ADVANCED ATMCRIME PREVENTION SYSTEM BYUSING WIRELESS COMMUNICATION

Dr. S. L. Prathapa Reddy
Professor
Department of Electronics and Communication Engineering
KSRM College of Engineering
Kadapa, Andhra Pradesh
slpreddy@gmail.com

N. Venkata Sreeja
Student, Department of ECE
KSRM College of Engineering
Kadapa, Andhra Pradesh
nagareddyvenkatasreejareddy@gmail.Com

K. Mounika
Student, Department of ECE
KSRM College of Engineering
Kadapa, Andhra Pradesh
mounikakuruba05@gmail.com

N. Sai Jithendra
Student, Department of ECE
KSRM College of Engineering
Kadapa, Andhra Pradesh
saijithendran03@gmail.com

P. Vasanth Reddy
Student, Department of ECE
KSRM College of Engineering
Kadapa, Andhra Pradesh
reddyvasanth2001@gmail.com

P. Praveen Kumar Reddy
Student, Department of ECE
KSRM College of Engineering
Kadapa, Andhra Pradesh
p.praveen2329@gmail.com

Abstract **– The purpose of this article is to design and construct an RFID and Internet of Things-based bank locker security system that can be put in homes, workplaces, and banks. For safe access, the system has a door locking mechanism that instantly activates, verifies, and authenticates users. Compared to other systems, passive RFID and IoT technology are more secure. A microcontroller, RFID reader, Internet of Things, and LCD make up the system. The submissive tag's ID number is read by the RFID reader and transmitted to the microcontroller. The microcontroller requests a master password to open the locker via SMS to the verified individual's mobile number if the ID number is legitimate. The locker is opened if the passwords match; if not, it stays locked. For every user, the system creates a log with their check-in and checkout details. A bulb is turned on if the data from authorized personnel's cards matches the information read by a smart card reader. Upgrading to a Thumb/IRIS identification system and incorporating IoT technology to notify departments of unwanted access attempts are two ways to improve the project.**

I.INTRODUCTION

A lot of embedded systems products employ microcontrollers. The Microprocessor (or microcontroller) in an embedded product is used to do a single task and only one task. Since the CPU inside a printer just does one thing get data and print it it is an example of an embedded system. Despite being the favoured option for many embedded systems, microcontrollers are occasionally insufficient for the job. Because of this, several general-purpose microprocessor manufacturers, including AMD, Cyrix, Motorolla, and Intel, have aimed their products at the upper end of the embedded market in recent years. Reducing space and power consumption is one of the embedded system's most important requirements. By adding additional features to the CPU chips, this can be accomplished. In addition to having some type of I/O and ROM on a single chip, all embedded CPUs have minimal power consumption. The tendency in higher-performance embedded systems is to incorporate an increasing number of functionalities on the CPU chip and provide the designer the freedom to choose which feature to employ.

II. LITERATURE SURVEY

A literature survey on an "Advanced ATM Crime Prevention System using Wireless Communication" would explore ATM crime prevention techniques,wireless communication in ATM security, crime detection and recognition, data encryption and security protocols, machine learning and artificial intelligence in crime prevention, and case studies and real-world implementations of advanced ATM security systems. The survey would examine existing methods, technologies, and applications of these technologies in ATM security, as well as their effectiveness in preventing various types of ATM crimes and their practical challenges.

III. EXISTING SYSTEM

ATM security systems using GSM and MEMS are gaining attention in the embedded systems industry. This project uses an ATMEL-based AT89S52 Microcontroller to monitor the MEMS module, GSM, and motor. The system alerts customers in dangerous situations with a voice annunciator and an emergency switch

