International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 09 | September - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

# ATM Security System Based on IOT

**Sri Vaishnavi Bhamidipati[1], Visalakshi Metla[2], Shiva Sagar[3], Dr. V Padmanabha Reddy[4]**

*[1]Student of Electronics and communication engineering, Institute of Aeronautical Engineering*
*[2]Student of Electronics and communication engineering, Institute of Aeronautical Engineering*
*[3]Student of Electronics and communication engineering, Institute of Aeronautical Engineering*
*[4]Professor of Electronics and Communication engineering, Institute of Aeronautical Engineering*

**Abstract -** The evolution of technology has led to many innovations that ease our life, like digitisation, automation, Artificial intelligence, Data science, etc. Though these technologies are helpful, they come with a cost. Digitisation makes us more vulnerable to cyber-attacks and crimes. Digitisation in finance sectors like banks, stock markets and ATMs is more susceptible to theft and cyber-attacks as they hold a high financial risk. One concern that we are addressing and aiming to improve is the Security System of ATMs. ATM systems made financial transactions more accessible, but they pose a risk to Financial and customer security. Various ATM security systems were developed to combat thefts and cyber-attacks, but they address customer security issues like ATM card trapping, skimming, and cloning. We aim to provide security for the bank and Cash Management Company loading the cash in the ATM. The ATM security system we are developing ensures proper authorisation using a biometric sensor.

***Key Words*:** Security System; ATM frauds; Embedded systems; Internet of things(IOT); Automation; Authorisation; Microcontroller; Arduino; Control systems.

## 1. INTRODUCTION

An ATM (Automated Teller Machine) is a self-service banking machine that provides customers with access to financial transactions securely and conveniently. ATMs let customers withdraw cash, deposit money, transfer funds, pay bills, check account balances and perform other banking transactions without visiting a bank. They are connected to a network that enables them to communicate with the customer's bank and process real-time transactions. ATMs typically require a debit or credit card to initiate any transaction and perhaps also need a personal identification number (PIN) for security purposes. They are widely available and accessible 24/7, making them a popular and convenient option for banking services.

The increasing threats to Banks and ATMs have been an alarming concern over the years. ATMs have made financial transactions (like cash withdrawal, cash deposit, Balance enquiry, etc.) more accessible, without the hassle of going to a bank, waiting in long queues and filling out forms; ATMs have eliminated this lengthy process for simple financial transactions. ATMs are simple and easy to use and hence have become widely accepted. ATMs come with the drawback of being highly susceptible to thefts and attacks as they hold abundant cash within them. Customers use an ATM card secured with a pin for authorisation to perform financial transactions.

ATM frauds can affect anyone who uses ATMs, including-cardholders who use the affected ATM, Bank customers who may have their personal and financial information stolen, Businesses that own or operate the affected ATM, Financial institutions that issue the affected cards and are liable for fraudlent transactions.

The ATM cash loading process involves replenishing the machine's cash supply to ensure it can continue to dispense cash to customers. Only authorized personnel with proper identification and security clearance can access the ATM's cash vault to load or replenish cash. The cash is counted and verified before being loaded into the machine to ensure the correct amount is being loaded. The cash is loaded into the ATM's cash dispenser, which counts and verifies the cash and updates the machine's internal records. The amount of cash loaded into the machine is reconciled with the machine's records to ensure accuracy Any unused or excess cash is securely stored in the machine's vault until it can be collected and transported to a secure location.

The ATM cash loading process is typically performed by specialized cash-in-transit companies or the bank's own security personnel. The frequency of cash loading depends on the volume of transactions and the amount of cash the machine can hold. It is important to ensure the security and accuracy of the cash loading process to prevent theft, fraud, and other security threats, and to ensure the machine is able to dispense cash to customers as needed.

Security system for ATM can be developed for authorisation of the cash management company employees who load the cash into the system. This security system will help in case of a theft to know who has accessed the system latest.

