BANK LOCKER SECURITY SYSTEM USING EMBEDDED SYSTEM

Shashidhara B P[1], Shreya N [2], Sristi Malashetti [3], Priyanka Panduranga Palekar [4]
Madhumathy P [5]

[1] Student, Department of Electronics and Communication Engineering, RV Institute of Technology and Management, Karnataka, India
[2] Student, Department of Electronics and Communication Engineering, RV Institute of Technology and Management, Karnataka, India
[3] Student, Department of Electronics and Communication Engineering, RV Institute of Technology and Management, Karnataka, India
[4] Student, Department of Electronics and Communication Engineering, RV Institute of Technology and Management, Karnataka, India
[5]Department of Electronics and Communication Engineering, RV Institute of Technology and Management, Karnataka, India

ABSTRACT

The main objective of this paper is to use diverse technologies to create a bank locker security system. A door-locking system utilizing RFID and GSM technology, combined with fingerprint scanning and IR sensor activation, will be used to enable secure access to bank lockers. This technology may unlock the door while simultaneously activating, validating, and approving the user. As a result, it appears that the specified system is very secure. It is possible to accomplish that by integrating hardware and software. The ARM LPC 2148 microcontroller can be used to implement the hardware component. The program will be written in C or assembly language, and the software portion will be completed using Keil µVision. The goal is to develop a system that is inexpensive, uses little power, is simple to use, and is compact in size.

Keyword: - *GSM, RFID, Fingerprint, IR sensors, Keyboard, ARM LPC 2148 Microcontroller*

1. INTRODUCTION

It is said that a bank locker is the safest place to store valuable necessities. In light of this, the security of these lockers has drawn considerable attention, particularly in urban areas. As a result, most people either install multiple locks or use a digital solution like alarm systems to address the safety danger. Alarm systems use a number of sensors and come in a wide range of designs. The sensor system might not be reliable at all times. However, it can recognize various environmental alterations, which are assessed and then trigger an alarm based on a pre-defined value. Biometrics, including GSM, RFID, and PIR sensors, exceed other technologies in terms of security and dependability. The great performance of fingerprint scanning for identification is one of its advantages.

Therefore, we use fingerprint technology as an identity module. The goal is to create a prototype to handle the serious problem of security for critical organizational systems, including bank lockers with the appropriate authorization. An antenna or coil, a transceiver (with a decoder), and a transponder (RF tag) with customized information are the components of an RFID system. The market is filled with a wide variety of RFID systems. These are divided into groups based on the frequency ranges.

Low-frequency (30-500 kHz), mid-frequency (900 kHz-1500MHz), and high-frequency (2.4-2.5GHz) RFID kits are some of the models that are most frequently used. An electrical device that monitors and detects infrared radiation in its environment is called an infrared (IR) sensor. A GSM module is a specific kind of device that uses a SIM card and requires a mobile operator subscription to function, much like a cell phone or pager.

A GSM modem resembles a phone from the standpoint of a mobile operator. Tags and readers are the two halves of the wireless system known as Radio Frequency Identification (RFID). Tags can be passive or active, employing radio waves to transmit their identity as well as additional information to adjacent readers. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead.

The LPC2141/42/44/46/48 microcontrollers combine a microcontroller with embedded high speed flash memory with capacities ranging from 32 kB to 512 kB. They are based on a 16-bit/32-bit ARM7TDMI-S CPU with real-time emulation and embedded debug support. 32-bit code execution at the highest clock rate is made possible via a 128-bit wide memory interface and a special accelerator architecture. The alternative 16-bit Thumb mode cuts code by more than 30% with little performance hit for applications that require small code sizes.