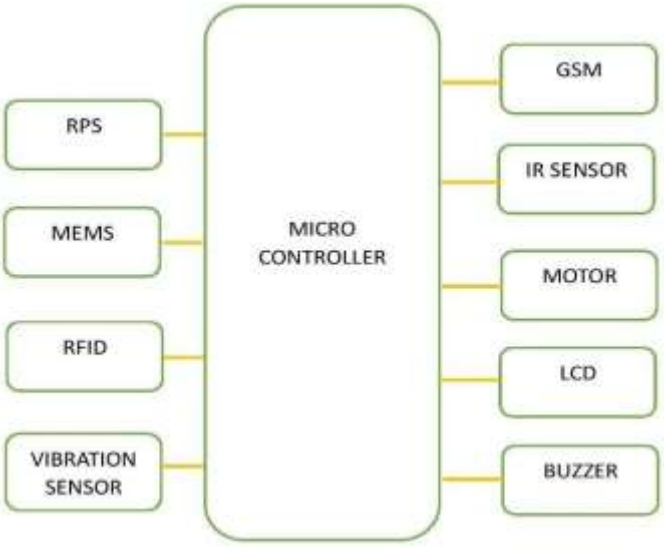

Fig . Block Diagram of Existed System

IV. PROBLEM STATEMENT

In recent years, automated teller machines (ATMs) have become a common target for various criminal activities, including card skimming, card trapping, cash trapping, and physical attacks on users. These crimes not only result in financial losses for individuals and financial institutions but also undermine trust in the banking system and compromise public safety. Therefore, the development of effective ATM crime prevention measures is crucial to safeguarding both the financial assets and the well-being of ATM users.

V. OPERATION OFPROPOSED SYSTEM

The proposed system aims to prevent ATM crimes by alerting authorized people and servers using SMTP protocol and sending an image of the thief to nearby police stations using IoT applications. A vibrating sensor activates a buzzer when an unauthorized person tries to clone the ATM, identifying and capturing the wrong person. The system also prevents card skimming and other ATM crimes by sending a picture of the thief to the user's email ID

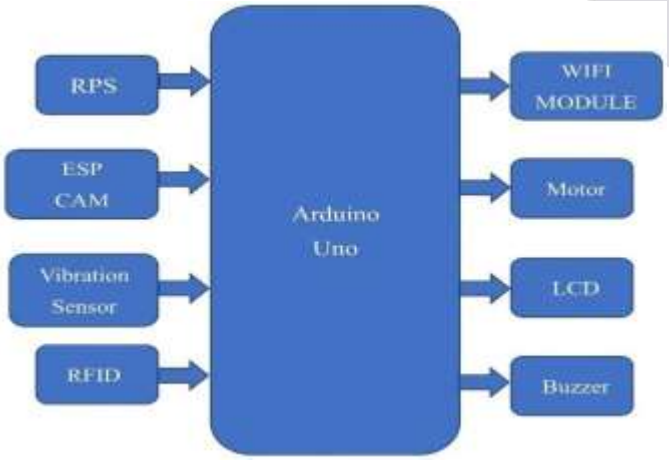

Fig . Block Diagram of the Proposed System

VI. POWER SUPPLY

Conversion of 230V alternative current into 5V direct current by using the following steps and diagram. Here we are using components that are

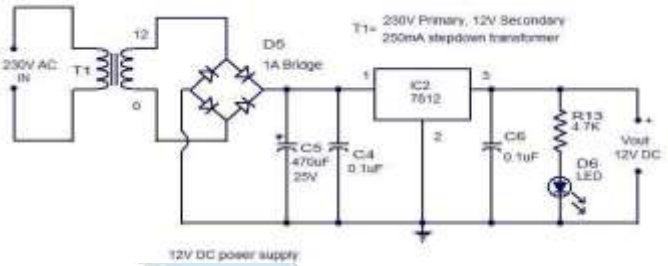

Fig . Power Supply

VII. Arduino Board

The Arduino line of microcontroller boards is intended for use in electronic design, experimentation, and prototyping. It is based on an ATmega microcontroller, which is a full-fledged computer featuring input/output pins, a CPU, RAM, and Flash memory. These pins can be used by Arduinos to connect sensors, LEDs, motors, speakers, servos, and other devices that can read or produce analog or digital voltages. They can operate with or without a keyboard or screen and are USB-connected to a computer.

