Biometric Locking with Security Alerting System Using GSM Module

Mohamed Elyash K
Department of Electrical and Electronics Engineering
Sri Eshwar College of Engineering
Coimbatore-641 202
mohamedelyask2002@gmail.com

Sethu M
Department of Electrical and Electronics Engineering
Sri Eshwar College of Engineering
Coimbatore-641 202
sethushetti23@gmail.com

Sakthivel S
Department of Electrical and Electronics Engineering
Sri Eshwar College 0f Engineering
Coimbatore-641 202
Sivasakthivel1707@gmail.com

Abstract - The biometric finger security locking system with message sending facility is a modern security system designed to protect personal belongings from unauthorized access. The system uses biometric fingerprint technology to grant access to only authorized individuals, ensuring maximum security.

The system is equipped with a messaging facility, allowing authorized users to send messages to designated recipients upon successful access. This feature enables users to send alerts to security personnel or designated contacts in case of emergency or suspicious activity. The system is easy to install and can be used in a variety of settings, including homes, offices, and other areas where security is a concern. The system provides an additional layer of security, ensuring that only authorized individuals are granted access, and messages can be sent in real-time to designated contacts. Overall, this system offers a secure and convenient solution for personal and professional security needs. A message alerting system is a software application that enables the automatic dissemination of alerts and notifications to users through various channels, such as email, SMS, voice calls, and mobile applications. This system plays a critical role in alerting individuals or groups about important events or emergency situations, such as natural disasters, security breaches, system failures, and other time-sensitive events. The message alerting system employs sophisticated algorithms and communication protocols to ensure that the alerts are delivered in a timely and reliable manner. With the increasing importance of real-time communication and the need for immediate responses, the message alerting system has become an indispensable tool for businesses, organizations, and government agencies alike.

I. INTRODUCTION

I.I. BIOMETRICS

Biometric systems are automated methods of identifying or verifying the identity of a person based on unique physical or behavioral characteristics. These systems use advanced technologies such as fingerprint scanners, facial recognition software, iris scanners, voice recognition, and DNA analysis to capture and analyze biometric data.

Biometric systems are becoming increasingly popular for a variety of applications such as access control, time and attendance tracking, law enforcement, and border control. These characteristics include fingerprints, face recognition, iris and retina scans, voice recognization. Biometric technology can quickly and efficiently identify.

Attendance tracking, law enforcement, and border control.
These systems offer several advantages over traditional methods of identification, such as passwords or ID cards, as biometric data cannot be lost or forgotten, and it is difficult to counterfeit or impersonate.
There are various types of biometric systems, including physiological biometrics, which analyze physical characteristics such as fingerprints, facial features, and iris patterns, and behavioral biometrics, which analyze patterns of behavior such as typing rhythm and voice pitch.
While biometric systems offer many benefits, there are also concerns about privacy, security, and accuracy. It is essential to ensure that biometric data is stored securely and used only for its intended purposes, and that the systems used to capture and analyze the data are accurate.

I.II. FINGURE PRINTS

Fingerprint locking is a security technology that uses biometric authentication to grant access to a device or system. It relies on unique patterns on an individual's fingers to verify their identity and allow them to unlock the device or gain access to the system. Fingerprint locking has become increasingly popular in recent years due to its convenience, speed, and high level of security. It is commonly used in smartphones, laptops, and other electronic devices as well as in physical access control systems for buildings and secure areas. The technology behind fingerprint locking involves capturing an image of the unique fingerprint pattern, converting it into a digital template, and comparing it with a stored template to verify identity. Fingerprint locking provides a more secure alternative to traditional password-based authentication methods, which can be easily compromised by hackers.
Locking modules are components used in many mechanical and electronic systems to control access to resources or physical spaces. They typically consist of a mechanism that can be locked or unlocked using a key, code, or other authentication method. Locking modules can take many forms, including padlocks, deadbolts, electronic door locks, and more. They may be used to secure doors, cabinets, safes, or other types of containers.
The main purpose of locking modules is to prevent unauthorized access to sensitive information or valuable assets. By controlling who has access to a particular resource or space, locking modules can help to ensure the safety and security of both people and property. Locking modules can be found in a wide range of settings, including homes, businesses, schools, hospitals, and government facilities. They may be used to secure everything from personal lockers to highly classified information.

I.III.GSM MODULE

The GSM (Global System for Mobile Communications) module is a type of device that enables communication between electronic devices over a cellular network. It is a type of wireless modem that allows devices to send and receive data, voice, and SMS messages over a mobile network.

GSM modules are used in a variety of applications, including vehicle tracking systems, remote monitoring and control, security systems, and industrial automation. They are often integrated into devices such as routers, alarms, and sensors to provide wireless communication capabilities.

GSM modules use a Subscriber Identity Module (SIM) card to authenticate and identify the device on the network. The module communicates with the network through a serial interface, and typically supports standard AT commands for sending and receiving data and messages.