The LPC2141/42/44/46/48 are perfect for applications like access control and point-of-sale where miniaturisation is essential due to their small size and low power consumption. These devices are well suited for communication gateways and protocol converters, soft modems, voice recognition, and low-end imaging because they have serial communications interfaces that range from a USB 2.0 Full-speed device to multiple UARTs, SPI, SSP, to I2C-bus and on-chip SRAM of 8 kB to 40 kB. They also have large buffer sizes and powerful processors. The aforementioned microcontrollers are suitable for industrial control and medical applications due to their various 32-bit timers, single or dual 10-bit ADC(s), 10-bit DAC, PWM channels, 45 fast GPIO lines, and up to nine edge or level sensitive external interrupt pins.

2. GSM AND RFID TECHNOLOGY

The GSM (Global System for Mobile Communications) technology, which is a cellular communication network standard, is frequently utilized by mobile phones and other handheld devices. The fundamental operations of GSM technology require the following actions:

Establishing a Connection: When a cell phone is powered on, it sends a signal to the nearby base station in order to establish a connection. The base station validates the request and subsequently sends the data back to the mobile phone to verify the connection.

Authentication: After establishing a connection, the mobile device asks the network for authentication. The network sends a challenge to the mobile device in order to encrypt a secret code stored on the SIM (Subscriber Identity Module) card.

The code is encrypted on the mobile device and sent back to the network for verification. If the code is accurate, the network verifies the mobile phone and assigns it a temporary identity number, or TMSI.

Call setup: The mobile phone can now make and receive calls using the assigned TMSI. Every time a call is made, the mobile phone sends a request to the network to connect to the recipient's phone number.

The calling process: The call is routed to the nearest base station by the network after finding the recipient's phone number. The base station sends a signal to the recipient's phone to establish a connection.

Termination of a call: When the call is over, the mobile device signals the network to cut off the connection.

GSM technology uses frequency division multiplexing (FDM) and time division multiplexing (TDM) to send and receive signals. TDM produces time slots from the available bandwidth and assigns a unique user to each one. When utilizing FDM to segment the available frequency spectrum into various channels, each channel is assigned to a different user. In the same frequency spectrum, many users can cohabit without interfering with one another because to this.

GSM technology also makes use of a number of security measures to protect network and mobile phone communication. These include encryption, authentication, and authorization methods to guarantee that only authorized users can access the network and communicate safely. Figure 1 illustrates the main components of the GSM Network.

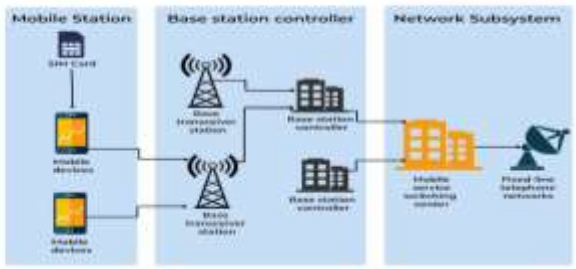

Fig -1: Working of a GSM Network

RFID: Radio waves are used in RFID (Radio Frequency Identification) technology, a sort of wireless communication technology, to identify and track persons or items.

The three steps that make up the basic operation of RFID technology are tag activation, data transmission, and data receiving.

Tag activation: When an RFID reader sends a radio signal to an RFID tag, the antenna on the tag activates. The tag's antenna then signals to the reader that it is prepared to communicate by sending a signal back.

Data transmission: When the tag becomes operational, it communicates information to the reader via radio waves. The tag has the capability to carry out data, including data pertaining to its specific ID, setting, and status.

Active, semi-active, and passive RFID tags are all accessible. Since passive RFID tags remain battery-less, they must rely on the scanner's power to transmit data. Active RFID tags have a unique power supply and can transmit data over farther distances. Semi-passive RFID tags have their own power supply for some activities but rely on the reader for communication.

Data reception: The data sent by the tag is ingested and analyzed by the RFID reader. The reader can then utilise this information for a variety of purposes, including managing assets, monitoring access control, and keeping track of inventory.

Asset tracking, supply chain management, access control, and inventory management are a few uses for RFID technology. Additionally, it can be combined with other technologies, including sensors and GPS, to provide real-time tracking and object or person observation.

