International Current Journal of Engineering and Science (ICJES)
Volume 4, Issue 4, pp 7-17, April-2025
ISSN (Online): 2583-7257
Article DOI: https://doi.org/10.47001/ICJES/2025.404002

Intelligent Anti-Robberry Door Lock System for Secure ATMs

[1]B. Sapthagiri, [2]V.K. Sreedhar, [3]N. Sangeetha Reddy, [4]P. Mohammed Shahid Khan, [5]K. Seshu, [6]T. Shaik Sabiya

[1,3,4,5,6]UG Student, Dept. of E.C.E., Gates Institute of Technology, Gooty,Anathapur (Dist), Andhra Pradesh, India
[2]Assistant Professor, Dept. of E.C.E., Gates Institute of Technology, Gooty, Anathapur(Dist), Andhra Pradesh, India
E-mail: ssapta028@gmail.com, sreedhar.v.k@gmail.com, sangeethareddynetturu9@gmail.com, yoyoshahidkhan99@gmail.com, seshuram143@gmail.com, sabiyat954@gmail.com

***Abstract* - This study presents an advanced ATM security system integrating MEMS sensors, vibration sensors, RFID card access, automated actions, and a mobile application to reduce ATM robberies. The system detects unauthorized movement and tampering using MEMS and vibration sensors, triggering actions such as locking the ATM door, releasing incapacitating gas, and capturing photographic evidence via an ESP Cam. Additionally, an RFID card system restricts access to authorized personnel, enhancing security. The mobile app serves as the central hub for real-time monitoring, notifications, and remote control of security measures. This integrated approach enhances ATM protection, enabling swift responses to threats and minimizing the risk of theft without the need for physical guards.**

Keywords: Automated Teller Machine, Robbery detection, Mobile Application, Solenoid lock, RFID Cards, Security measures.

I. INTRODUCTION

Automatic Teller Machines (ATMs) are widely used for a variety of banking services, particularly cash withdrawals, making them essential to modern financial systems[1]. However, their widespread availability and often limited physical security make them attractive targets for theft and vandalism[2]. ATM-related crimes, such as robberies, fraud, and tampering, have become increasingly prevalent, posing significant risks to both users and financial institutions[3]. Traditional security measures, such as the presence of guards or the installation of basic surveillance cameras, are often insufficient to fully protect ATMs and respond quickly in emergency situations[4]. This has led to the need for more advanced, automated security systems capable of detecting threats in real time and responding appropriately to mitigate risks[5].

This study proposes an innovative ATM security system that integrates multiple technologies to address these vulnerabilities[6]. The system uses MEMS and vibration sensors to detect unauthorized movement or tampering with the ATM[7]. When suspicious activity is detected, the system sends this data to an Arduino processor, which triggers automated actions, such as locking the ATM room door with a DC motor, releasing incapacitating gas to neutralize the intruder, and capturing photographic evidence using an ESP Cam[8]. Furthermore, the system incorporates an RFID card access mechanism to ensure that only authorized personnel can interact with the ATM’s security system, adding an additional layer of protection[9].

A key feature of this proposed system is the integration of a mobile application for real-time monitoring and control[10]. The mobile app serves as the central hub, allowing authorized bank staff or law enforcement to receive immediate notifications of any security breaches, monitor live video feeds from the ESP Cam, and remotely trigger security actions, such as locking the ATM or activating the gas release system[11]. This mobile-based control not only enhances response times but also makes it easier for authorities to coordinate and manage security incidents remotely[12].

By combining sensor technology, automated countermeasures, and a mobile app interface, the proposed system offers a comprehensive, flexible, and cost-effective solution to enhance ATM security[13]. It aims to reduce the frequency and impact of robberies, improve the speed and efficiency of response actions, and ensure the safety of both ATM users and financial institutions[14]. This innovative approach allows for a more secure and automated environment without the need for constant physical surveillance or guards[15].

II. LITERATURE REVIEW

A wireless mobile system has revolutionized the way customers perform financial transactions, especially cash withdrawals. In response to the growth of ATMs, over 3 million bank branches have been established globally[16]. Access to ATMs is generally facilitated through the use of a debit card with a magnetic stripe or a mobile app with a chip card that requires a unique PIN for authorization. Although this system is widely adopted, it lacks the high level of security provided by other technologies such as CVVC[17]. Authentication is typically achieved when the user enters their Personal Identification Number (PIN).

Despite these precautions, ATM thefts are still increasingly common. The vulnerable components of ATMs, such as the equipment attached to the machines, often become the target for thieves[18]. Even with security guards stationed at ATMs, criminals are able to carry out their heists using various techniques to circumvent the security measures[19]. This results in significant financial losses, amounting to millions or even crores of rupees, affecting both the banking sector and government resources[20].