GSM technology is widely used around the world, making the GSM module a versatile and reliable option for wireless communication in many different applications.

A message sending system is a technology that enables individuals or organizations to send and receive messages electronically. This can include email, text messaging, instant messaging, and other forms of digital communication.

In order to use a message sending system, users typically need access to an electronic device such as a computer, tablet, or smartphone, as well as an internet connection or cellular data plan.

There are many different types of message sending systems available, each with their own unique features and capabilities. Some systems are designed for personal use, while others are tailored for businesses or organizations. Additionally, some systems are more secure than others, with built-in encryption and other features designed to protect user privacy.
Overall, message sending systems have revolutionized the way people communicate and connect with one another, providing a fast, convenient, and efficient way to stay in touch regardless of geographic location or time zone.

II.I. NECESSITY OF LOCKINGS

Locks are necessary for several reasons. Here are a few reasons why:
1.Security: Locks provide security by preventing unauthorized access to homes, offices, vehicles, and other personal belongings. They act as a deterrent against burglars and other intruders, making it harder for them to gain access to your property.

2.Privacy: Locks also provide privacy by allowing you to control who has access to your personal space. For example, you may want to lock your bedroom door to prevent someone from entering without your permission.

3.Safety: Locks can also provide safety by preventing children or pets from accessing areas of your home that may be dangerous or off-limits. For example, you may want to lock the door to your swimming pool to prevent young children from entering unsupervised.

4.Compliance: In some industries and settings, locks are required to comply with regulations and laws. For example, healthcare facilities are required to keep certain medications and equipment locked up to prevent unauthorized access.

Overall, locks are a necessary component of security, privacy, safety, and compliance in various settings.

II.II. NECESSITY OF SECURITY LOCKINGS

Security locks are necessary to protect people and their belongings from theft, vandalism, and unauthorized access. They provide a barrier that prevents intruders from gaining access to property, homes, or businesses. Security locks come in many different forms, including door locks, padlocks, electronic locks, and combination locks.

Security locks are especially important in high crime areas or in situations where valuable assets are at risk. They are also essential in areas where privacy and confidentiality are important, such as in medical facilities, financial institutions, and government buildings.

Without security locks, individuals and businesses would be vulnerable to theft, property damage, and other forms of crime. The presence of security locks not only deters criminals but also provides peace of mind to individuals and businesses, knowing that their property and assets are protected.

Overall, security locks are a necessary part of our daily lives, and it is important to choose the appropriate type of locking system to meet the specific security needs of your home or business.

III. BLOCK DIAGRAM

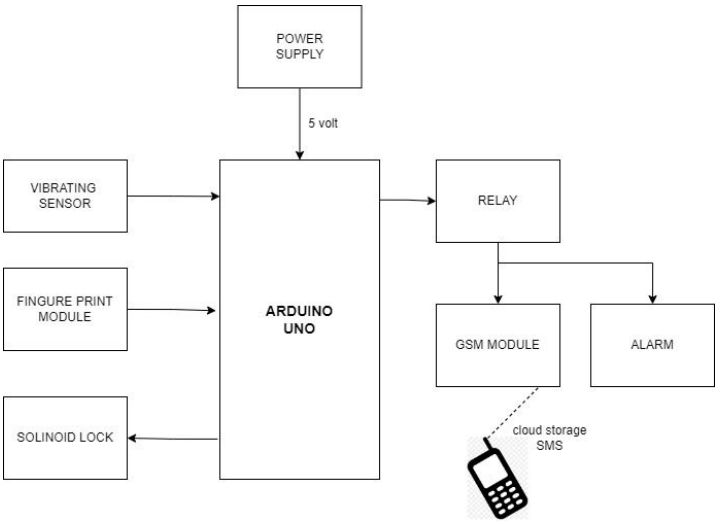


Fig.1.Block diagram for the biometric locking system

A. ARDUINO UNO

Arduino Uno can be programmed using the Arduino software, which is an open-source integrated development environment (IDE) based on the Processing programming language. The software includes a code editor, a compiler, and a bootloader that allows the board to be programmed over the USB connection.

The Arduino Uno is commonly used in a wide range of projects, such

as robotics, home automation, and Internet of Things (IoT) applications. Its ease of use, low cost, and flexibility make it a popular choice among hobbyists, students, and professionals alike.
Arduino UNO is a popular open-source microcontroller board based on the ATmega328P microcontroller. It is widely used in various applications, such as robotics, automation, IoT, and education. The board has a simple design, is easy to program, and can be interfaced with a wide range of sensors, actuators, and other electronic components.

The Arduino UNO board has 14 digital input/output pins, six analog input pins, a USB interface, a 16 MHz quartz crystal oscillator, a power jack, and a reset button. The digital pins can be used as either input or output pins, and can be controlled using the Arduino programming language. The analog pins can be used to read analog voltage values from sensors, such as temperature sensors, light sensors, and potentiometers.