## 2. LITERATURE REVIEW

Extensive research has been conducted on security and management systems for ATMs, addressing the diverse challenges encountered in this domain. Scholars have explored various aspects, including access control mechanisms, biometrics, and surveillance systems, to enhance ATM security. This literature survey provides an overview of existing research, highlighting key findings and advancements in the field. By identifying trends and gaps, this survey aims to

contribute to the ongoing development of ATM security systems.

The study presents a method proposing the detection of stolen ATM machines in real-time using GSM technology, supposedly aiming to mitigate losses. It suggests a combination of vibration sensors, DC motors, stepper motors, and a buzzer to notify the respective bank and police station. Additionally, a camera is employed for continuous video recording, accompanied by a stepper motor releasing gas to render the thief unconscious, and a DC motor shutting the ATM door. The Security Based ATM theft project claims to prevent theft by utilizing ARM controller-based embedded systems and vibration sensors for vibration detection. In the event of vibrations, a buzzer will sound, the ATM door will automatically close with the help of a DC motor, and a stepper motor will release gas inside the ATM to render the thief unconscious. A camera will continuously record video footage, which will be transmitted to a PC. The Real-Time Clock (RTC) is said to record the time of the robbery and transmit a message to the nearest police station and the corresponding bank via GSM. The output message is displayed on an LCD display board. The project supposedly employs Keil tools for implementation, enabling the automatic control of the DC motor and stepper motor for door locking and gas release. The overall aim of this project is claimed to be the prevention of ATM theft and assisting in the apprehension of culprits. [1]

In the current landscape, where ATMs are extensively used for cash withdrawals, incidents of ATM robberies persist despite the presence of CCTV cameras. This has necessitated a re-evaluation of security systems. An existing security system utilizes smart technology, incorporating a Face Recognizing Camera to capture the identities of individuals entering, along with tilt and vibration sensors to detect suspicious activities. While its aim is to alert users through social media platforms via IOT and GSM networks, concerns arise regarding the use of chloroform as a means to render thieves unconscious. The effectiveness and practicality of this system warrant further scrutiny. Despite the extensive presence of CCTV cameras, the persistently high incidence of ATM robberies brings into question the effectiveness of existing security measures. In an attempt to address this issue, a proposed security system for ATM theft relies on advanced technology to combat physical attacks on ATMs. The inclusion of a Face Recognizing Camera aims to capture user identities, while tilt and vibration sensors are intended to detect any suspicious activities. Although a temperature sensor monitors the ATM booth's temperature, its practical relevance remains uncertain. The system claims to alert authorities via social media platforms such as Facebook, Twitter, and Gmail, utilizing the IOT and GSM network. However, the use of liquidator chloroform to incapacitate thieves raises ethical concerns. While the system promises realistic monitoring and control, its ability to effectively reduce robberies requires careful evaluation. [2]

This paper presents a purportedly innovative perspective on ATM Security Management, introduced through the GAMMA project and its "core" prototype, the Security Management Platform. The GAMMA project, part of FP7, aims to address emerging vulnerabilities in ATM systems. The proposed GAMMA vision emphasizes a collaborative framework for security management, advocating self-protection and resilience within the ATM system. It envisions a distributed federated environment that facilitates the sharing of security information. Implemented as a network of distributed nodes within the ATM system, the Security Management Platform prototype provides interfaces for internal and external security stakeholders. While it aims to manage security comprehensively, encompassing prevention, incident identification, and crisis resolution, its practicality and effectiveness warrant further examination. The primary objective of the GAMMA project is to address emerging vulnerabilities in ATMs through the development of innovative solutions. This entails establishing a collaborative framework for security management and implementing a self-protective and resilient ATM system capable of sharing security information in a distributed environment. At the core of this endeavour is the Security Management Platform prototype, comprising a network of embedded nodes within the ATM system that facilitate interactions with both internal and external security stakeholders. This platform assumes responsibility for overseeing the entire spectrum of security, encompassing prevention, incident identification, and crisis resolution within the ATM ecosystem. By emphasizing the sharing of security information among stakeholders, including alerts, reports, and countermeasures, the GAMMA project endeavours to provide a holistic approach to ATM security management. [3]