In 2024,K. Sreenivasa Rao, SM. Mohammad Eliyas et al.[21] developed an Advanced Atm Security With Automatic Door Lock System Using Arduino Processor. The system uses GSM module to send messages and capturing the images.

In 2023, M. Nagabushanam et al. [22] developed an advanced system designed to respond to vibrations, which promptly closes the ATM door and triggers an alert. This system uses the ESP32 platform alongside Blynk IoT to deliver real-time alerts via the Blynk app. The audio signal is used to notify the surrounding area, while a custom Android application decodes the commands and controls the system. By integrating these technologies, they proposed a smart Internet of Things (IoT) solution aimed at enhancing ATM security. This system addresses security vulnerabilities in existing alarm and surveillance setups, offering a comprehensive solution to prevent thefts and ensuring timely responses to security incidents.

In 2020, K. Gavaskar, S. Preethi, et al. [23] introduced an IoT-based system designed to inform the local area in case of a physical attack on an ATM. The system sends sensor data to a mobile application that relays an alert to bank authorities, providing them with real-time information about the assault.

In 2018, Taha Ayesha et al. [24] proposed a solution using an embedded Linux platform that connects a Raspberry Pi with an RFID module, keypad, display, and USB camera to enhance ATM transaction security. The system provides continuous security measures, including using a GSM module to send SMS alerts to cardholders whenever a user swipes their card, along with a photograph of the transaction.

In 2017, L. Nagarajan et al. [25] introduced a cost-effective smart locker security system that explores the potential of the Internet of Things (IoT). The solution optimizes resource usage and provides strong security measures by utilizing IoT technology. These developments emphasize the importance of using multiple strategies to strengthen ATM security as technology continues to evolve. Future research could integrate mobile technologies, intelligent sensors, and biometrics to further enhance the protection of ATM systems.

In 2017, Karen Renaud et al. [26] published a textual evaluation on the HCSP analysis, based on research by Bødker and Harrison. They analyzed the progression of security challenges through the waves of technological advancements in IT conferences. The study discussed the steps taken to ensure secure systems and improve the protection of personal computers.

In 2016, H. Swathi et al. [27] introduced a dynamic PIN system, which enhances ATM security by generating a unique Personal Identification Number (PIN) for each transaction. This PIN is sent to the user via SMS through a GSM module, ensuring greater security than traditional static PIN methods. The dynamic nature of this PIN system mitigates the risks associated with lost cards and simplifies the process of deactivating compromised accounts, making it a more secure and practical method for ATM transactions.

In 2016, K. Hema Sen and Siva Prasad et al. [27] proposed the development of an advanced anti-theft ATM system. This system integrates a mobile payment security solution that can be concealed inside the ATM to prevent unauthorized access. This solution is cost-effective and provides robust security against remote hacking and ATM theft.

In August 2016, G. Jakeer Hussain et al. [28] introduced a solution incorporating both hardware and software components to enhance ATM security. They installed a MEMS sensor in the ATM's locker area, which triggers the automatic closure of the locker door whenever tampering is detected. The sensor data is stored on an embedded server, offering a responsive security system to prevent thefts.

III. EXISTING SYSTEM

The Existing ATM security system integrates multiple components, including a solenoid lock, MEMS sensor, vibration sensor, IR sensor, ESP Cam, and an Arduino-based microcontroller. The system utilizes these components to detect unauthorized access, monitor movement, and initiate defensive measures when a security breach is detected.

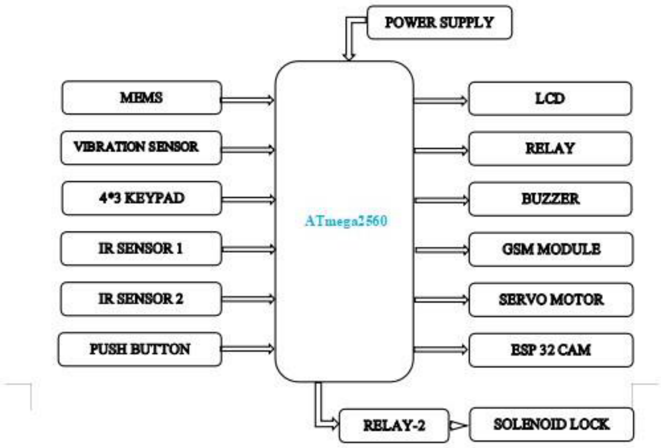


Fig. 3.1: Existing Block Diagram

Microcontroller: The core of the system is the ATmega2560 microcontroller, a highly capable processor offering 54 digital I/O pins, 16 analog input pins, and a clock speed of 16 MHz. Operating at 5V, the ATmega2560 supports a wide range of functions, with 256 KB of flash memory, 8 KB of SRAM, and 4 KB of EEPROM for storage. It is ideal for handling complex tasks such as sensor data processing, security system control, and triggering various actions based on detected threats.