To program the Arduino UNO board, you need to connect it to a computer using a USB cable and install the Arduino Integrated Development Environment (IDE) software. The IDE provides a user-friendly interface for writing, compiling, and uploading code to the board. The code is written in C/C++ programming language and can be easily modified and uploaded to the board using the IDE.

Once the code is uploaded, the Arduino UNO board can perform various tasks, such as controlling motors, turning on/off LEDs, reading sensor data, and communicating with other devices over serial communication. The board can be powered using a USB cable or an external power supply, depending on the application requirements.
Here, Arduino UNO is a versatile and easy-to-use microcontroller board that can be used in a wide range of applications. Its simple design, user-friendly IDE, and compatibility with various sensors and electronic components make it an ideal platform for prototyping and experimenting with electronics and programming.

B. POWER SUPPLY

A 5V power supply is a device that provides a constant 5-volt DC (direct current) output voltage to power electronic devices. It is commonly used to power small electronic devices such as microcontrollers, sensors, and other low-power devices.

There are different types of 5V power supplies, including AC-DC power supplies, DC-DC converters, and voltage regulators. AC-DC power supplies convert alternating current (AC) to direct current (DC), while DC-DC converters step down or step up the voltage level to produce the required output voltage. Voltage regulators, on the other hand, maintain a constant output voltage regardless of changes in input voltage or load.

A common example of a 5V power supply is the USB charger used to charge smartphones and other portable devices. USB chargers typically provide a 5V DC output voltage and can deliver up to 2.4A of current.

When selecting a 5V power supply, it is important to consider the required output current, the input voltage range, and the efficiency of the device. It is also important to ensure that the power supply is suitable for the intended application and meets relevant safety standards.

C. RELAY MODULE

An electrical gadget called a relay module is made to control high-voltage or high-current circuits with low-voltage signals. Typically, it comprises of one or more electromechanical relays, which are electrically signal-operated switches. For safety and noise reduction purposes, the relay module offers isolation between the control circuit and the circuit being controlled.

Relay modules are frequently employed in a wide range of applications, including automotive systems, industrial automation, and home automation. They are especially helpful when a low-voltage control signal is used to switch a high-voltage or high-current load, like turning on and off lights, motors, or heaters. Relay modules come in a variety of forms, including single-relay, multi-relay, and solid-state.
The main function of a relay module is to isolate the control circuit from the high voltage and high current circuit it is controlling, thereby preventing damage to the control circuit. This is achieved by using the small electrical signal from the control circuit to activate the relay, which then switches the high voltage and high current circuit on or off.

Relay modules can be used in a wide range of applications, including industrial control systems, home automation, and automotive systems. They are commonly used to control lights, motors, pumps, and other electrical devices.

To use a relay module, you need to connect the control circuit to the input terminals of the module and the high voltage and high current circuit to the output terminals of the module. When the control circuit sends a signal to the relay module, the relay switches on or off, depending on its configuration, allowing or preventing current flow to the high voltage and high current circuit.

In summary, a relay module is an important component in electronic circuits that allows low voltage control signals to switch high voltage and high current circuits on and off, while providing isolation between the two circuits to prevent damage to the control circuit.

D. GSM MODULE

A GSM (Global System for Mobile Communications) module is a piece of hardware that allows mobile devices to communicate with the cellular network using the GSM protocol. It typically includes a modem, a microcontroller, and other components required for cellular network connectivity.

GSM modules are widely utilized in wireless communication applications such as security systems, remote monitoring systems, and tracking devices. They can be controlled via AT instructions and interfaced with a microcontroller or a computer using various interfaces such as UART, SPI, or USB.

GSM modules come in a variety of sizes and configurations, ranging from simple surface-mount modules to bigger modules with capabilities like GPS and Bluetooth connectivity.

Message sending services are typically provided via GSM modules. Here are a few examples:

1.Sending Short Message Service (SMS): This is a basic function of GSM modules. You can use this feature to send brief text messages to other mobile devices. Messages are typically limited to 160 characters.

2.Multi-part SMS sending: If you need to send a longer message, you can split it into many parts and send them as individual SMS messages using this function. The receiving device will then put the pieces together to display the entire message.

3.Sending Unstructured Supplementary Service Data (USSD): Unstructured Supplementary Service Data (USSD) is a communication protocol used by GSM networks to convey messages between a mobile device and an application server. You can send and receive SMS messages using the USSD sending function.

E. VIBRATING SENSOR

Vibrating sensors are devices that detect and convert changes in vibration or mechanical oscillations in a system into electrical signals that can be read and analyzed. Vibrating sensors are defined as follows:

1.Accelerometer: A sensor in a system that measures acceleration, vibration, and shock. It turns movement into an electrical signal, which may then be analyzed to determine the amount and direction of the vibration.

2.A gyroscope is a sensor that detects a system's rate of rotation or angular velocity. It measures the angular displacement of an item using the mechanical gyroscopic action.