While the system claims to offer a high level of security, primarily through face detection, its effectiveness in accurately detecting human faces remains uncertain. Furthermore, the repetition of emphasizing the provision of reliable security raises questions about the system's actual reliability and practicality. The implementation of a smart ATM security system that utilizes the Embedded Linux platform, employing a compact Raspberry Pi board and OpenCV software for efficient image processing. The system's primary objective is to ensure high-level security by employing a series of sequential actions. It begins by capturing the user's face and verifying its proper detection. In instances of detection failure, the system promptly alerts the user and initiates the locking mechanism for the ATM cabin door. To grant access, the system generates a unique OTP (One-Time Password) and sends it via SMS to the registered mobile number of the designated watchman using a GSM module. The watchman then enters the OTP through a keypad, and the system performs a verification process to unlock the door. Through this approach, the system aims to enhance ATM security, although the practicality and reliability of the proposed solution warrant further investigation. [4]

The past security system employed by Automated Teller Machines (ATMs), which relied on magnetic cards and static PINs, has proven to be vulnerable, resulting in numerous security breaches. These vulnerabilities had led to mysterious financial losses for many bank customers. In this paper, an existing two-factor authentication system that combines the use of an ATM card with dynamic PINs is introduced to address these security flaws. The study includes the development of a prototype of an It is important to note that while this research paper introduces an alternative solution, further investigation is needed to assess its practicality, scalability, and real-world effectiveness. A purported solution introduced in this paper is a two-factor authentication system designed for Automated Teller Machines (ATMs) and mobile banking applications in an attempt to address the security vulnerabilities arising from the use of magnetic cards and static PINs. The system relies on the combination of an ATM card and dynamically generated PINs using a random number generator. The development of a prototype involved utilizing the Raspberry Pi 3B, smart card, smart card reader/writer, keypad number, and LCD monitor. An evaluation was

conducted, albeit questionably, through a questionnaire and assessments of randomness and quality of service. However, the extent to which this system genuinely mitigates security risks and provides a robust solution remains a subject of scepticism. [5]

The increasing prevalence of ATM fraud poses a significant challenge, highlighting the limitations of conventional security measures such as RFID cards and security guards. Drawing upon my extensive experience, this paper presents an innovative solution that leverages the power of a Raspberry Pi and fingerprint module to establish a robust and dynamic security framework for ATM centers. Through the integration of an Embedded Web Server, the system enables real-time monitoring and comprehensive control over the ATM environment. This cutting-edge approach not only enhances security but also delivers notable advantages in terms of cost-effectiveness and simplified management compared to traditional security methods. [6]

## 3. LITERATURE REVIEW

The existing method, discusses the importance of security in Automated Teller Machines (ATMs) and proposes a low-cost solution using a stand-alone Embedded Web Server (EWS) that works on Raspberry Pi with Linux operating system. The EWS offers a networking solution with multiple application fields over the internet, and the proposed setup includes modules for authentication of shutter lock, web-enabled control, sensors, and camera control. The project consists of two sides - one at the door with a microcontroller and another inside the ATM with Raspberry Pi. Smoke and vibration sensors are used for protection, and alert messages are sent to an authorised personnel if either is detected.

The existing system, employs a number of intelligent sensors, including the PIR (Passive Infrared) Sensor, ADXL335 Accelerometer, and FSR (Force Sensor Relay), to detect an attack and avert it. Sensitive Resistor) to sense vibration, force, abrupt acceleration, heat, and changes in orientation. The well-known ATMEGA-328 from ATMEL is the controller in use here. The ATMEL family's ATMEGA328 microcontroller serves as the foundation of this system. By using the sensors to detect changes in force, temperature, and ATM orientation, the system keeps a constant eye on its surroundings turn on the siren; display a warning.

The setup is for ATM security, comprising of the modules camera, sensor, web enabled control.