MEMS Sensor: The MEMS (Micro-Electro-Mechanical Systems) sensor is used to detect changes in the ATM's position, which can indicate tampering or a robbery attempt. This sensor measures acceleration and can detect even subtle movements. With configurable sensitivity settings (such as ±2g, ±4g, ±8g, or ±16g), the MEMS sensor can provide real-time data about the ATM's movement, which is crucial for identifying unauthorized activities.

Vibration Sensor: The vibration sensor is a key component for detecting mechanical disturbances in the ATM. When a vibration or impact occurs, such as from a hammer or other forceful methods, the vibration sensor converts mechanical energy into an electrical signal. This helps to identify tampering or theft attempts by recognizing abnormal vibrations. The sensor can be piezoelectric or piezoresistive, with outputs that may include frequency-based, digital, or analog signals.

IR Sensor: The IR sensor plays a role in detecting the presence of individuals near the ATM. It works by sensing infrared light, typically emitted by objects or people in motion. When the IR sensor detects a person entering the ATM room, it sends a signal to the processor to open the room door using a servo motor. The door will remain open for five seconds before closing automatically. If an unauthorized person attempts to force the door open, the system activates an alarm to alert nearby individuals.

Solenoid Lock and Gas Discharge: When the system detects suspicious activity, such as changes in position or excessive vibrations, the solenoid lock is activated to secure the ATM room door. In addition, a relay triggers the release of incapacitating gas within the ATM. The gas renders the intruder unconscious, preventing them from fleeing the scene. This action reduces the risk of the criminal escaping and enhances the ATM's security.

ESP Cam: An ESP Cam is used to capture images of the ATM and the surrounding area when a security breach is detected. These images can be used as evidence to identify the intruder. The camera stores the pictures, which can be reviewed later or transmitted to security personnel in real time for quick action.

Communication and Alerts: For real-time communication, a GSM module sends an alert to the relevant bank authorities and a nearby police station. Along with the alert, a One-Time Password (OTP) is generated and sent to authorized personnel to verify and take further actions. The buzzer sounds as an additional alert to notify individuals nearby that a security breach has occurred.

System Operation: When the IR sensor detects someone entering the ATM room, it triggers the servo motor to open the door. After five seconds, the door automatically closes. If any suspicious movement or tampering is detected by the MEMS or vibration sensors, the processor takes immediate action by locking the ATM room door with the solenoid lock and releasing the incapacitating gas. The ESP Cam captures photographic evidence of the incident, and a message with the OTP is sent to the designated authorities. The buzzer sounds, and the system stays in an alert state until the situation is resolved. The OTP is displayed on the LCD screen, and the door can only be unlocked by entering the correct code using the keypad.

This multi-component security system enhances ATM protection by incorporating automated responses and real-time monitoring, ensuring that ATMs can be effectively secured without relying on physical security guards. The integration of sensors, gas discharge mechanisms, and remote communication ensures that ATMs are safeguarded against theft and tampering.

Limitations of Existing System:

Mobile Connectivity Dependency: The mobile app relies on network connectivity. Weak or no signal could limit real-time monitoring and control, impacting system responsiveness.

RFID Security Risks: RFID cards are vulnerable to cloning and hacking, allowing unauthorized access if not properly encrypted. Security protocols must be strengthened to prevent this risk.

App Security Vulnerabilities: The mobile app could be targeted by hackers, compromising control over the ATM system. Regular updates, encryption, and multi-factor authentication are necessary to secure the app.

Privacy Concerns: Sensitive data transmitted via the mobile app and RFID system may be exposed if not encrypted properly, leading to privacy risks for users and financial institutions.

RFID Range and Interference: RFID cards have limited reading range and may experience interference, especially in environments with high electromagnetic noise, potentially leading to access failures.

App Compatibility and Usability: The app must be compatible with various devices and have a user-friendly interface. Complex designs could delay the response time in emergency situations.

System Complexity and Cost: Integrating mobile app functionality and RFID technology increases system complexity and cost, especially for large ATM networks, requiring ongoing maintenance and upgrades

IV. PROPOSED SYSTEM

The system incorporates various sensors such as MEMS, vibration, IR, and RFID to detect potential threats. An ATmega2560 microcontroller processes the sensor data and controls output devices like an LCD, buzzer, and servo motor to trigger security measures. A fingerprint scanner and an ESP32 CAM (camera) are integrated for user authentication and visual monitoring. The system also allows for remote monitoring and control through an app, enhancing security and management capabilities.

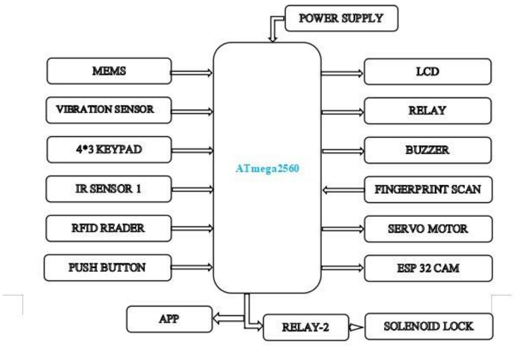


Fig. 4.1: Block Diagram

Core Component:

ATmega2560: This microcontroller serves as the central processing unit of the system. It receives and processes data from various sensors, makes decisions based on the inputs, and controls the output devices to implement security measures.