3.Strain gauge: A sensor that measures an object's deformation as a result of external forces such as stress or strain. It is often used to assess mechanical performance.

4. A Piezoelectric: A sensor that converts mechanical energy into electrical energy is known as a piezoelectric sensor. It makes use of the piezoelectric phenomenon, which happens when certain materials develop an electric charge as a result of mechanical stress.

5.Tilt Sensor: A sensor that monitors an object's tilt angle or inclination in relation to the gravitational field. It is extensively used in levelling, alignment, and orientation applications.

6.A proximity sensor detects the presence or absence of an object within a specified distance or proximity. It detects the object using numerous technologies such as capacitive, inductive, ultrasonic, or optical sensing.

Overall, vibrating sensors are widely utilized in a variety of industries, including automotive, aerospace, manufacturing, healthcare, and many others, to monitor and manage the performance of machines, structures, and other structures.

F. FINGURE PRINT MODULE

The fingerprint module is a piece of hardware that captures and processes a person's unique fingerprint. It is frequently used in biometric security systems to identify and verify an individual's identification. The module normally consists of a sensor that captures an image of the fingerprint, as well as software that analyses and compares the fingerprint's unique traits to those stored in a database. Fingerprint modules are commonly used for secure authentication in access control systems, time and attendance monitoring systems, and mobile device.

The fingerprint module is primarily used for biometric identification and authentication. It is a safe and dependable technique of validating a person's identity that is extensively used in a variety of applications such as mobile phones, laptop computers, and access control systems. The fingerprint module performs the following functions:

1.Authentication: The fingerprint module is used to validate an individual's identity by comparing their fingerprint to the stored template. It is a safe and dependable method of authenticating people and granting access to critical data and applications.

2.Identification: By matching an individual's fingerprint to a database of fingerprints, the fingerprint module can be used to identify them. This is useful in situations such as law enforcement and border control where identification is required.

Fingerprint sensors are often employed in biometric systems to authenticate an individual's identification. Biometric systems authenticate a person's identity by using distinctive physical or behavioural features, and fingerprints are one of the most often used biometric identifiers due to their uniqueness and durability.

A fingerprint sensor collects a person's fingerprint image and converts it to a digital format that can be analyzed and compared to a database of authorized fingerprints. To capture the fingerprint picture, the sensor employs several technologies such as optical, capacitive, or ultrasonic.

When a person places their finger on the sensor, the image of their fingerprint is captured and compared to a database of authorized fingerprints. The biometric system enables access if the fingerprints match.

G. SOLINOID LOCK

A solenoid lock is an electromagnetic locking system that creates a magnetic field by using an electric current, causing a metal armature or bolt to be drawn into a locked position. When electricity is applied to the solenoid, it becomes magnetized and attracts the armature or bolt, locking the door or gadget.

Security systems, access control systems, and vending machines all use solenoid locks. They can be controlled by a key, a keypad, a card reader, or other access control systems. Solenoid locks are commonly employed in circumstances requiring a high level of security, such as banks, jails, and other sensitive buildings. They are often thought to be more secure than traditional mechanical systems.

An electronic lock controlled by an electric current is known as a solenoid lock. When a current is applied to the lock, the electromagnetic force of the solenoid pulls the lock mechanism and unlocks the door. Here are some common applications for solenoid locks:

Solenoid locks are frequently used in access control systems, such as those used in hotels, workplaces, and residences. These locks are frequently combined with card readers or keypads, allowing authorized users access.

1.Security: Solenoid locks can be used to secure a variety of doors, including exterior, interior, and cabinet doors. They are highly secure and can only be unlocked with the relevant access code, card, or key.
2.Automatic Doors: Solenoid locks are also available.
Solenoid locks are also utilized in automatic doors like those found in supermarkets and hospitals. The lock keeps the door closed until an authorized individual arrives, at which point the solenoid unlocks it.
3.Safes and vaults: Solenoid locks are used to offer an extra degree of protection to safes and vaults. They are frequently used in conjunction with mechanical locks, ensuring that only authorized persons have access to the safe or vault's contents.
4.Lockers: Solenoids are often utilized in lockers found in schools, gyms, and businesses. They are a simple and secure solution to keep personal belongings, and they can only be accessed with the appropriate access code or key.

H. ALARM

A device that generates a loud sound or signal at a predetermined time or in reaction to a specific occurrence is known as an alarm. It is often used to warn people of a potentially dangerous situation or to remind them of an important assignment or appointment. Alarms can be located in a variety of locations, such as homes, companies, automobiles, and public places.