Generally speaking, RFID technology provides a useful and efficient way to identify and follow people or things without direct physical touch or line of sight. Due to its ability to function in difficult circumstances and provide real-time data, it is a useful tool in many industries.

3. EXPERIMENTAL METHODOLOGY

The proposed Bank locker security system implementation starts from RFID authentication, continuing with the password matching and fingerprint authorization. Initially, the user is provided with an RFID Tag at the time of acquiring the bank locker. The Tag is a unique authorization key and thus cannot be replaced. Each Tag consists of a serial number that is pre-programmed.

Further, if the Tag matches the serial number in the program when scanned, the next process is executed. Otherwise, the owner of the locker is notified via the GSM module using SMS validation.

Once the RFID authentication is completed, the second step is the keypad password matching. The user enters the password that was initially set. The same password is also programmed and once it is verified the next process begins. Again, if this step fails then the user is notified with a message stating invalid authorization.

Finally, the last step involves fingerprint scanning. Once this biometric authentication is completed the DC motor is activated and thus the user can access the bank locker.

It is important to note that all the three processes needs to be successfully completed in order to access the secured locker.

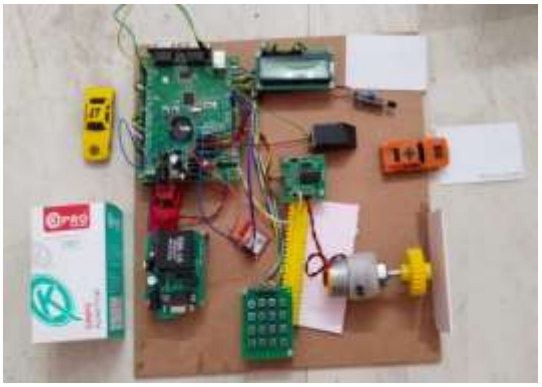

Fig -2: Experimental Setup

Even if a single authorization process does not take place, then the user or the owner is notified with the message invalid operation.

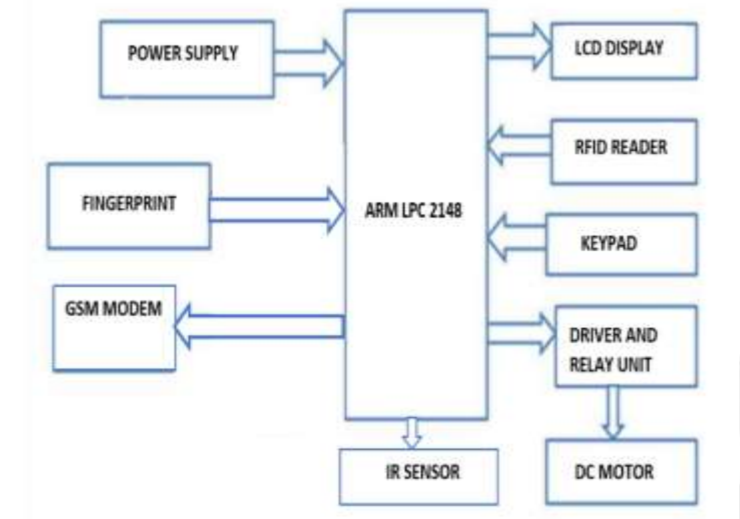

Fig -3: Block Diagram

All of the above-mentioned technologies provide highest level of security. Despite it being a lengthy process, the threat is minimized by a large factor.