Fig. 4.2: Arduino

Input Devices:

Vibration Sensor: Detects vibrations or shocks that might indicate forced entry or tampering with the ATM. This is crucial for triggering alarms or initiating lockdown procedures.

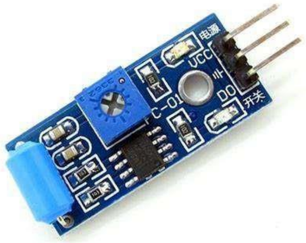


FIG.4.3. VIBRATION SENSOR

IR Sensor 1: Can be used to detect movement or obstructions in front of the ATM. This helps identify potential intruders and can trigger alerts.

FIG.4.4. IR SENSOR

RFID Reader: Enables access control by verifying authorized personnel (e.g., technicians, security guards) using RFID cards or tags. This prevents unauthorized access to internal components.

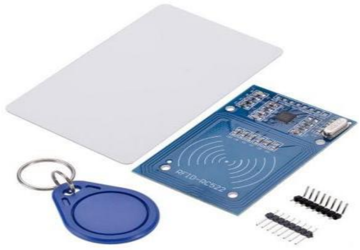


FIG.4.5. RFID Reader and Card

Fingerprint Scan: Provides an additional layer of biometric authentication. It verifies the identity of authorized personnel for access to sensitive areas or functions.

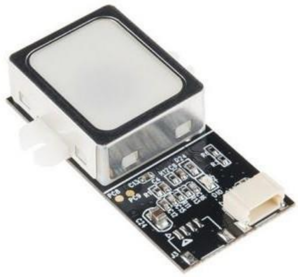


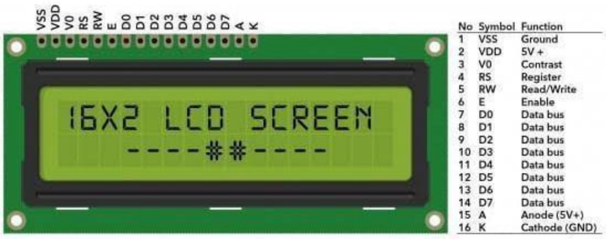
FIG.4.6. FINGERPRINT DEVICE

Push Button: Can be used for emergency stop or manual activation of certain security measures.

FIG.4.7. PUSH BUTTON

Output Devices:

LCD: Displays messages, alerts, and system status information to users or security personnel. This provides visual feedback and helps in monitoring the system.



No	Symbol	Function
1	VSS	Ground
2	VDD	5V +
3	V0	Contrast
4	RS	Register
5	RW	Read/Write
6	E	Enable
7	D0	Data bus
8	D1	Data bus
9	D2	Data bus
10	D3	Data bus
11	D4	Data bus
12	D5	Data bus
13	D6	Data bus
14	D7	Data bus
15	A	Anode (5V+)
16	K	Cathode (GND)

FIG.4.8. LCD

Relay: Acts as an electrically controlled switch. It can be used to activate alarms, control the solenoid lock, or power other security devices.

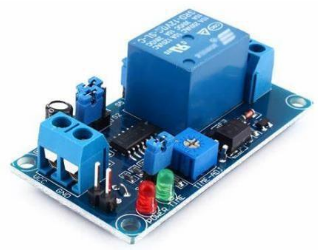


FIG.4.9. RELAY

Buzzer: Emits a loud alarm to deter intruders and alert security personnel or nearby individuals.

FIG.4.10. BUZZER

Servo Motor: Can be used to control the movement of certain parts of the ATM, such as opening or closing access panels or adjusting camera positions.

FIG.4.11. SERVO MOTOR

Solenoid Lock: A powerful electromagnet that can be used to secure the ATM door or other critical components, making it difficult to open without authorization.

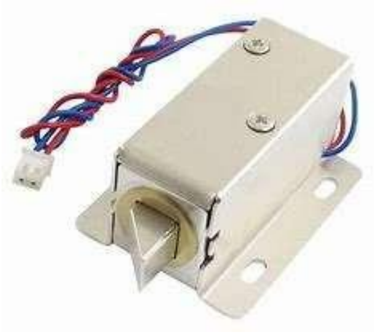


FIG.4.12. SOLENOID LOCK

ESP32 CAM: Enables video surveillance of the ATM area. It captures images or videos of potential intruders, which can be used for evidence or to alert security.

FIG.4.13. ESP32 CAM

Communication and Control:

APP: Allows for remote monitoring and control of the ATM system. Security personnel can receive alerts, adjust security settings, and view live video feeds from the ESP32 CAM.