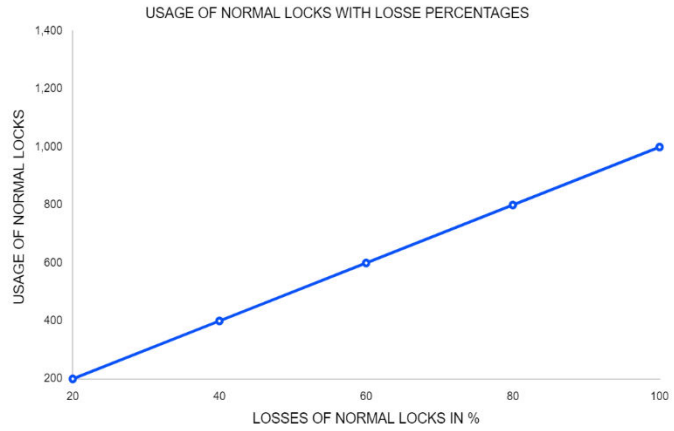
A buzzer is a sort of alarm that emits a loud, continuous buzzing sound. It is often used in industrial and commercial environments to signal an emergency or the conclusion of a task. Buzzer alarms are also used in home appliances such as ovens and washing machines to indicate when a cycle is complete.

An alarm is a signal or gadget that alerts people to a specific danger, hazard, or condition. It could be a loud noise, a flashing light, or a message indicating that immediate action is required. Alarms can be set off by a variety of circumstances, including fire, smoke, burglary, medical problems, and natural disasters. An alarm's objective is to swiftly and effectively alert individuals of an emergency so that they can take appropriate action to ensure their safety or lessen the effects of the incident.

An alarm's purpose is to warn or notify people of an imminent danger, emergency, or vital event. Alarms are used to deliver a warning signal to persons in the neighbourhood in a range of contexts such as homes, companies, and public locations. Alarms can be activated by a variety of events, such as smoke, fire, burglary, or medical issues, and they can be configured to emit a variety of sounds and signals to fit various scenarios.
Alarms can serve as a deterrent to would-be intruders or criminals by drawing attention to the site and increasing the chance of getting detected, in addition to alerting individuals to potential danger. Alarms can also give folks with peace of mind.

IV. MODEL GRAPH

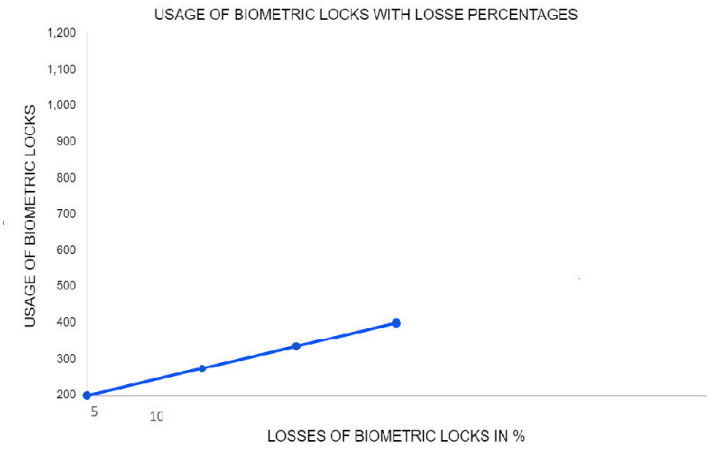
The Graphs are explain about the usage level of normal locks and the biometric locks with the losses percentage of the normal locks and the biometric locks. It clear about that we can get the clarification of how to select the locks of our lockers while seeing this graph. It shows the individual explanation about that the damages which occurs in the both normal and also the biometric locks. Normally we new about the biometric locks which safely protect our lockers against the strangers. So the losses takes place only in the normal locks, why because it has not any security systems against the thief. Essentially, the graph depicts the comparison of two or more axes. This allows us to quickly determine the explanation for the graph. As a result, choosing between standard and biometric locks is simple.



Example graph
Fig.2.Usage of normal locks with lose percentage

The first graph compares the use of standard locks and their losses in percentage terms. It claims that regular locks are used more frequently than biometric locks. Biometric locks must be protested in this case. However, no security mechanisms or innovative procedures were incorporated to these standard locks. As a result, the losses increased in tandem with the utilization levels.

As a result, the only choice is to adopt biometric locking systems. When compared to traditional locks, biometric locks have significantly lower losses.



Example graph
Fig.3.Usage or biometric locks with lose percentage

The second graph compares the use of biometric locks and the percentage losses they cause. It claims that biometric locks are used less frequently than standard locks. Biometric lock protests are also required here. It has high-security systems in place, as well as modern locking methods. As a result, the losses are far lower than with standard locks. However, no security mechanisms or innovative procedures have been applied to standard locks. As a result, the losses increased in tandem with the utilization levels.

We can employ biometric locking systems with advanced options to avoid locking losses and damages. The graph says that if we use the biometric locs with the advanced implementation we can able to reduce the damages of our lockers.