The block diagram in Figure 1 shows how an RFID reader is used to authenticate a person outside the shutter. The RFID reader sends serial data to the controller unit which controls the door lock based on the data read from the RFID card. If the card is authorized, the door opens for the person and displays an authorized message on the LCD screen. If the card is unauthorized, the door remains closed and an unauthorized message is displayed on the LCD screen.

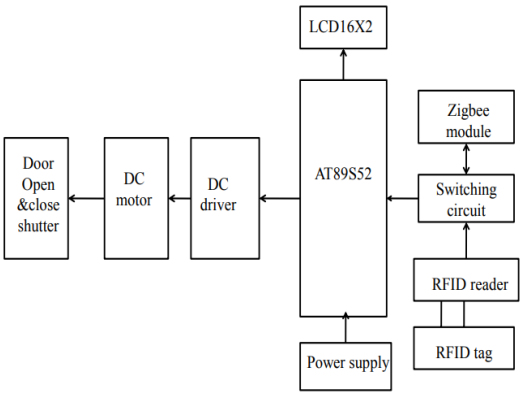


*Figure 1 Existing block diagram module at ATM door*

The block diagram depicted in Figure 2 illustrates the internal sensor monitoring system implemented within an ATM. It showcases the integration of several sensors to enhance security measures discreetly. For power-saving purposes, a PIR sensor is employed to automatically control the lights, turning them on or off upon detecting a person entering or exiting the ATM. Additionally, a smoke sensor is utilized to promptly detect and alert the nearest police station in the event of smoke presence. Simultaneously, a buzzer is activated to provide an audible indication.

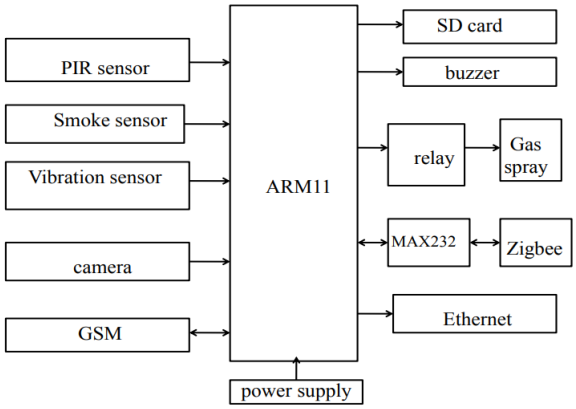


*Figure 2 existing block diagram module inside the ATM*

In case vibrations are detected by the vibration sensor, the Raspberry Pi is triggered, prompting the Pi camera to capture an image of the individual. This image is then securely stored in the SD card. Furthermore, a buzzer generates sound to attract attention. Concurrently, an alert message is sent to the nearest police station. As an added safety measure, the GAS spray system is activated, inducing unconsciousness in the person, leading to the automatic closure of the ATM shutter. To ensure data recording, the sensor values are efficiently uploaded to an HTML webpage through the utilization of Ethernet connectivity.

### *A. Limitations*

- The existing system is restricted on customer security, it is impotent to provide security to financial institutions like banks.

- The existing system is prohibitively expensive, rendering this model impractical for widespread implementation across all ATMs.
- This system is vulnerable to hacking attempts. Any internet-connected system is at risk of being targeted for hacking, and if the security measures in place are not sufficiently robust, unauthorized access and data loss may occur.
- Due to its reliance on an ARM 11 processor and numerous sensors, this is a complex system that may not be feasible for deployment across a broader network.
- Phishing attacks are heavily reliant on digital tools and technology, thus increasing the likelihood of such attacks occurring.
- False alarms may occur as a result of the vibration or smoke sensors detecting non-threatening activity, potentially leading to unnecessary panic and disruption if alert messages are sent to authorized personnel.

## 4. PROPOSED FRAMEWORK

The project endeavours to create and implement a state-of-the-art Security Based ATM theft detection system, inspired by real-life incidents that surround us. It addresses the critical issue of preventing ATM thefts and unauthorized access to the ATM cash loading system, striving to overcome the limitations of existing technologies in our society.