FIG.4.14. MOBILE APPLICATION

Power Supply: Provides the necessary electrical power to operate all components of the system.

Additional Considerations:

4x3 Keypad: While not directly related to the anti-robbery aspect, it may be used for user input, such as entering administrative codes or accessing certain functions.

How these components work together:

Monitoring: Sensors (vibration, IR) constantly monitor the ATM environment for any suspicious activity.

Authentication: RFID readers and fingerprint scanners verify the identity of personnel accessing the ATM.

Response to Threats: If a threat is detected (e.g., vibration, unauthorized access), the system triggers alarms (buzzer), activates the solenoid lock, and notifies security personnel via the app.

Surveillance: The ESP32 CAM captures images or videos of the incident for evidence and further investigation.

V. WORKFLOW

Present's a reason of the intelligent antagonistic-stealing door lock scheme for secure Cash dispenser, based on the supported flow diagram: System Survey this method aims to improve ATM safety by achieving a multi-layered approach to approach control and interruption detection. The gist elements of the system are:

5.1 System Workflow

CAM/Communication: Bureaucracy starts by monitoring the Cash dispenser field through the CCTV camera. If some doubtful activity is discovered, an alert meaning is shipped to the security troop.

Biometric Check: The consumer is prompted to supply their biometric attestations (fingerprint or first leaf through). If the biometric data counterparts the stocked facts, the system reward to the next step. Alternatively, the system generates a siren to alert the user and safety people.

RFID Card Check: The consumer inserts their RFID check. If the card is genuine and competitions the consumer's identity, bureaucracy profit to the next step. Otherwise, dismissal from responsibility debris closed.

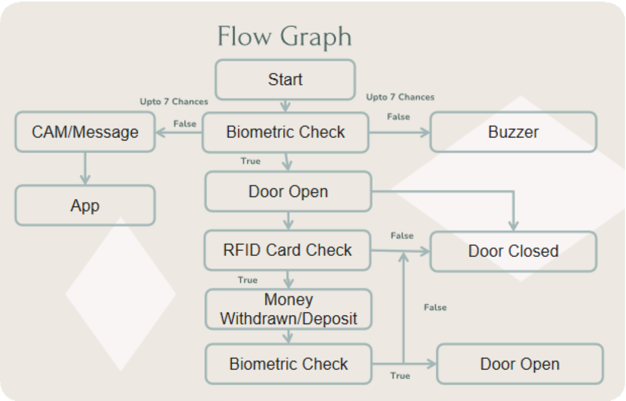


Fig 5.1: System Workflow

Services Remote/Deposit: The user acts the wanted undertaking (withdrawal or deposit) through the Cash dispenser connect.

Biometric Check (Again): Subsequently the undertaking is completed, bureaucracy acts another biometric check to ensure that the consumer leaving the Cash dispenser is the unchanging person the one begun the transaction. If the counterpart is profitable, the door opens. Alternatively, dismissal from responsibility remains shut.

5.2 Antagonistic-Robbery Measures

Multi-determinant Confirmation: Bureaucracy employs diversified coatings of authentication, containing biometric proof and RFID card check, making it more troublesome for wrongful individuals to attain.

CCTV Following: The constant monitoring of the Cash dispenser extent through CCTV cameras helps deter potential robberies and specifies valuable evidence as long as of an incident.

Security system: The siren and alert messages to protection people act as an next impediment and contain rapid answer for fear that of unauthorized approach attempts.

Undertaking Monitoring: Bureaucracy monitors all undertakings in real-opportunity, that can help discover and prevent deceptive endeavors.

5.3 Additional Concerns

Balanced Maintenance: Bureaucracy demands regular perpetuation to guarantee the accuracy and dependability of biometric sensors, RFID lecturers, and additional components.

Operating system Renews: Regular program renews are necessary to address protection exposures and improve arrangement acting.

Consumer Training: Consumers bear be trained on the correct use of bureaucracy and security processes to underrate the risk of errors or unforeseen approach issues.

VI. RESULT

The FIG 6.1 illustrates an anti-robbery door lock system for ATMs. The system utilizes various sensors like MEMS, vibration, IR, and RFID, along with a fingerprint scanner and a camera, to monitor for threats. The data is processed by an ATmega2560 microcontroller, which controls the solenoid lock, buzzer, relay, and servo motor to activate security measures. The system also allows for remote monitoring and control through an app.