V. MATERIALS USED

A. TABLE FOR CONTROLLING DEVICES

CONTROLLING DEVICES	
S.no	**Name of the materials**
1	Arduino nano
2	LM2596
3	Magnetic door sensor
4	Relay module
5	Vibrating sensor
6	Finger print module
7	DF player

B. TABLE FOR TRANSMITING AND RECEIVING DEVICES

TRANSMITING & RECEIVING DEVICES	
S.no	**Materials Used**
1	GSM Module
2	Solinoid lock
3	Mobile phone

VI. CIRCUIT DIAGRAM

1.ABOUT FINGER PRINT MODULE

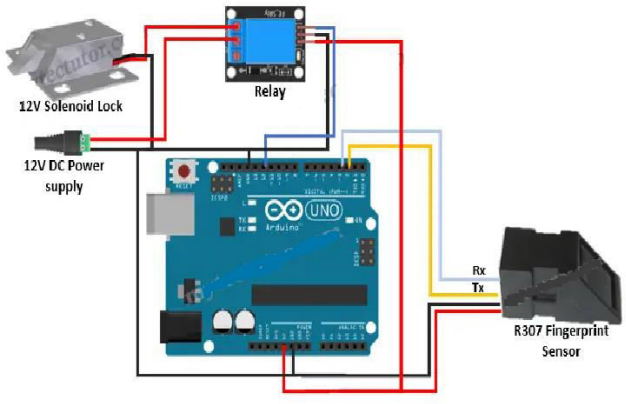


Fig.4.Shows the finger print module with solenoid lock

There are finger print sensor, relay module, power supply, solinoid lock, and other components in this Arduino uno, finger print module. The task at hand is to control the sensors' inputs. First, electricity is supplied to this module, and the entire system is activated. When we want to unlock our locker, we produce a finger print on an already existing sensor, and the sensor accepts our biometric prints and sends the input to the Arduino uno. It validates the input from the fingerprint module, and if it is correct, the value is sent to the solinoid locking system, allowing it to open. And the entered fingerprint is incorrect. It is incorrect for the finger print module to deliver the message (information) to the Arduino module. The Arduino module can validate and transmit the same message to the relay module, which will activate the alarm and send the message to the phone via the GSM module. The relay can then feed power to the alarm, which will begin alarming until it is turned off. In addition, the relay is linked to the GSM module, allowing it to be activated and deliver the message to the associated mobile phone. Not only is the input accepted by the finger print module, but most of the time the criminal will reach our locker, so he will not offer his finger print; instead, he will try to break the locker, steal our property, and flee. In this case, the vibrating sensor will provide data to the Arduino. When the robber breaks our locker, the sensor vibrates and becomes active. The message is then sent to the relay by the Arduino. The relay can then activate and send data to the alarm as well as the GSM module. The same thing will happen after that. This is how the entire module can function.

2.ABOUT GSM MODULE

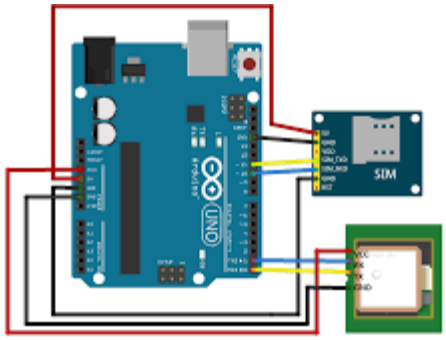


Fig.5.Shows the SGM module with Arduino

The GSM module is then linked to the Arduino uno in the second circuit diagram. If the entered fingerprint is incorrect, the relay module can warn the GSM module, and after the input from the relay module is received, the GSM can deliver the message to the linked mobile phone. The message is already saved in the module, and if information is received from the relay, the saved message is sent to the mobile phone. The finger print module and vibrating sensors can provide information to the relay. In the majority of cases, the robber will break our locker and take all of our possessions. If the locker is broken, the vibrating sensors activate and give the information to the relay, which can then send the message to the alarm and the GSM module. The process is then repeated. This is how the second circuit could function.

VII. USER AUTHENTICATION

A. ENDORESEMENT TO FINGERPRINT MODULE

Fingerprint modules are biometric devices that authenticate users by

using their fingerprints. They are made up of a sensor that captures an image of a person's fingerprint and software that analyses and compares the fingerprint to a database of authorized users. Fingerprint modules provide various advantages over other biometric systems, including the following:

1. High accuracy: When compared to other biometric technologies, fingerprint modules have a high accuracy rate. This is due to the fact that each person's fingerprint is unique and cannot be simply copied.

2. Quick and simple: Fingerprint modules are quick and simple to use, with authentication taking only a few seconds. Users are not required to memorise passwords or carry access cards.

3. Scalability: Fingerprint modules may be simply incorporated into current security systems and scaled to handle huge numbers of people in use.

4. Low cost: Compared to other biometric technologies, fingerprint modules are relatively inexpensive, making them a popular choice for a wide range of applications.

5. Dependable: Fingerprint modules are extremely dependable and require little maintenance.
Overall, fingerprint modules are a popular and dependable biometric identification and access control solution.