The proposed system introduces a revolutionary biometric registration process for accessing ATM rooms, enabling the storage of individuals' biometric details upon entry. To enter the ATM room, one must authenticate their identity by placing their finger on the fingerprint module, which acts as a biometric clock.

The primary idea of project is to design a seamless biometric solution utilizing fingerprint technology. By employing the R307 fingerprint module, individuals can effortlessly unlock and lock doors using their unique fingerprint, eliminating the need for cumbersome key chains. Enrolling fingerprints in the module is a straightforward process accomplished through intuitive push buttons.

The Figure 3 shows us the schematic diagram of how various components are connected to the Arduino uno board.

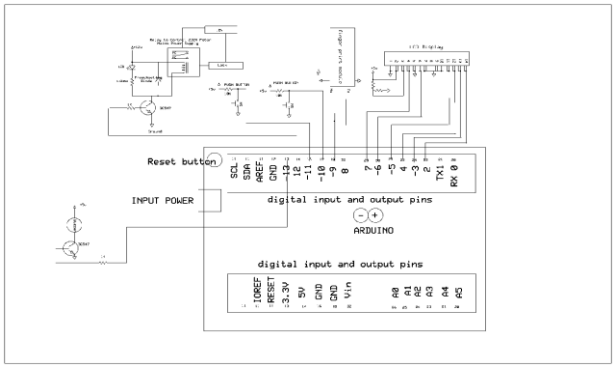


*Figure 3 Schematic diagram of ATM security system based on IOT*

The project utilizes the Arduino UNO microcontroller as the central controlling device. It interfaces with various components such as the fingerprint module, relay, solenoid lock, buzzer, and LCD module. When a user wishes to lock or unlock the door, they simply place their finger on the fingerprint module. Upon successful fingerprint authentication, the Arduino triggers the relay to unlock the door. In case an unauthorized person attempts to gain access, the system alerts with a distinct buzzer sound. Fingerprint recognition is renowned for its unparalleled security as it can uniquely identify individuals and is resistant to easy duplication. The status of the project is conveniently displayed on the LCD module, providing real-time feedback.

Overall, this project showcases a pioneering approach in enhancing ATM security, harnessing the power of biometric technology and leveraging the reliability of fingerprint recognition to fortify security measures in an efficient and user-friendly manner.

## 5. IMPLEMENTATION AND RESULTS

In this project we are going to work on ATM security using a finger print detector. We have to register a fingerprint using the biometric module. Also it supports multiusers. So, required number of people can register their fingerprint. Then the fingerprint will be stored and connected with the Arduino. As to load the cash it is secured with the biometric. If the detected biometric is matched with the existing fingerprint then it will be opened. If not other chances will be provided but if it detects any unusual activity. It rings the buzzer so, that the security guard will get the alert. So that embezzlement or thefts can be detected. The Figure 4, shows how we will implement the model.

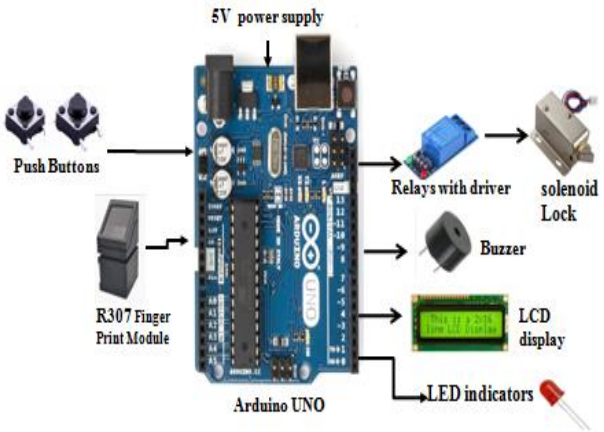


*Figure 4 Implementation of proposed model*

First, the person can register his/her fingerprint using the biometric sensor. It can be done by following the instructions displayed in the LCD display. The LED in the model can be used to detect the fingerprint and verifies the scanning of fingerprint.

