



ADVANCED ATM SECURITY WITH AUTOMATIC DOOR LOCK SYSTEM USING ARDUINO PROCESSOR

¹K. Sreenivasa Rao, ²SM. Mohammad Eliyas, ³L. Manjunath, ⁴M. Meghana,
⁵P. Kiran Kumar

¹Associate Professor, ^{2,3,4,5}Scholar

^{1,2,3,4,5}Department of Electronics and Communication Engineering

^{1,2,3,4,5}Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh, India.

Abstract : Automatic Teller Machines can be used for a variety of purposes, most notably cash withdrawals. ATM customers will do billions of transactions and make use of a wide range of services. Meanwhile, because there is little security, the number of robberies in ATMs is also large. Therefore, it is necessary to suggest new technologies that can solve this issue. Our study's primary goal is to reduce the number of ATM robberies. The MEMS sensor is utilized here to detect changes in the ATM's position whenever a heist takes place. The ATM's vibration sensor detects vibrations and initiates the appropriate action. The Arduino processor receives information once the vibration and/or position change are detected. Subsequently, the ATM room door is shut using a DC motor, and a relay is set off to discharge gas into the ATM, rendering the burglar unconscious. An ESP Cam will be utilized to take pictures of the event, and a second relay will be set off to automatically lock the ATM door. The message is sent by the GSM module together with an OTP to the relevant bank authorities and a nearby police station. Eventually, the buzzer will sound an alarm. To unlock the ATM door, enter the OTP using the keypad at the door; the OTP will be shown on the LCD. ATM systems are safeguarded without the need for guards thanks to this system, which also makes it simple to apprehend the thief.

Keywords: Automated Teller Machine, Robbery detection, GSM notification, Solenoid lock, Security measures.

INTRODUCTION

ATMs are becoming among the most crucial tools in our daily lives in the current situation. We are able to take money out of the authorized account whenever we want thanks to this feature. With the assistance of an ATM, a user can carry out a number of banking operations, including cash withdrawals and money transfers. The frequency of crimes involving ATMs has been shown to be rising, hence it is imperative that ATM security be improved [1]. Even though the banks have security guards stationed at the ATM locations, the security setup is insufficient to protect the building in the event that a group of thieves attempts to take the ATM. In recent times, there have been numerous instances where a mob of individuals broke into an ATM, overwhelmed the guards, and took money out of the machine. Generally speaking, one person cannot control a group of robbers [2].

Because the need for ATMs is growing daily, security is an important consideration. Modern demands call for security systems, which detects theft. Transaction security for authorized user identification was offered by earlier technologies. However, this is only applicable to safe ATM transactions. While GSM-based approaches are also employed for the same reason, earlier research concentrated on biometric techniques to improve ATM security. Certain systems, however, combine the two methods. A one-time password (OTP) is issued to the transaction's registered phone as part of GSM-based security [3]. Each user is given a special card and an ID code that they can use to conduct all transactions in secret and anonymously. [4] A total of 212,530 thefts and 4,439 robbery incidents occurred in 2007. Similarly, in 2010 and 2011, there were 269,410 thefts and 4,409 robbery cases, as well as 270,109 thefts and 4,509 robbery cases. Such that for the last 12 years, the number of theft and robbery incidents has gradually climbed. Theft and robbery account for a large percentage of crimes against financial organizations over 90% and crimes against ATMs have increased as a result of the growth in external ATM usage and its constant vulnerability to crime. Thus, preventing robberies is greatly aided by the use of automatic security systems. The goal of this project is to create a system that will assist in catching the robbers when they try to take the ATM. In addition, this technology will serve as an ATM facility security barrier [5].

The idea for using MEMS sensors and vibration detection is what the suggested project comprises of. Every time someone tries to damage, force open, or move the ATM machine, these sensors will produce a signal. The authorized person of the bank and police station will receive an SMS through the GSM module informing them of the situation upon detection of such a signal. Additionally, we are employing a wireless camera so that the authorized person can have the incident images on their phone in such circumstances [6]. Subsequently, the DC pump sprinkler system within the ATM chamber will initiate, dispersing a chloroform chemical to induce unconsciousness while concurrently sounding an alarm. Operational The proposed project aims to enhance security for ATM machines and expedite the identification of robberies through the utilization of an embedded system [7].