B. ENDOREMENT TO VIBRATING SENSOR

Electronic devices that detect and measure vibrations or movements are known as vibrating sensors. They are widely employed in a variety of applications, such as industrial machinery, vehicle safety systems, and wearable technologies.

Vibrating sensors provide various advantages over other types of sensors, including the following:
1. Sensitivity: Vibrating sensors are extremely sensitive, detecting even minor vibrations or movements.
2. Durability: Vibrating sensors are resistant to severe conditions and extreme temperatures.
3. Low power consumption: Because vibrating sensors consume little power, they are perfect for use in battery-powered devices.
4. Simple to install and use: Vibrating sensors have simple interfaces that make them accessible to a wide range of users.
5. Low cost: Vibrating sensors are less expensive than other types of sensors, making them a popular choice for many applications.
Overall, vibrating sensors are a dependable and adaptable technology with a wide range of applications. They have great sensitivity, endurance, low power usage, simplicity of use, and low cost.

C.ENDORSEMENT TO GSM MODULE

GSM modules are technological devices that enable cellular network connectivity. They are widely utilized in a variety of applications, such as remote monitoring and control systems, wireless data transfer, and mobile apps.

GSM modules provide various advantages over other communication methods, including the following:

1. Global coverage: GSM modules offer global coverage and can work in most countries, making them excellent for global applications.

2. High data transfer rates: GSM modules provide high data transfer rates, allowing for real-time monitoring and control the needs.

3. Ease of use: GSM modules are simple to use and integrate with other systems, having simple interfaces that allow them to be accessible to a wide range of users.

4. Low cost: When compared to other communication technologies, GSM modules are comparatively inexpensive.

5. Reliability: GSM modules are extremely dependable, providing a consistent connection with minimum latency.
GSM modules are a dependable and adaptable technology that may be employed in a variety of applications. They provide extensive coverage, fast data transfer, convenience of use, cost-effectiveness, and dependability.

VIII. SOURCES AND AREAS

1.Banking and Financial Services: Fingerprint biometric locking is used to safeguard banking and financial services such as ATMs and online banking. Customers can validate their identities using their fingerprints, making it more difficult for fraudsters to access their accounts.
2.House Locking: Once the user's biometric data has been registered, the biometric lock can be set to give only authorized users access. When attempting to utilize the home appliance, the user must provide their biometric data to the lock's scanner. The system will then compare the given biometric data to the data stored in its database to decide whether or not the user is authorized to access the appliance.

3.Mobile devices: Many mobile devices now include fingerprint scanners, allowing users to access their devices and make payments with a simple scan of their finger.

4.Law Enforcement: Law enforcement agencies employ biometric locking with fingerprints to identify suspects and solve crimes. To identify prospective suspects, fingerprints recovered at crime scenes can be compared to fingerprints in a database.
5.Access Control: Biometric locking based on fingerprints is often used to manage access to restricted locations such as protected buildings or computer systems. Only those with authorized fingerprints will be able to obtain access to the restricted area. Employees or authorized individuals can be registered in the system.

IX. DISCUSION

Biometric locking with a security alerting system utilizing a GSM module is a technology that combines biometric authentication with a security alerting system to improve home or other private space security. By leveraging biometric data to verify authorized users and alerting homeowners or authorized personnel when an unauthorized person attempts to use the home appliance, this technology delivers a high level of protection.

The biometric locking system authenticates and grants access based on a person's unique physiological traits, such as fingerprints, facial recognition, or iris scans. After registering the user's biometric data, the system compares it to the data supplied by the user throughout

the authentication procedure. If the system recognizes the user's biometric data, it gives access; otherwise, it denies access.When an unauthorized person attempts to access the home appliance, the security alerting system uses a GSM module to send text messages or phone calls to the homeowner or authorized personal. This technology sends real-time alerts to the homeowner or authorized individuals, allowing them to take fast action to prevent unauthorized entry.

This technique has the advantage of providing a high level of protection while eliminating the need for keys or passwords, which can be easily lost, forgotten, or stolen. Another benefit is that the security alerting system does not require a local internet connection, making it more reliable than other security systems.

However, there are several potential drawbacks to employing this technique. For example, the biometric locking system can be costly, and its usefulness may be limited depending on the quality of the biometric data collected. Furthermore, the GSM module may necessitate a membership or additional fees for data usage.

Finally, biometric locking combined with a security warning system based on a GSM module is a promising technology that provides increased protection for houses or other private places. While there are certain limitations to this technology, it provides a high level of security and real-time notifications, making it an appealing alternative for those wishing to improve their home security.

X. REFERANCE

[1] N. N. Nagamma, M. V. Lakshmaiah and T. Narmada, "Raspberry Pi based biometric authentication vehicle door locking system," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI),Chennai,India,2017,pp.2348-2351,doi: 10.1109/ICPCSI.2017.8392138.