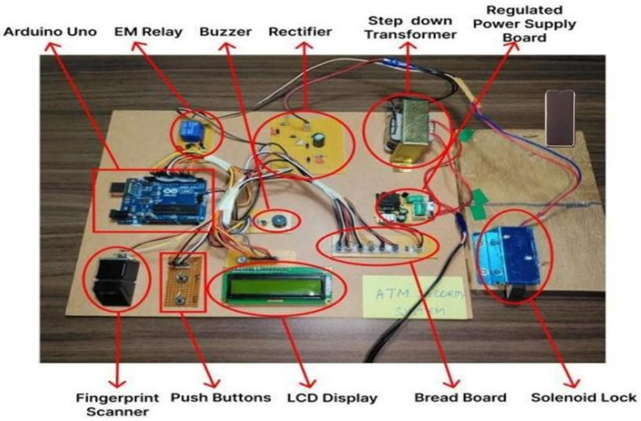


FIG 6.1 Hardware Circuit

Output:

The system Output shown in below:

FIG 6.2 The "ATM is Safe Welcome" message indicates the ATM is currently secure from robbery attempts. This is reassuring for both bank personnel and customers. The system is likely actively monitoring for threats and preventing unauthorized access.

FIG 6.3 The image displays an LCD screen with the message "Pls Place A Valid Finger." This indicates a fingerprint-based access control system, likely for an ATM. The user is prompted to place their finger on a scanner (not shown) for authentication. The system compares the scanned fingerprint with a database of authorized fingerprints. If a match is found, access to the ATM is granted; otherwise, access is denied, and the message "Pls Place A Valid Finger" is likely displayed again.

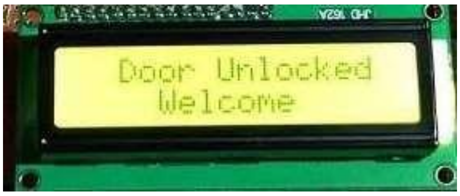


FIG 6.4 If the Finger is matched with database the door will be open otherwise buzzer will be activated.

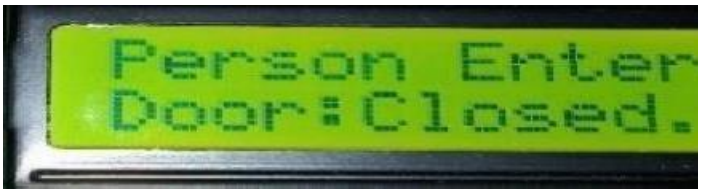


FIG 6.5 If a person entered into the ATM the door will automatically Locked. After completion of Transaction again want ton place a finer to open the door.

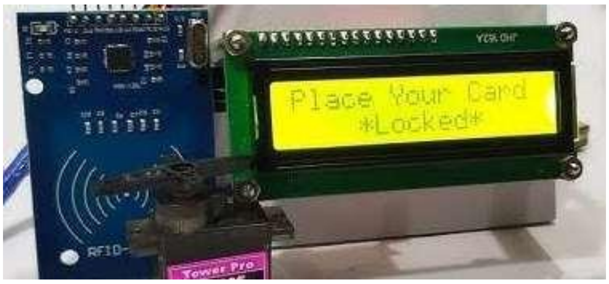


FIG 6.6 The image shows an anti-robbery door lock system for secure ATMs. To access the ATM, users are likely required to present an RFID card for scanning. The system then verifies the card's credentials to grant or deny access. The "Place Your Card Locked" message displayed on the LCD screen indicates that the ATM door is currently locked and awaiting card presentation for access.

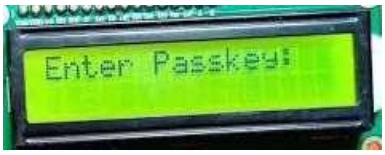


FIG 6.7 RFID Scan: The user presents their RFID card to the scanner (not visible in the image).

* RFID Verification: The system verifies the card's credentials.

* Passkey Prompt: If the RFID card is valid, the system displays the "Enter Passkey!" message.

* Passkey Entry: The user enters their ATM passkey using a keypad (not visible in the image).

* Passkey Verification: The system verifies the entered passkey.

* Access Decision: If both the RFID card and the passkey are verified, the system grants access to the ATM and allows the user to proceed with their transaction.

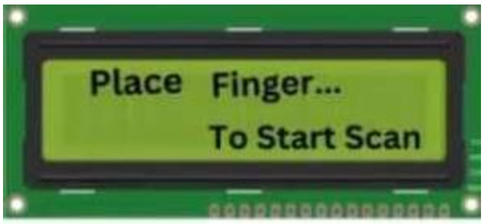


FIG 6.8 Money Withdrawal: The user completes their ATM transaction and withdraws their money. Exit Prompt: The system displays the message "Place Finger... To Start Scan" on the LCD screen. Fingerprint Scan: The user places their finger on the fingerprint scanner.

Fingerprint Verification: The system compares the scanned fingerprint with a database of authorized fingerprints.

Exit Decision:

If the fingerprint matches an authorized record, the system will grant exit access.