Through the code we gave the fingerprint will be registered. So, whenever, a person wants to open the ATM he/she must give the biometric, if it matches then it will be opened.

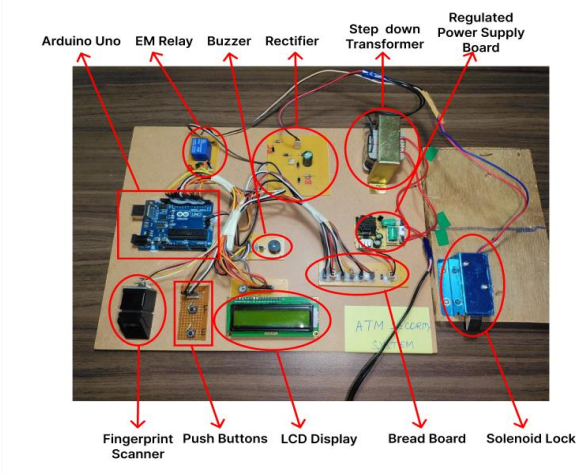


*Figure 5 Setup of ATM Security System*

The hardware set up of the proposed system will look like Figure 5.

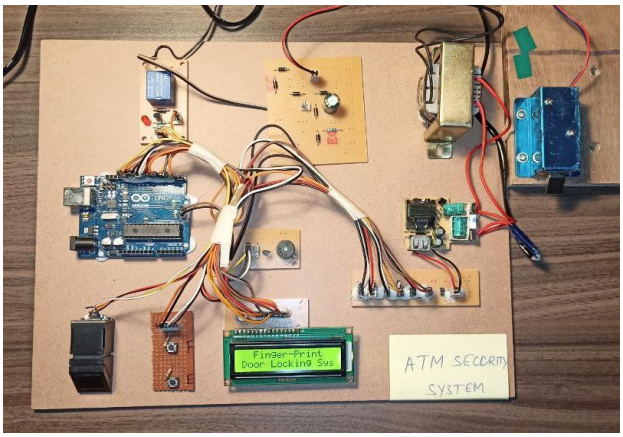


*Figure 6 Set up connected to power supply*

The Figure 6 shows us the setup connected to a power supply, and the setup turns on. We can see that the LED screen displays Fingerprint Door locking system. In Figure 7, the setup is now ready to scan the finger for verifying the authorization. Now the LCD display will show the status "Keep Finger for Scanning".

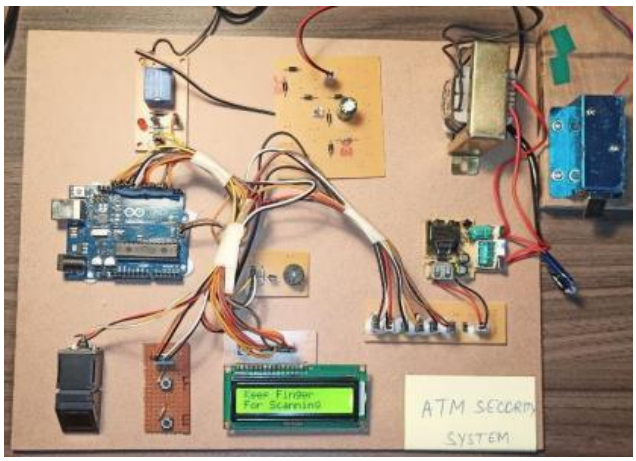


*Figure 7 Setup ready to scan finger for authorisation*

The Set-up is now ready to scan a finger to detect authentication for security of ATM.