Fig . Arduino Board

VIII. ESP32 CAMERA

The ESP32-CAM is a development board that enables face recognition, video streaming, surveillance, and photo capturing. It has an OV2640 camera, GPIOs, and a microSD card port.

Fig.ESP32Cam

IX. RFID

Fig.3: Existing system

The RFID Reader Module 125KHz is a popular tool for Radio Frequency Identification projects, allowing for direct interface with microcontrollers using UART Wiegand26 output formats. Its 2.54mm output pin pitch allows for easy breadboard integration. The EM-18 RFID Reader is small, easy to use, and can work with any 125KHz RFID tags, providing UART/RS232 communication

Fig. RFID Reader

X. VIBRATION SENSOR

In order to provide an adjustable digital output based on the degree of vibration, this module includes an LM393 comparator chip, an adjustable potentiometer, and a vibration sensor. Both raising and lowering the sensitivity to the appropriate level can be accomplished by adjusting the potentiometer. When activated, the module outputs a logic level high (VCC); otherwise, it emits a low (GND). Furthermore, an onboard LED is activated upon activation of the module.

Fig. Vibration Sensor

XI. Wi-Fi MODULE:

All of the components required for wireless communication utilizing Wi-Fi technology will be integrated into a Wi-Fi module. It usually consists of a microcontroller or CPU, memory, support circuitry, and a system-on-chip (SoC) or module with a Wi-Fi radio transceiver. Devices can connect to wireless networks, access the internet, share data, and interact with other devices within the Wi-Fi network coverage area thanks to the Wi-Fi module

Fig . Wi-Fi Module.

XII. MOTOR

Industrial applications frequently use brushless DC motors, which use a DC without brushes. They are made up of a stator, permanent magnets on the rotor, and a revolving armature with an electromagnet. The rotor rotates 180 degrees when an electric current is delivered, which flips the magnetic field. In contrast, brushless DC motors flip the electromagnetic field inside out, doing away with the requirement for brushes. The electromagnets that turn the rotor 360 degrees are charged by a computer.

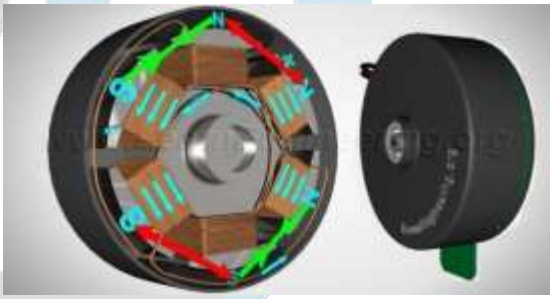

Fig. Brushless DC Motor

XIII. LCD (LIQUID CRYSTAL DISPLAY)

The technology used for displays in notebooks and other tiny computers is called liquid crystal display, orLCD. Similar to gas-plasma and light-emitting diode (LED) technologies, LCDs enable displays that are significantly thinner than cathode ray tube (CRT) technology. Due to its ability to block light instead of emitting it, LCDs use a lot less electricity than gas-display and LED displays.

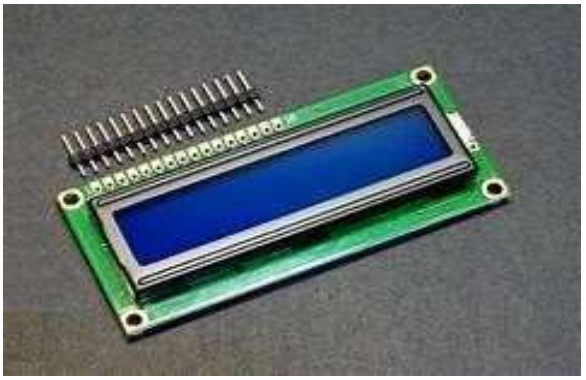

Fig . Liquid Crystal Display

XIV. BUZZER:

An alarm is often similar to a buzzer. Every time we push the switch button, the machine is activated and an output, such as an alarm sound, is produced. There are two pins on the buzzer. The microcontroller's data pin is attached to the negative end. The microcontroller's Vcc is linked to the positive end.