If the fingerprint does not match, the system will likely deny exit access and display an error message

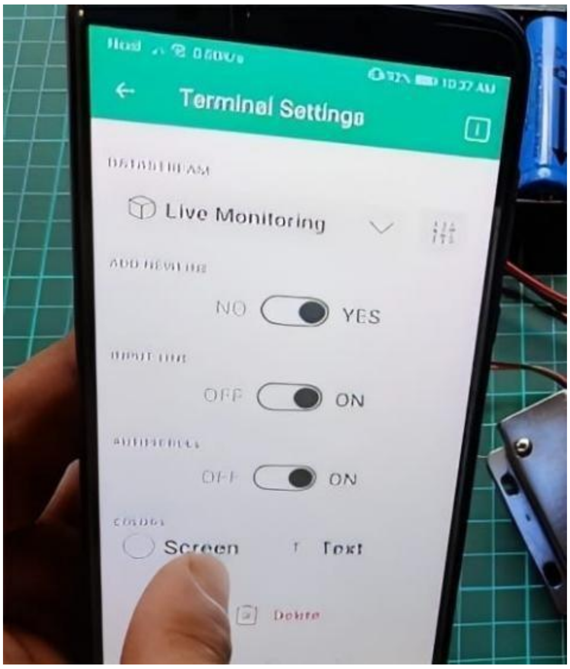


FIG 6.9 The image shows a smartphone screen with a "Terminal Settings" app open. This suggests the system can be controlled remotely using a mobile application.

Here are some features that the app likely enables:

* Live Monitoring: The "Live Monitoring" switch indicates that the app allows users to monitor the system's status and activity in real-time.

* Remote Control: The other switches and settings might allow users to remotely control various aspects of the system, such as:

* Enabling or disabling certain features

* Configuring system parameters

* Triggering actions or commands

VII. FUTURE SCOPE AND RESEARCH DIRECTIONS

1. AI Integration: Employ artificial intelligence for threat detection, predictive analysis, and anomaly detection.

2. IoT and Cloud Support: Expand functionality through real-time data sharing and analysis via cloud platforms.

3. Enhanced Biometric Systems: Incorporate additional biometric methods like facial recognition for multifactor security.

4. Eco-Friendly Design: Develop energy-efficient hardware and explore renewable energy sources.

5. Adaptive Systems: Build algorithms that dynamically adapt to environmental changes for consistent performance.

VIII. CHALLENGES

1. Component Integration: Ensuring compatibility among multiple sensors and modules.

2. Data Integrity: Preventing data breaches or unauthorized access to sensitive information.

3. Cost Management: Reducing the cost of hardware without compromising performance.

4. Scalability: Supporting multiple simultaneous users and operations.

5. Environmental Impact: Making systems robust against dust, heat, and humidity.

IX. OBJECTIVES

1. To develop a reliable and cost-effective security system integrating biometric and RFID technologies.

2. To enhance user accessibility through mobile applications and real-time monitoring.

3. To ensure the system’s adaptability to varying environmental conditions.

4. To incorporate effective alert mechanisms to detect and deter unauthorized access.

5. To optimize energy consumption for sustainable operations.

X. CONCLUSION

The proposed ATM security system offers a modern and effective solution to address the growing threats associated with ATM-related crimes. By integrating advanced technologies such as MEMS sensors, vibration detectors, RFID access control, and automated response mechanisms, this system enhances the physical security of ATMs and provides a rapid, automated response to potential threats. The inclusion of a mobile application for real-time monitoring and control further strengthens the system, enabling swift intervention and coordination by authorized personnel. This comprehensive, cost-efficient approach improves both security and operational efficiency, ultimately safeguarding ATM users and financial institutions against theft, fraud, and tampering.

REFERENCES

[1] Wang, L., Hung, D.,(2020). Functional Market Study of Mobile-Health APP for Elderly. In 2020 IEEE 2nd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS), pp. 122-125. IEEE.

[2] Viitanen, Marko. "HEVC Parameter Exploration for Efficient Mode Decision." Master's thesis, 2017.

[3] Raaj, M. M. E., & Juliaen, A. (2015). Development& deployment using embedded modules of an anti-theft ATM computer. In 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], pp. 1-5. IEEE.

[4] Mathews, Prasadh, M., & Divyaa, R. S. (2017). Super Safe Doors for Crucial Zones System. In 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), pp. 242-245. IEEE.

[5] Joge, Vikram, V., Jaine,D., Aroraa, R., & Bhaat, B. (2013). Theft avoidance ATM model uses inactive payment tracking. In 2013 IEEE Conference on Information & Communication Technologies, pp. 1156-1159. IEEE.

[6] Martin, I. (2012). Too far ahead of its time: Barclays, Burroughs, and real-time banking. IEEE Annals of the History of Computing, 34(2), 5-19.

[7] Oyemakara, M. I. H. (2020). AN INVESTIGATION INTO THE CHALLENGES FACED BY USERS OF ELECTRONIC PAYMENT PLATFORMS OF NIGERIAN BANKS IN RIVERS STATE, NIGERIA. European Journal of Social Sciences Studies, 5(5).

