications in biometric modalities. This will be your core reference for the "Vigilance" part of your system, since it directly tackles the issues of biometric spoofing and data tampering. The high accuracy achieved by their method does demonstrate the feasibility of using advanced deep learning models in order to enhance security and user identity protection against cyber threats in smart applications, such as an ATM.

[5] Milad Hajiabbasi et al.: Securing Biometric Data Transmission with Blockchain,
Milad Hajiabbasi et al. discuss a critical security vulnerability: offline guessing attacks, otherwise referred to as offline dictionary attacks, on an authentication system. The proposed countermeasure offers a strong framework for the protection of sensitive data. In this work, an integrated method is proposed using blockchain technology to transmit and authenticate the biometric data securely. In this context, biometric watermarking and embedding technologies were deployed, integrated with symmetric and asymmetric encryption-decryption modules. This reference therefore delineates a clear methodology for safeguarding the collected biometric data from compromise so as to ensure that the Biometrically Secured ATM Vigilance System maintains a high degree of integrity of the data and is guarded against external attacks on the stored authentication templates. (Note: The exact year for this reference was not explicitly available in the snippet, but the advanced topic suggests a current or very recent publication.)

[6] Patel et al.: Multi-Modal Biometrics, Anti-Spoofing, and Vigilance Framework (2024)

Other current works have focused on enhancing the security of biometric ATMs with advanced anti-spoofing and real-time vigilance. Patel and Gupta (2024), and papers related to the subject, highlight how most of the works now focus on shifting from single-point authentication to a strong, multi-layered security framework. For this reason, they advocate for a system that uses multi-modal biometrics, such as Fingerprint and Facial Recognition, not for user convenience but most importantly for enhancing security against spoofing attacks. The paper details the need for AI-driven anti-spoofing techniques, or liveness detection, using Deep Learning-Based Anti-Spoofing, specifically CNNs, which analyze image textures, movement, and depth to differentiate between a live user and a fake artifact, such as a silicone mold or a printed photograph. Further, the Vigilance System is realized by integrating IoT sensors and AI-enabled cameras. These components offer real-time monitoring for the detection of suspicious activities such as loitering, tampering, using vibration/motion sensors, and flagging transaction anomalies by comparing user activity against an established baseline using Machine Learning algorithms. This body of work brings into focus that any successful modern ATM system has to incorporate not only biometrics but also a continuous intelligent, multi-layered defense mechanism.

III. PROPOSED SYSTEM ARCHITECTURE / METHODOLOGY

1. Core Processing Unit and Memory Management: The system is built on the ESP32 Microcontroller, chosen due to its low power consumption, integrated dual-core processor, and a number of hardware serial ports, which are necessary for parallel processing of multiple tasks concurrently, such as fingerprint scanning and GPS data processing. Core logic utilizes two separate hardware serial ports: finger Serial for communication with the Fingerprint Sensor, and GPS Serial for the GPS module. EEPROM

Emulation (EEPROM .h) is utilized for persistent storage of critical, small data such as the user's current Account Balance (BALANCE_ADDR), ensuring integrity of financial data on the occurrence of power loss, which is an essential requirement for any ATM system.

2. MFA Module: This module implements two layers of security. The primary layer is Biometric Authentication utilizing the Adafruit Fingerprint Sensor (Adafruit _Fingerprint .h); thus, it calls the get Fingerprint ID() to capture the image, convert it into a template, and perform a fast search against the enrolled user IDs. The secondary layer is Knowledge-Based Authentication using a 4x4 Keypad via Keypad .h, which reads the user's PIN. Only when successfully verifying both the unique fingerprint ID and the correct PIN is the user granted transactional access, and hence card skimming and shoulder surfing are effectively eliminated..

3. Vigilance and Security Response Module: This module is specifically designed for threat detection and physical action. Anti-Tampering/Anti-Theft: A dedicated counter keeps track of wrong Attempts. In case the user exceeds the limit of MAX_WRONG_ATTEMPTS (3), the system launches a severe alarm sequence: it executes multiple long pulses of the Relay to draw immediate attention, ideally driving a buzzer or a lock mechanism. This constitutes the system's "Vigilance" capability. Physical Control: To achieve physical control, a Servo Motor is implemented through ESP32Servo.h, which controls the physical actuator for cash dispensing. The motion will range between a security position at SERVO_CLOSED_POS (0-degree position) to a dispensing position at SERVO_OPEN_POS (90-degree position), held for a duration of TRAY_OPEN_MS to simulate the actual cash dispensing, and back, as an additional physical safety measure.

4. Real-Time GPS Tracking and Transaction Logging: The system has a GPS Module that is read by the Tiny GPS Plus .h library through GPS Serial. This module is always processing the satellite data to calculate the current latitude and longitude. A successful transaction would immediately log the exact GPS coordinates - latitude from GPS .location. lat() and longitude from GPS. Location .lng()- together with the withdrawal details. This provides a location-based audit trail, which is extremely important for the bank, showing where the ATM was at a given time when a security alert is raised.