LITERATURE REVIEW

A wireless phone system that facilitates financial transactions for customers, specifically cash withdrawals. Globally, 3 million bank branches have been established in response to advancements in the ATM sector. ATMs are remembered by the use of a reversible debit card or a mobile application with a chip card that needs a unique key. It is more varied and has fewer safety data than CVVC. The client's personal identification number (PIN) is entered to provide authentication. ATM thefts are nevertheless becoming more common in society in the interim. The ATM robbery target is the equipment mounted on the ATM that is not secured. Despite the presence of guards at ATMs, thieves are nevertheless able to carry out the break-in with the help of certain cunning techniques. GOVT has a few millions and crores of cash as a result.

In 2023, M. Nagabushanam et al. [8] built a complex system that responds to vibrations, instantaneously closing the ATM door and generating an alert. They did this by leveraging the ESP32 platform and Blynk IoT. The surrounds are alerted by an audio signal, which is communicated through the Blynk IoT app. Using the Blynk app for command decoding, a customized Android app is used to control the system. By combining these elements, an intelligent Internet of Things security solution with possible practical uses is to be developed. A comprehensive solution to prevent ATM theft and guarantee a timely response to security incidents is provided by the project, which addresses existing security gaps in alarm systems and surveillance cameras.

In 2020 saw the proposal by K. Gavaskar, S. Preethi, et al. [9] for the notion that in the event of a physical assault on the ATM, the neighborhood is also informed and information about the assault is conveyed via IoT. A mobile application receives all of the sensor data and sends an alarm to bank officials.

In 2018, Taha Ayesha et al. [10] developed a solution that uses an embedded Linux platform to link a Raspberry Pi with an RFID module, a keypad, a display, and a USB camera to safeguard ATM transactions. The security function is given consecutive acts, like ATMs. A Raspberry Pi processor and GSM module are used to send an SMS alert to the card holder when the user swipes the card containing the person's photographed.

In 2017, L. Nagarajan et al. [11] presented a cost-effective smart locker security system as part of their system that explores the possibilities of the Internet of Things (IoT). The solution optimizes resource consumption and offers effective security measures by utilizing Internet of Things capabilities. Together, these findings highlight the significance of using a variety of strategies to strengthen ATM systems as technology breakthroughs continue to alter the security landscape. A possible path for building robust defences against changing threats in the financial transaction's domain is the integration of mobile technologies, intelligent sensors, and biometrics. These bases can be expanded upon by future research to further improve ATM systems' integrity and security.

In 2017 (ELSEVEIR), by Karen Renaud et al. [12] a textual assessment of the HCSP analysis was published. We determined their field alterity using the waves that Bødker and Harrison et al. suggested. We demonstrated why it appeared from the main conference journals of the HCSP that we would now also be working on first surge. Papers from the third and fourth waves were beginning to surface, based on a cursory look at a few of the IT conferences. In order to guarantee that our business is established and to enhance the security of personal computers, we have put forth a number of suggestions and ideas.

In 2016, H Swathi et al. [13] introduced a dynamic Personal Identification Number (PIN) that is produced by the user and sent by SMS to their mobile phone in order to solve security risks associated with traditional ATM access methods in 2016. A Global System for Mobile Communications (GSM) module transmits this PIN to the ATM. This dynamic PIN system is more flexible and secure than traditional approaches since the user-defined PIN (UDPIN) can be modified for every transaction. Prototype implementation shows enhanced security, removing worries about misplaced access cards and facilitating streamlined deactivation procedures. It turns out that the system is a more practical and efficient way to secure ATM transactions.

In 2016, K. Hema Sen, Siva prasad et al. [14] promised the development of a cuttingedge anti-theft ATM system. In this project, a sophisticated and economical mobile payment security solution was proposed. To prevent robbers from accessing it, it can be hidden inside the ATM. The suggested method is not like the current ATM theft and hacking from a distance. Dependable building is suitable and reasonably priced.

In August 2016 by G. Jakeer Hussain et al. [15] This suggested solution was created through the development of integrated features for all hardware and software components that are successfully constructed and used through testing. He placed a MEM sensor in the ATM's locker area in order to use it in this system. The data is kept in the embedded server, the door automatically closes when a user tries to open the money locker, and the mems sensor is triggered.

EXISTING SYSTEM

3.1 Traditional ATM Security System

ATM security is currently underequipped since CCTV-based security solutions are used to supply it. The camera in these systems continuously records and stores the information on the bank server. The system produces a human-machine lag, and further assistance is given by a watchman (a human security guard), who is similarly ill-prepared. Other than these fundamental safeguards, no other feature is accessible. This contributes to rising forgeries rates and raises the possibility of actual ATM thefts.