[2] W. Ping, W. Guichu, X. Wenbin, L. Jianguo and L. Peng, "Remote Monitoring Intelligent System Based on Fingerprint Door Lock," 2010 International Conference on Intelligent Computation Technology and Automation, Changsha,China,2010,pp.1012-1014,doi: 10.1109/ICICTA.2010.436.

[3] N. Meenakshi, M. Monish, K. J. Dikshit and S. Bharath, "Arduino Based Smart Fingerprint Authentication System," 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai,India,2019,pp.1-7,doi: 10.1109/ICIICT1.2019.8741459.

[4] D. Addy and P. Bala, "Physical access control based on biometrics and GSM," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 2016, pp. 1995-2001, doi: 10.1109/ICACCI.2016.7732344.

[5] Chikara, P. Choudekar, Ruchira and D. Asija, "Smart Bank Locker Using Fingerprint Scanning and Image Processing," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020,pp.725-728,doi: 10.1109/ICACCS48705.2020.9074482.

[6] J. Soares and A. N. Gaikwad, "A self banking biometric machine with fake detection applied to fingerprint and iris along with GSM technology for OTP," 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2016, pp. 0508-0512, doi: 10.1109/ICCSP.2016.7754189.

[7] Z. M. Tahmidul Kabir, N. Deb Nath, U. R. Akther, F. Hasan and T. I. Alam, "Six Tier Multipurpose Security Locker System Based on Arduino," 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka,Bangladesh,2019,pp.1-5,doi: 10.1109/ICASERT.2019.8934615.

[8] J. Baidya, T. Saha, R. Moyashir and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017, pp. 1-6, doi: 10.1109/CCWC.2017.7868448.

[9] K. Tshomo, K. Tshering, D. Gyeltshen, J. Yeshi and K. Muramatsu, "Dual Door Lock System Using Radio-Frequency Identification and Fingerprint Recognition," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay,India,2019,pp.1-5,doi: 10.1109/I2CT45611.2019.9033636.

[10] M. N. Hossain, A. U. Khan Supto, M. M. Faruk and S. K. Biswas, "Design & Development of Fingerprint Based Electro-Magnetic Door Lock System," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT),Kharagpur,India,2021,pp.1-5,doi: 10.1109/ICCCNT51525.2021.9580064.

[11] Yang, H. Xia and W. Du, "Intelligent fingerprint lock based on STM32," 2020 Chinese Automation Congress (CAC), Shanghai, China,2020,pp.4048-4088,doi: 10.1109/CAC51589.2020.9327366.

[12] Ibrahim, A. Paravath, P. K. Aswin, S. M. Iqbal and S. U. Abdulla, "GSM based digital door lock security system," 2015 International Conference on Power, Instrumentation, Control and Computing (PICC),Thrissur,India,2015,pp.1-6,doi: 10.1109/PICC.2015.7455796.

[13] W. Ahmad, N. Jan, S. Iqbal and C. Lee, "Implementation of ZigBee-GSM based home security monitoring and remote control system," 2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), Seoul, Korea (South), 2011, pp. 1-4, doi: 10.1109/MWSCAS.2011.6026611.

[14] M. A. Kader, M. Y. Haider, M. R. Karim, M. S. Islam and M. M. Uddin, "Design and implementation of a digital calling bell with door lock security system using fingerprint," 2016 International Conference on Innovations in Science, Engineering and Technology (ICISET), Dhaka, Bangladesh,2016,pp.1-5,doi: 10.1109/ICISET.2016.7856484.

[15] V. J. Govindraj, P. V. Yashwanth, S. V. Bhat and T. K. Ramesh, "Smart Door Using Biometric NFC Band and OTP Based Methods," 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-4, doi: 10.1109/INCET49848.2020.9153970.

[16] A. T. Noman, S. Hossain, S. Islam, M. E. Islam, N. Ahmed and M. A. M. Chowdhury, "Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System using GPS, GSM and RFID," 2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT), Dhaka, Bangladesh,2018,pp.97-101,doi: 10.1109/CEEICT.2018.8628051.

[17] W. -S. Yoo and S. A. Shaik, "Development of Home Management System Using Arduino and AppInventor," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 2016, pp. 379-380, doi: 10.1109/COMPSAC.2016.96.

[18] A. Saroha, A. Gupta, A. Bhargava, A. K. Mandpura and H. Singh, "Biometric Authentication Based Automated, Secure, and Smart IOT Door Lock System," 2022 IEEE India Council International Subsections Conference (INDISCON), Bhubaneswar, India,2022,pp.1-5,doi: 10.1109/INDISCON54605.2022.9862840.

[19] H. F. Alqahtani et al., "Automated Smart Locker for College," 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCAIS48893.2020.9096868.

[20] T. J. Salai Thillai, T. Sarath Babu and B. S. Reddy, "Arduino based safeguarding system by using sound," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India,2019,pp.765-769,doi: 10.1109/ICCMC.2019.8819674.