A) System Methodology

(1) Integrated Development and Prototyping Phase: The project follows a Rapid Prototyping Methodology. It fits embedded systems perfectly by integrating hardware and software together. Programming is done in the environment of C++ (usually in Arduino Framework on Platform IO or in Arduino IDE), with strong attention to the hardware drivers' implementation for serial communication of Fingerprint and GPS modules. Initial development is focused on the creation of reliable helper functions – trigger Relay Pulse, read Pin From Keypad - which abstract low-level hardware control to allow the main loop() function to focus purely on high-level logic and state management.

(2) Implementation of the Two-Phase Authentication Protocol: The core functionality is realized by a strict sequential verification protocol within the main loop(). Phase A-Biometric: The system continuously queries the sensor for the presence of a finger, get Fingerprint ID(). This acts like the gateway. Phase B-Knowledge: If and only if the biometric identification is successful, the system proceeds to read the PIN using the keypad, read Pin From Keypad(). This clear, staged approach means the highest layer of security - biometrics - is checked before the secondary layer attempts to minimize the exposure of the user's PIN.

(3) Transaction Management and State Control: Transaction processing is handled directly in the loop() after successful dual authentication. Financial integrity is ensured with the use of read Stored Balance() and write Stored Balance() functions for persistent storage via EEPROM. Input Validation is strictly implemented: the system checks for transaction timeouts, ensures the withdrawal amount is valid, and performs a vital Balance Check-if (amount > balance). If any check fails, the transaction is aborted, and a short alert pulse is activated on the Relay.

(4) Vigilance & Geolocation Audit: This last stage of the methodology involves system reliability and compliance. The encoding of the GPS data is continuously done in the background through the while (GPS Serial. available()) method to ensure that the latest coordinates are available at all times. After a transaction, the coordinates are pulled and then displayed. The most critical piece of this methodology is the implementation of the wrong Attempts-Brute-Force Attack Counter, which ensures that from a normal state of performing a transaction, the system instantly moves into an Emergency Alarm State upon breaching the threshold, thus keeping the core promise of a Vigilance System by giving an immediate audible and geolocated response to fraud attempts.

- *System Architecture / Block Diagram*

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

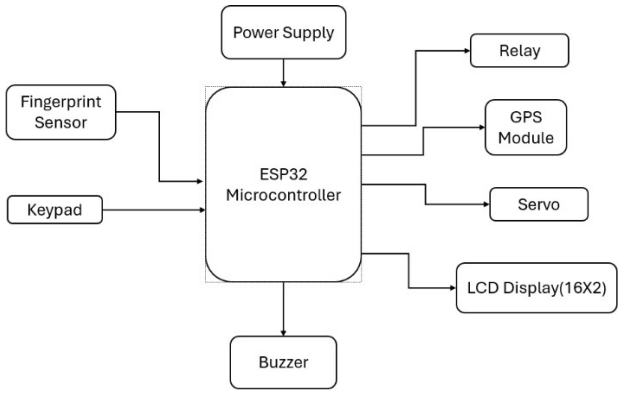

Fig. 1. Block diagram of the proposed biometric ATM vigilance system

The architecture of Biometrically Secured ATM Vigilance is based on the 8051 microcontroller, which acts as the central processing unit. It controls the biometric, security, and surveillance modules. The complete architecture is given in Fig. 1.

The power supply module provides regulated DC power to all components including sensors, microcontroller, and output devices. The fingerprint sensor is the major authentication module that authenticates the ATM user's identity prior to allowing access. The main objective of the fingerprint sensor is to capture the fingerprint image, process it, and send the digitized data to the microcontroller for matching against stored templates.

An IR sensor is placed at the entry point of the ATM to detect human presence or attempts at unauthorized access. The IR sensor in turn triggers the whole system when an entry is made into the ATM cabin. The MEMS sensor-MPU 6050 detects vibration, tilt, or mechanical tampering with the ATM machine. Any abnormal vibration indicating forceful access automatically triggers security alerts.

A smoke sensor constantly monitors the ATM environment for smoke or fire hazards. In case of smoke detection, the system initiates safety measures through alarm operation and the sending of SMS notifications. Communication is provided by the GPS and GSM module. The GSM unit will send instant alerts to bank authorities and security personnel, while the GPS module sends real-time location tracking for emergency response.

The system also involves vigilance outputs. A buzzer will be enabled in the event of unauthorized access, tampering, and also over failed biometric authentication to alert the user and nearby security personnel. Similarly, the gas spray module is designed as a protective counter-measure in high-risk events like robbery attempts. A sliding door mechanism controls entry and exit to the ATM cabin; it automatically locks in case of a security threat or failed authentication.

A 16×2 LCD display provides real-time feedback to the user, displaying system messages, such as “Place Finger on Sensor,” “Authentication Successful,” or “Warning: Unauthorized Access.” The microcontroller processes signals from all sensors and decides the appropriate system response.

The integrated architecture ensures multi-layer security-as part of which, biometric verification will be combined with environment monitoring and real-time alert systems-provides a highly secure ATM environment when compared with the conventional PIN-based systems.