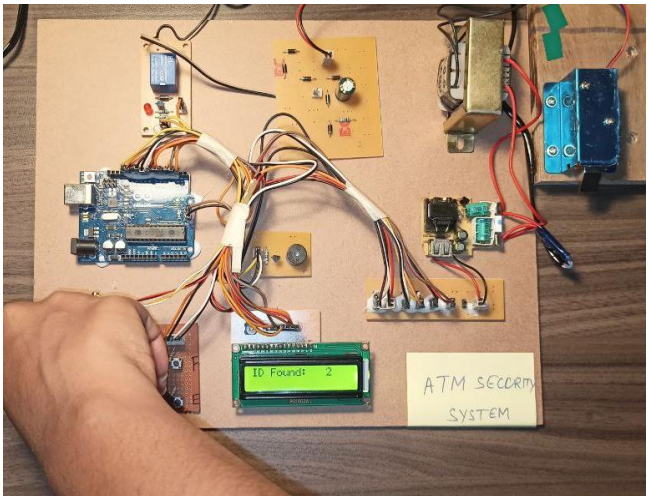


*Figure 8 ID found when an authorised person tries to access*

In Figure 8, an authorised person tried to access the security system. The authorised person fingerprint was stored in ID no 2 so, the LCD display shows the "ID Found: 2". In this context, 2 is the location where the fingerprint of the authorised is stored. In Figure 9, the access is granted and the solenoid lock will unlock, and will be open for a certain period before locking again.

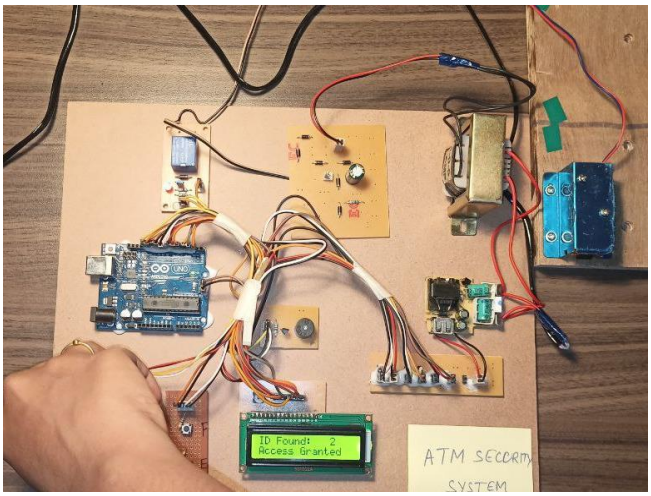


*Figure 9 Access granted, lock opens*

In Figure 10 when an unauthorised person tries to access, the Id won't be found, and the lock won't be unlocked, and the buzzer will go off alerting.LC display will show the status as "Finger not Found Access Denied".

The Arduino board pin connections for the components are as follows: the fingerprint module is connected to pins 8 and 9, the push buttons are connected to pins 10 and 11, the electromagnetic relay is connected to pin 12, the buzzer is connected to pin 13, and the LCD screen is connected to pins 2 to 7.

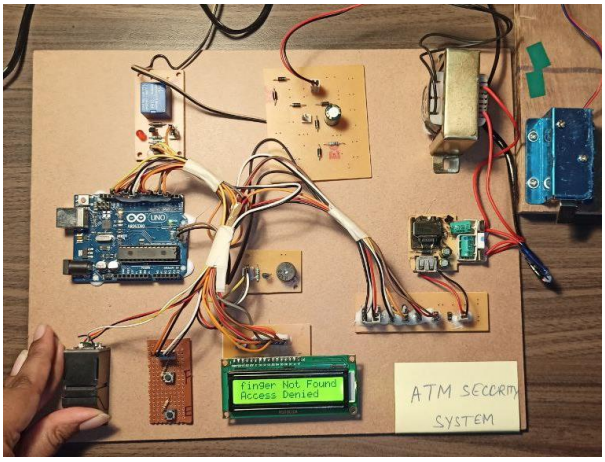


*Figure 10 Access denied to unauthorised access*

To provide power to the solenoid lock, we utilize an AC power supply sourced from household supply boards. This is achieved by using a DC adapter along with a step-down transformer, which converts the 230V AC input to a 12V AC output. Since we require a 12V DC supply to control the solenoid lock, we employ an RPS board that converts the 12V AC to pulsating DC through a rectifier section and then smoothens it using a capacitor.