Fig. Buzzer

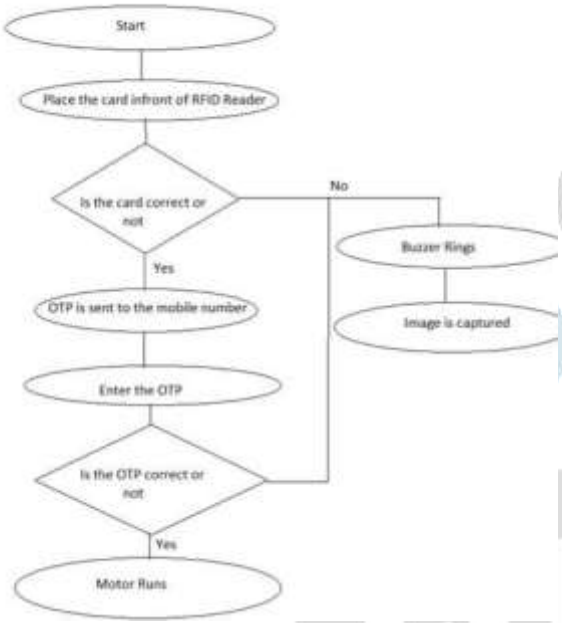

Fig . Flow Chart

STEP: 1. initialization of the system.
2. Check the system parameters (sensor, smart card).
3. Check the vibrating sensor.
4. Send a message if the sensor is activated.
5. Check the authentication for sending the im age to mail.

XV. RESULT

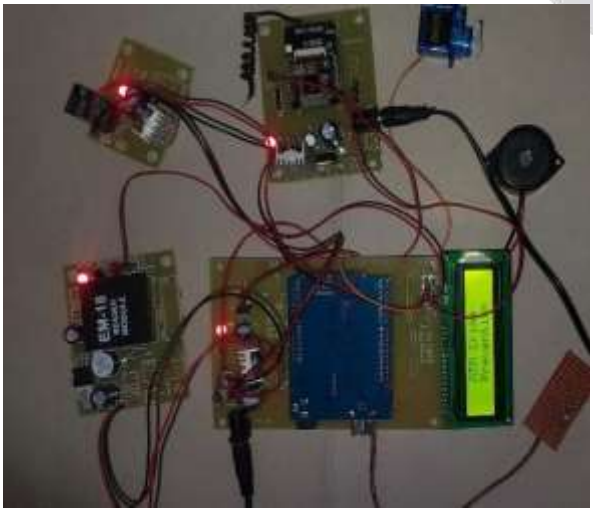

Fig. Project Kit

Hence, the result of the Advanced ATM Crime Prevention System using Wireless Communication project is that whenever there is a chance of theft at that time in the vibrating sensor the mercury level meets the point to activate the vibrating sensor and then Buzzer will be initiated to alert the Crime. There will be an alert message through email to the user whenever the card credentials are incorrect and the buzzer will be initiated at this time also.

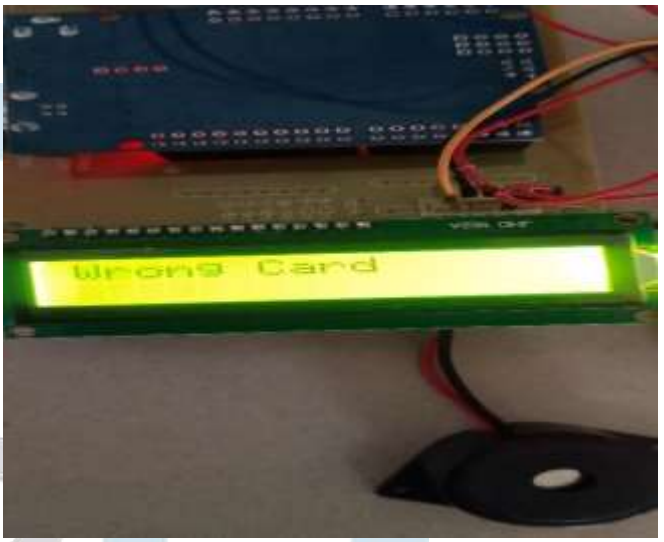

Fig. Display of the wrong card

Fig. E-mail proof

The most amount of bits that may be concealed in a picture is referred to as its capacity. Two tests of image quality are the peak signal to noise ratio (PSNR) and the noise to signal ratio (SNR).