3.2 Advanced Anti-Theft ATM Security using Raspberry Pi

This article describes the current system, which is a sophisticated security system installed in ATMs.

Block diagram:

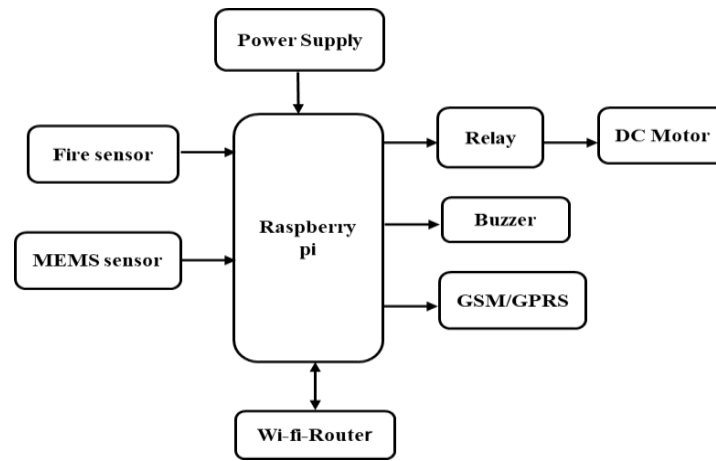


Fig1: Existing block diagram

IR sensors, a DC motor, a Raspberry Pi, a MEM sensor, a GSM module, a buzzer, a fire/smoke/gas sensor, and a camera linked to an embedded web server are some of the parts that make up the system. There are several steps in the process:

1. Entrance Door Security:

- When a person is present, infrared sensors identify them and alert the Raspberry Pi.
- A DC motor is turned on by the Raspberry Pi, which opens the front door after it receives the signal.
- As the person enters, the camera takes four to five pictures simultaneously.

2. Money Locker Security:

- Vibrations are detected by a MEMS sensor installed in the money locker area.
- The Raspberry Pi is alerted by the MEMS sensor if someone tries to rob the money locker by smashing or cutting it open.
- The Raspberry Pi reacts by shutting the door, discharging an unconscious spray, utilizing GSM to send alerts to the bank authorities and police, turning on a buzzer for general public notice, and taking pictures of the incident.

3. Fire/Smoke/Gas Detection:

- The ATM has an installed gas, smoke, or fire sensor.
- The sensor takes pictures, triggers an alarm, and sends notifications in the event of a fire or gas leak.

4. Embedded Web Server:

- Images are stored and accessed by the system via an embedded web server.
- As an operating system, Linux is employed.
- The web server software is called Apache.
- The database server is no other than MySQL.
- Programming dynamic web components is done with Perl or PHP.

Limitations of the Existing System:

- Cost: Installing a sophisticated security system like this could be costly, particularly for smaller ATM locations.
- Maintenance: Regular maintenance and updates may be necessary for complex systems, which raises the cost of operation.
- Lower prediction accuracy: It is not always possible to locate the burglar when relying just on the MEM sensor.
- Resource Requirements: The scalability and responsiveness of the system may be impacted by resource constraints on the embedded web server.

In conclusion, even though the current system has cutting-edge security features, it is crucial to take into account the related expenses, upkeep needs, possibility of false alerts, and privacy issues. The system's long-term efficacy depends on regular updates and compliance with laws [11].

PROPOSED SYSTEM

This combination of the module solenoid lock, MEMS sensor, vibration sensor, IR sensor, and ESP cam is suggested for ATM security.

4.1 Description

An ATmega2560 chip with 54 digital I/O pins, 16 analog input pins, and a clock speed of 16 MHz powers the Arduino ATmega2560, a multipurpose microcontroller. While it runs at 5V, running it between 7 and 12V is advised. Ample resources for a variety of applications are provided by its 256 KB of flash storage, 8 KB of SRAM, and 4 KB of EEPROM. Using microfabricated mechanical elements, the MEMS accelerometer a sensor for Micro Electro Mechanical Systems measures acceleration. It usually connects using SPI or I2C protocols. There are several ranges available, such as $\pm 2g$, $\pm 4g$, $\pm 8g$, or $\pm 16g$, and the sensitivity is typically expressed in milligrams. Conversely, the vibration sensor transforms mechanical vibrations into electrical impulses; it is typically piezoelectric or piezoresistive. Its output might be based on frequency, digital, or analog voltage. When combined, these parts create a potent sensor and control system that may be used for everything from detecting movement to monitoring the health of structures.