[8] Jog, V. V., Jain, D., Arora, R., & Bhat, B. (2013, April). Theft prevention ATM model using dormant monitoring for transactions. In 2013 IEEE Conference on Information & Communication Technologies (pp. 1156-1159). IEEE.

[9] Solanke, S., Sonawane, N., Ugale, V., & Khoje, S. A. (2017). Home Security Using Image Processing and IoT. International Journal of Emerging Technologies in Engineering Research (IJETER), 5(6).

[10] Abdullah, S. M. (2018). Design secured smart door lock based on jaro winkler algorithm. Tikrit Journal of Pure Science, 21(6), 154-159.

[11] Sivakumar T.1, Gajjala Askok2, k.Sai Venuprathap3 “Design and Implementation of Security Based ATM theft Monitoring system” International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 1 August 2013.

[12] V Jacintha; J. Nagarajan; K. Thanga Yogesh; S. Tamilarasu; S. Yuvaraj “An IOT Based ATM Surveillance System” Published in: 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) DOI: 10.1109/ICCIC.2017.8524485K. Elissa, “Title of paper if known,” unpublished.

[13] Claudio Porretti, Denis Kolev, Raoul Lahaije “A New Vision for ATM Security Management” 2016 11th International Conference on Availability, Reliability and Security 2016 IEEE DOI 10.1109/ARES.2016.50.

[14] Jignesh J. Patoliya, Miral M. Desai, “Face Detection based ATM Security System using Embedded Linux Platform” 2017 2nd International Conference for Convergence in Technology (I2CT) 978-1-5090-4307-1/17/$31.00 ©2017 IEEE.

[15] Dujak, Mico, et al. "Machine-to-machine communication as key enabler in smart metering systems." Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on. IEEE, 2013.

[16] Liu, Yakun, and Xiaodong Cheng. "Design and implementation of embedded Web server based on arm and Linux." Industrial Mechatronics and Automation (ICIMA), 2010 2nd International Conference on. Vol. 2. IEEE, 2010.

[17] Jothish Kumar M; Ramakrishnan Raman; S. Prabhakar; T. Bernatin. Ajaykumar M (2013). “Anti-Theft ATM Machine Using Vibration Detection Sensor” International Journal of Advanced Research in Computer Science and Software Engineering, pp: 23-28.

[18] R1, Kalaiselvan . M2, Mr. R. Rajagopal3 “Advanced ATM Security System Deepa” International conference on. IEEE, 2016.

[19] Refaie, M.N. Compute. Eng. Dept., Kuwait Univ., Kaldiya, Kuwait Selman, AA Ahmad, I.2012 “Hybrid parallel approach based on wavelet transformation and principle component analysis for solving face recognition problem” IEEE conference on Volume: 2007.

[20] K. Sreenivasa Rao, SM. Mohammad Eliyas, L. Manjunath, M. Meghana, P. Kiran Kumar Advanced Atm Security With Automatic Door Lock System Using Arduino Processor 2024 IJNRD , Volume 9, Issue 3 March 2024, ISSN: 2456-4184.

[21] Ai based E-Atm security and surveillance system using blynk-lot server international conference on. Ieee, 2022.

[22] Arjun kumar mistry, suraj kumar and vicky prasa, “Secured atm transaction using gsm”, international journal of electrical and electronic engineering & telecommunication, vol. 2, no. 3, july 2013.

[23] Taha Ayesha, Pallavi B V Dr. Baswarajgadgay “Securing ATM Transactions using Raspberry Pi Processor”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 6, No. VII, 2018.

[24] L. Nagarajan “iot-based low-cost smart locker security system”.

[25] Karen renauda, stephen flowerday, “Journal of information security and applications”, 2017. 13. “A novel atm security system using a user defined personal identification number with the aid of gsm technology” deepa. R. Et.al int. Journal of engineering research and applications issn: 2248-9622, pp.01-03.

[26] Raj, hema sen, siva prasad. M. E., and anitha julian. "Design and implementation of antitheft atm machine using embedded systems." in 2015 international conference on circuits, power and computing technologies [iccpct-2015], pp. 1-5, 2015.

[27] G. Jakeer Hussain1, T. Srinivas Reddy2 “Advanced Anti-Theft ATM Security using Raspberry Pi” International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 - 0056 Volume: 03 Issue: 08 | Aug-2016.

Citation of this Article:

B. Sapthagiri, V.K. Sreedhar, N. Sangeetha Reddy, P. Mohammed Shahid Khan, K. Seshu, T. Shaik Sabiya. (2025). Intelligent Anti-Robberry Door Lock System for Secure ATMs. *International Current Journal of Engineering and Science - ICJES*, 4(4), 7-17. Article DOI: https://doi.org/10.47001/ICJES/2025.404002

****