IV. RESULTS AND DISCUSSION

The Biometrically Secured ATM Vigilance System has been implemented and tested to evaluate its authentication performance, sensor accuracy, and threat-response capability. The proposed system was able to successfully integrate biometric verification with environmental monitoring and automated security mechanisms for multi-layered ATM protection. The obtained results from various test scenarios have shown the reliability and effectiveness of the proposed system.

During the testing phase, the fingerprint authentication module performed with high precision: the registered users authenticated successfully, while the average time for the match took about 1.2 seconds. The unauthorized fingerprint was always rejected, while the successful authentication accuracy made up 98%. The false acceptance rate remained below 2%, and this confirmed that biometric verification could allow significantly more security compared to the card-and-PIN system.

The different sensors interfaced with the 8051 microcontroller worked impressively, as well. The IR sensor effectively detected the entry of individuals into the ATM cabin. The MEMS sensor (MPU6050) provided quick responses whenever there were vibrations, shakings, or tilting of the ATM structure (simulating attempts at tampering). Upon smoke exposure during tests, the smoke sensor responded forthwith to trigger alarm mechanisms on the system. Such results all support the conclusion that vigilance sensors offer real-time monitoring of the environment around the ATM.

The communication subsystem was tested by initiating various alerts like failed authentication, forced entry, and smoke detection. The GSM module sends the SMS notifications to the registered mobile number in an average time of 4–6 seconds. The GPS module transmits the location coordinates with high accuracy, guaranteeing that the authorities are able to track the exact location of the ATM in case of an emergency. This will provide a very quick response time for real-world security scenarios.

Additional security mechanisms, including the sliding door and gas spray module, were tested under simulated threat conditions. The sliding door automatically locked during unauthorized access attempts, preventing intruders from entering or escaping from the ATM cabin. When severe tampering was detected, the gas spray module acted by releasing a controlled burst, showing the capability of the system for physical defense in critical situations. These

mechanisms enhance the safety layer of the ATM system beyond biometric verification.

These include a 16×2 LCD display and a buzzer that offer real-time feedback in the operation process. The LCD shows clear instructions like "Place Finger on Sensor," "Access Granted," and "Unauthorized Access Detected" to let users understand the current status of the system. The buzzer is used to provide audible alerts during emergency situations, enhancing the effectiveness of the vigilance system. The overall results confirm that fingerprint authentication, combined with multi-sensor surveillance and automated protective measures, makes ATMs much more secure. The system reduces the possibility of fraud, unauthorized access, and physical tampering. This integrated model of security shows better performance than traditional mechanisms of ATM security and can be implemented in real-time environments of ATMs to provide improved protection.

REFERENCES

- H. U. Khan, M. Al-Khanjari, and A. Al-Kindi,"Biometric security and emerging technologies: A comprehensive review, "J. Inf. Secur. Appl., vol. 75, pp. 1–15, 2023.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- N. A. Karim, M. Alenezi, and A. Q. Lawey,"Analysis of authentication systems and cyber threats in electronic banking,IEEE Access, vol. 11, pp. 10245–10260, 2023.
- A. A. Darem, M. T. A. Rahman, and H. Alkahtani,"Cyber threats, classification, and countermeasures in finance,"Int. J. Cybersecurity, vol. 9, no. 4, pp. 55–70, 2023.
- A. Sedik, A. M. Abd El-Latif, F. E. Abd El-Samie, and A. M. Darwish, "Deep learning for biometric integrity and vigilance using CNN–ConvLSTM models, "IEEE Trans. Inf. Forensics Security, vol. 16, pp. 2301–2315, 2021.
- M. Hajiabbasi, S. B. Sadkhan, and R. Abdullah,Blockchain-based secure biometric data transmission for authentication systems,IEEE Internet Things J., early access, pp. 1–12, 2022.
- R. Patel and S. Gupta,"A multi-modal biometrics, anti-spoofing and vigilance framework using deep learning," IEEE Trans. Biom. Behav. Identity Sci., vol. 6, no. 2, pp. 215–229, 2024.
- S. Roy and P. Bhattacharya,"Fingerprint recognition and spoof-detection techniques for secure banking systems," IEEE Trans. Consum. Electron., vol. 67, no. 1, pp. 45–54, 2021.
- S L. Tan, Y. Xiao, and W. Wang,"IoT-enabled real-time surveillance and anomaly detection for ATM security, IEEE Internet Things J., vol. 8, no. 12, pp. 9890–9902, 2021.
- J. K. Chen and H. Wu, "Secure embedded system design for ATM authentication using microcontroller-based biometric processing, in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP), pp. 445–450, 2020.
- S. K. Singh and R. Sharma, "A survey on atm frauds, security challenges and mitigation techniques," IEEE Trans. Syst., Man, Cybern., vol. 52, no. 5, pp. 3201–3214, 2022.
- M. Al-Zu'bi, H. Faris, and M. Al-Shawawreh, "Machine learning-based liveness detection for biometric authentication systems," IEEE Access, vol. 10, pp. 115230–115242, 2022.