Block Diagram

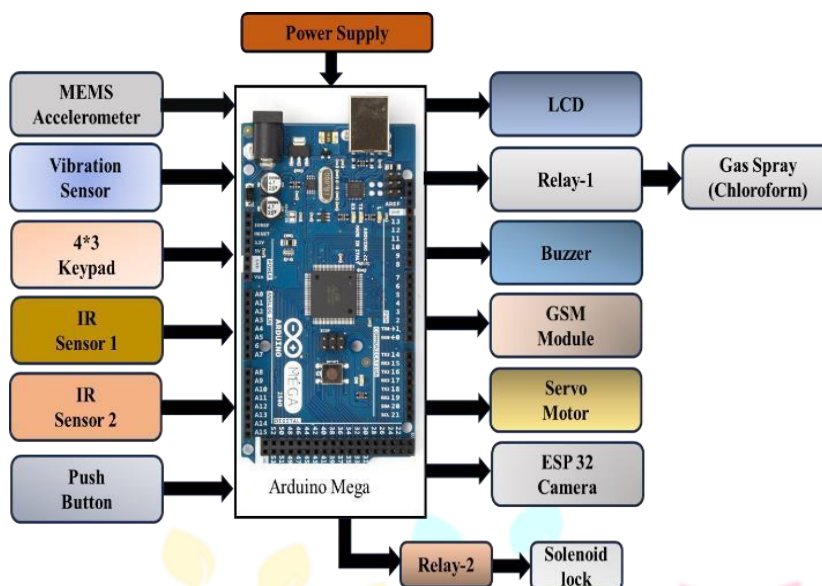


Fig2: Proposed block diagram

Functionality:

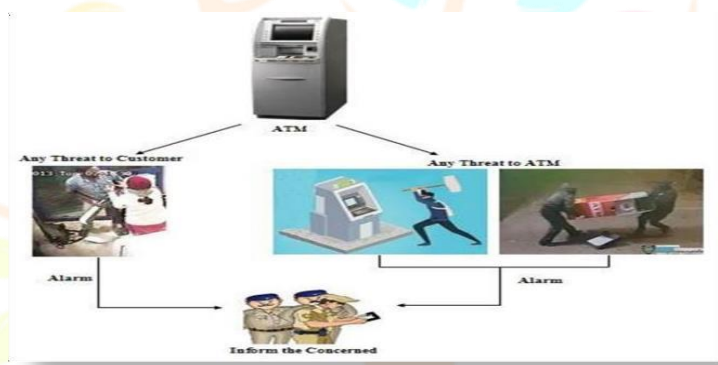


Fig3: Various Activities

The ATM room's doors are initially closed. The IR sensor recognizes when someone enters the space and signals the processor to use a Servo motor to open the door and will be closed after 5-seconds. An alarm will go off to forcefully close the door if someone enters the room and tries to do so against their consent. Here, the vibration and MEMS sensors are primarily used to identify robberies.

The ATM is being detected here for changes in position using the MEMS sensor, and vibrations from the ATM (such as those caused by a hammer or machine) are being detected by the vibration sensor. Information about vibration and/or positional changes is transferred to the Arduino CPU. After locking the ATM room door with a solenoid lock, a relay will be set off, releasing gas within the machine to render the burglar unconscious (as opposed to allowing them to flee). The incident's photos will be taken using the ESP Cam. The processor will store it.

The message is sent by the GSM module together with an OTP to the relevant bank authorities and a nearby police station. Eventually, the buzzer will sound an alarm. To unlock the ATM door, enter the OTP using the keypad at the door; the OTP will be shown on the LCD. This technology allows ATMs to be secured without the need for guards, and it makes it simple to carry out the crime.

V. EXPERIMENTAL RESULTS

The experimental results are based upon the Arduino Processor and the hardware components arrangement figure is shown below.