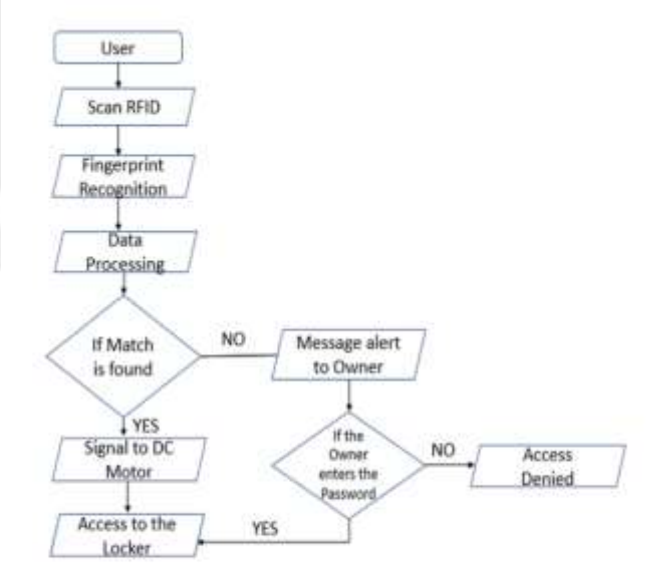

Fig -4: Flow chart

4. RESULTS AND DISCUSSION

The code written in keil software in C language is an integration of all the components, i.e., RFID, GSM, Fingerprint, keypad, and IR sensor. This integrated code is dumped into the ARM processor LPC 2148. Once this process is completed, we can observe the step-by-step output.
The RFID Tag is scanned against the sensor and if the users Tag serial number matches with the serial numbers available in the data base then it is known that the user is authorized.

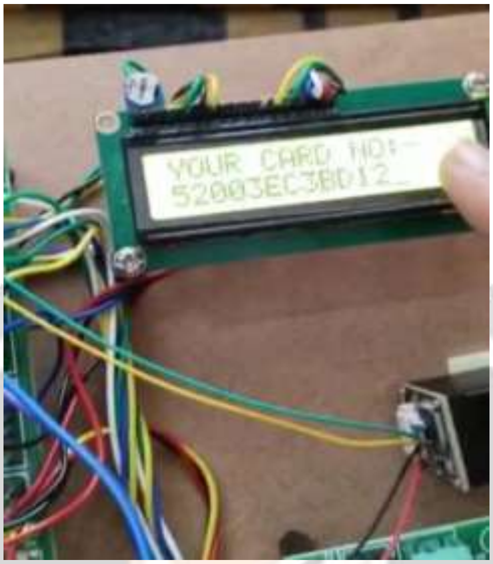

Fig -5: RFID Scanner Output

Password entering is the second step in the authentication process. After the RFID scanning is successfully completed the system asks the user to enter the password set in the beginning.

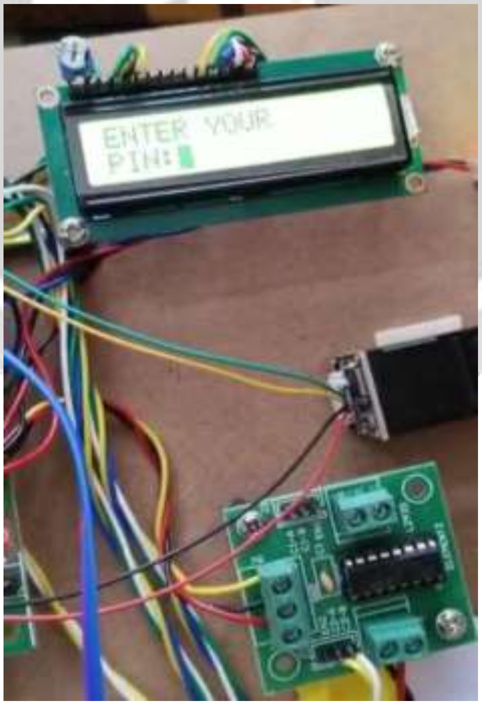

Fig -6: Password Entry

The third step in authentication is fingerprint scanning. After the password is successfully verified the system asks the user to place their registered fingerprint to the sensor.