When a wrong card is placed or a wrong password is entered then automatically the image copy of the person who is involved in card skimming will be sent to the authorized mail of the user. Then it will be helpful to identify the person who was involved in the ATM crime. Buzzer also will be initiated and the card will be locked to avoid thefts

XVI. CONCLUSION

Utilizing the stability and dependability of SMART CARD features, ATM security was implemented through the use of SMART CARD recognition and a Wi Fi module. Furthermore, the system still has the original verification techniques that involved entering the owner's ID that the controller sent. For the stability and dependability of owner recognition, the security elements were significantly improved. The entire system will be constructed using embedded technology, which makes it more dependable, user-friendly, and safe. Furthermore, the system incorporates the ATM's security, which is as follows: A temperature sensor is used to prevent fires in the ATM center. The sprinkler will be turned on if there is a fire. Vibrating sensors determine tilt with respect to gravity using a micromachined acceleration sensing element with a DC response.

XVIII. FUTURE SCOPE

Fingerprints are being used as an authentication method in this project. Future initiatives will rely on biometrics, such as fingerprints. Since each person's fingerprints are permanently unique, it will be quite simple to apply in the future. Among the numerous benefits the system will offer are the following: we will remember our fingers, users will respect them, scammers will be scared of them, and privacy will be protected. Because each finger is unique, fingerprints do not change over time, and they prevent unwanted access, allowing each individual to have 10 simple applications for identity-based on global identification. Biometrics will be the primary way of authentication and security in future systems, which will eradicate fraud and forgeries in many enterprises.

XIX. REFERENCES

1. S. B. Singh and P. K. Gupta, " Wireless Communication and Network Security," 1st ed., Springer, 2023, ch.4, sec. 2, pp. 85– 105
2. [L. N. Choudhury and T. M. Brown, " Real-time Monitoring of ATM Security Using IoT," Int. Symp. Internet of Things, San Francisco, CA, USA, June 5-7, 2022, Paper no. 123. Handbooks:
3. "Handbook of Wireless Networks and Mobile Computing," 2nd ed., Wiley, Hoboken, NJ, 2023, pp. 45– 67. Manuals:
4. Tech Press, "Wireless Communication Security: A Practical Guide," 1st ed. (2022). Accessed: October 21, 2023.[Online]. http://www.techpress.com /wirele Available: ss-security-guide Software:
5. Arduino IDE for programming and uploading code, (2023), Arduino. Accessed: October 21, 2023. [Online]. Available: https://www.arduino.cc/en/software. Journals [Print]:
6. J. K. Doe and A. B. Smith, " Enhancing ATM Security Using Wireless Sensor Networks," Journal of Network Security, vol. 14, no. 5, pp. 210– 220, May 2023. Journals [Online]:
7. R. K. Patel and M. A. Ali, "Wireless Communication Technologies for Secure ATM Transactions," International Journal of Inform ation Security, vol. 11, no. 4, pp. 150– 162, April 2022. Accessed: October 21, 2023. [Online]. Available: https://www.ijinfosec.com/articles/2022/04/002
8. Jacobs, B. & Poll, E. (2010) Biometrics and Smart Cards in Identity Management..
9. G. DeMicheli, Synthesis and optimization of digital circuits. McGrawHill, 1994.
10. R.Drechsler and A. Breiter, "Hardware project management - what we can learn from the software development process for hardware design,"in 4th Conference of Informatics and Information Technologies, 2003.
11. Adeoti, J. (2011). Automated Teller Machine (ATM) frauds in Nigeria: the way out.
12. Rodriguez A. B. (2010). Cryptographic Function in a smart card
13. International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014.
14. International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X
15. International Journal of Control, Automation, Communication and Systems (IJCACS), Vol.1, No.2, April 2016.