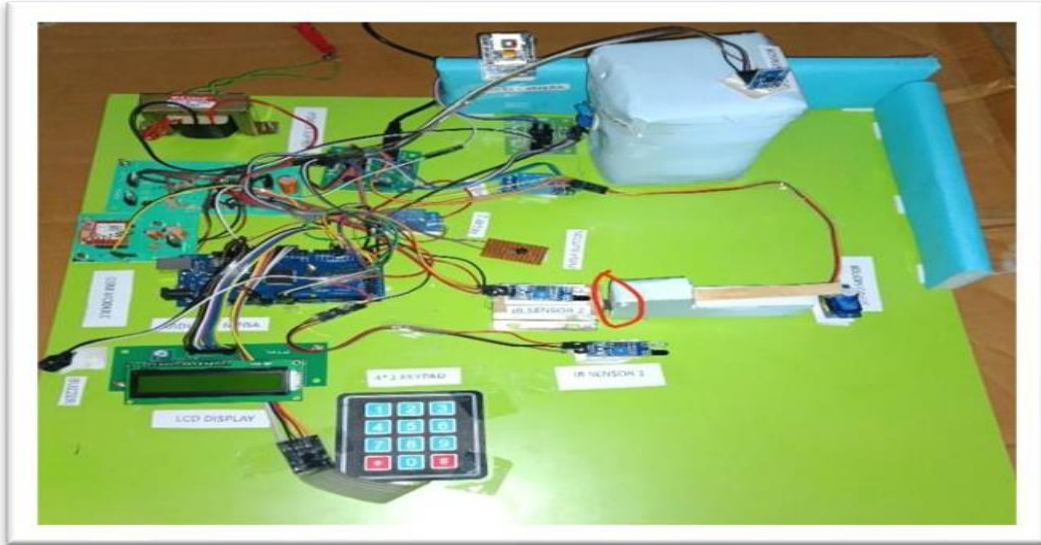


Fig4: Hardware Circuitry arrangement



Fig5: The LCD display indicates that the "GSM Module Initialized" this state occurs as soon as the power source is applied.

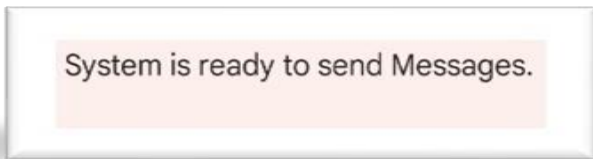


Fig6: The system notifies registered mobile phones via text message that "System is ready to send messages" and displays on the LCD that the ATM is safe.



Fig7: This figure shows the status of system while opening of the door



Fig8: This figure shows the status of system while closing of the door



Fig9: The sensors may identify an intrusion as robbery if the intruder is attempting to move or harm the system. The system then turns on and displays the ATM's status on the LCD.



Fig10 : Various actions when after theft then the system will become an idle state following this procedure. Additionally, the LCD displays the result "Theft Found Door is Locked".



Fig11: LCD Message for OTP. Pressing the * key will cause the OTP to appear on the LCD and be sent to the registered mobile device. The door will unlock if we input the right OTP. Otherwise, we can regenerate the OTP by pressing the * key once more if we enter the wrong one.



Fig12: LCD Message after OTP verification then, press the reset button on the system if we want to utilize it again.

CONCLUSION

To sum up, the integration of solenoid lock, MEMS sensor, vibration sensor, IR sensor, and ESP Cam, as suggested, provides a comprehensive approach to improve ATM security and reduce the likelihood of thefts. The technology considerably lowers the possibility of successful robberies by identifying unauthorized access attempts and swiftly launching the necessary measures, such as closing the ATM room door and turning on gas discharge to render intruders helpless. The incorporation of real-time alert features through the GSM module guarantees prompt connection with pertinent authorities, enabling quick action and the capture of offenders. An OTP-based keypad entry system is also included to improve security and make access easier for authorized staff. All things considered, this cutting-edge security system effectively safeguards ATMs, doing away with the necessity for human security guards and improving user and financial institution safety.

REFERENCES

- [1] 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.
- [2] 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.
- [3] Jothish Kumar M; Ramakrishnan Raman; S. Prabhakar; T. Bernatin.

- [4] 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.
- [5] R1, Kalaiselvan .M2, Mr. R. Rajagopal3 "Advanced ATM Security System Deepa" International conference on. IEEE, 2016.
- [6] 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.
- [7] Ai based E-Atm security and surveillance system using blynk-lot server international conference on. Ieee, 2022.
- [8] K. Gavaskar, u. S. Ragupathy, s. Elango, m. Ramyadevi, "Iot based security system for organization", department of eee, b.l.d.e. a's v.p. dr. P. G. Halakatti college of engineering and technology, vijayapura-586103 vijayapura, karnataka, india, ©2020 ieee.
- [9] 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.
- [10] 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.
- [11] L. Nagarajan "iot-based low-cost smart locker security system".
- [12] 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.
- [13] 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.
- [14] 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.