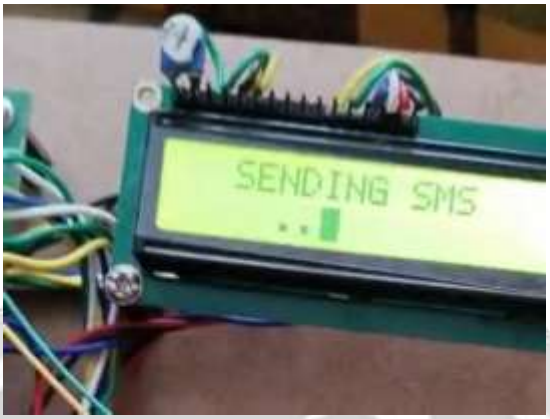

Fig -7: GSM Output

GSM Module is used to send a notification to the owner when the locker is being accessed in an unauthenticated manner. If any of the above steps fail then the notification is sent via the SMS to the user's registered phone number.

5. CONCLUSION

Thus, by implementing this Smart Bank locker security system project using RFID, Fingerprint, password and GSM technology safety of every important material stored at bank locker can be guaranteed. Using this smart technology only an authorized person can open the lock and collect his belongings. This is a real time application which tells that there is a need to bring in a revolution in the bank locker security system by making the procedure a little easy and more systematic for the bank officials.

This is a low-cost equipment, low in power consumption, compact in size, wide operating range, highly secured and reliable stand-alone unique system. The model proposed in this paper combines various sensors together that otherwise has not been implemented previously. It can be further enhanced by using an IoT based system and other biometric sensors.

In addition to this the future scope of this project is to develop smart bank Locker security system based on "Digital Signature", "IRIS and Retina" Scanning for visual identification of the person.

6. REFERENCES

[1] H. S. Detroja, P. J. Vasoya, D. D. Kotadiya and C. B. Bambhroliya, "GSM Based Bank Locker Security System using RFID, Password and Fingerprint Technology", International Journal for Innovative Research in Science and Technology, Vol. 2, Issue 11, (2016), pp. 110-115.

[2] S. Mohammed and A. H. Alkeelani, "Locker Security System Using Keypad and RFID", The 2nd international conference of Computer Science and Renewable Energies, (2019), doi: 10.1109/ICCSRE.2019.8807588.

[3] S. Sridharan, "Authenticated secure bio-metric based access to the bank safety lockers," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-7, doi: 10.1109/ICICES.2014.7034063.

[4] A. Faraz Hussain et al., "Zigbee and GSM Based Security System for Business Places," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2021, pp. 264-267, doi:10.1109/ICACITE51222.2021.9404577.

[5] A.Chikara, P.Choudekar, D.Asija, "Smart Bank Locker Using Fingerprint Scanning and Image Processing", 6th International Conference on Advanced Computing & Communication Systems (ICACCS), 2020, doi:10.1109/ICACCS48705.2020.9074482

[6] A.Kumar, P.Sood, U.Gupta, "Internet of Things (IoT) for Bank Locker Security System", 6th International Conference on Signal Processing and Communication (ICSC), 2020, doi:10.1109/ICSC48311.2020.9182713

[7] A.Islam, M.Hasan Mamun, F.Ahmed, T.Khatun, “Multi Level Bank Locker Security System with Digital Signature Authentication and Internet of Things”, Research Square, 2022, doi: 10.21203/rs.3.rs-2173423/v1.
[8] A. V. Mhaskar and P. Bhangale,“A Survey on IOT based Secure Bank Locker System.”,International Journal of Research Publication and Reviews, Vol 2, no 12, pp 1143-1146, December 2021.
[9] R. Ramani, S. Valarmathy, S. Selvaraju and P.Niranjan, “Bank Locker Security System based on RFID and GSM Technology”, International Journal of Computer Applications, Vol 57, no 18, November 2012.
[10] P. Sugapriya, K. Amsavalli, “Smart Banking Security System Using PatternAnalyzer”,International Journal of Innovative Research in Computer and Communication Engineering ,Vol.3, Special Issue 8, October 2015.
[11] M.Gayathri, P.Selvakumari, R.Brindha “Fingerprint and GSM based Security System” International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.
[12] M. Lourde, D. Khosla, “Fingerprint Identification in Biometric Security Systems” International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010