Additionally, we utilize a regulated power supply board to convert the 230V AC input to a 5V DC output, which is distributed throughout the input and output modules using a breadboard.

The fingerprint scanner serves as the authorization mechanism for individuals accessing the system, while the electromagnetic relay is responsible for operating and unlocking the solenoid lock. The relay is utilized to introduce a delay and provide electrical isolation between high-voltage and low-voltage systems, ensuring the protection of both the low-voltage systems and the users.

The LCD screen is used to display the system status, and the piezo buzzer is employed to alert unauthorized access attempts. Two control buttons are incorporated to facilitate the formatting of existing users and the enrollment of new users.

To operate the push buttons, one needs to hold the button and then press and release the reset switch on the Arduino. The button should be held until the status is displayed on the LCD screen. Once the enrollment process is successfully completed, the reset button on the Arduino should be pressed once.

These connections and components work together to create a functional and secure ATM security system based on the Arduino board.

## 6. CONCLUSION

In conclusion, the proposed security-based ATM theft detection system using biometric fingerprint technology and the integration of various hardware components marks a significant advancement in the field of ATM security. This innovative system effectively overcomes the drawbacks of existing technology by providing biometric registration for accessing ATM rooms and ensuring the integrity of the ATM cash loading system.

By leveraging the R307 fingerprint module, the system offers a robust and reliable authentication method, allowing only authorized individuals to enter the ATM room. The utilization of the Arduino UNO microcontroller, along with components such as the relay, solenoid lock, buzzer, and LCD module, enhances the system's functionality and security.

Overall, this project represents a significant step towards enhancing ATM security, mitigating the risk of theft and unauthorized access. By combining biometric fingerprint technology with carefully selected hardware components, the system provides a robust and reliable security solution. Financial institutions and ATM users can benefit from the improved security measures, offering peace of mind and safeguarding valuable assets.

## 7. FUTURE SCOPE

The realm of IOT-based ATM security systems holds exciting potential for research and development. An area of interest lies in fortifying data security by integrating advanced encryption techniques. These methods would play a crucial role in enhancing the protection of sensitive user data and transaction records during communication between ATMs and central servers. By securing this data against unauthorized access and tampering, a higher level of trust and security can be established within the ATM network.

Furthermore, the integration of machine learning algorithms presents an avenue for proactively identifying irregular patterns and potential fraud within ATM transactions. Such algorithms can be trained to recognize deviations from normal usage behavior, triggering alerts for further investigation. In parallel, the application of block chain technology offers a novel approach to ensure the integrity and transparency of ATM transactions. Through its decentralized and tamper-resistant nature, block chain can potentially mitigate risks associated with data manipulation or unauthorized alterations, fostering a secure environment for financial operations.

In conclusion, the future landscape of IOT-based ATM security systems beckons for comprehensive research and innovation. Through avenues such as advanced encryption, machine learning for anomaly detection, block chain integration, biometric authentication, and tailored intrusion detection systems, the security and reliability of ATM operations can be significantly enhanced, ensuring a secure and trustworthy banking experience on a global scale.

## REFERENCES

[1] 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

[2] 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.

[3] 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

[4] 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

[5] Rendy Munadi; Arif Indra Irawan; Yuman Fariz Romiadi 2019 International Conference on Mechatronics, Robotics and Systems Engineering (MoRSE) DOI: 10.1109/MoRSE48060.2019.8998716

[6] Prachi; Markande, Shriram (2016). [IEEE 2016 International Conference on Inventive Computation Technologies (ICICT) - Coimbatore, India (2016.8.26-2016.8.27)] 2016 International Conference on Inventive Computation Technologies (ICICT) - Design and implementation of anti-theft module for ATM machine. , (), 1– 4. doi:10.1109/INVENTIVE.2016.7830141