IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART BANK SECURITY SYSTEM USING EMBEDDED SYSTEM AND IOT

Mr.M.Vasudevan[1] , K.T.Vishnu Suriyan[2] , S.Tharun Prasanth[3] and K.Vignesh[4]

[1]Asst.Head of The Department, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu, India

[2] Student, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu ,India

[3] Student, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu ,India

[4] Student, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu, India

ABSTRACT:

The conventional bank security system is not effective and theft of cash, jewels etc. happen easily. This paper proposes a bank security system that utilizes various IoT technologies such as fingerprint recognition, IR sensors, ultrasonic sensors, a keypad, and an ESP32 camera module to enhance the security of a bank. The system uses the fingerprint recognition system to verify the identity of the users, and the IR sensor and ultrasonic sensor to detect any unauthorized access to the restricted areas. The system also employs a keypad for manual access control. The ESP32 camera module is utilized for real-time monitoring of the bank premises and is equipped with motion detection features that trigger an alert in case of any unusual activity. The proposed system offers a multi-layered security approach that ensures the safety of the bank premises and its customers. The system is reliable, cost-effective, and easy to install, making it an ideal solution for small and medium-sized banks.

Keyword : Arduino Uno, NodeMCU, ESP32, Finger print sensor

INTRODUCTION:

Bank security is a crucial aspect of the banking industry, and with the increasing risk of security breaches and theft, banks need to ensure that their premises and customers are safe and secure. IoT technology and embedded systems provide real-time monitoring of the bank premises and can alert security personnel in case of any security breach. This paper proposes a bank security system that utilizes IoT technology and embedded systems to enhance the security of a bank. The proposed system utilizes various sensors and devices, such as motion sensors, door sensors, and cameras, to detect any unusual activity or unauthorized access to restricted areas. The system is designed to alert the security personnel in case of any security breach, allowing for quick response and resolution.The system is also equipped with embedded systems, such as microcontrollers, which can perform complex tasks and communicate with the various sensors and devices. The embedded systems make the system more efficient and reliable and allow for remote monitoring and control of the security system. This paper will discuss the benefits of using IoT technology and embedded systems in bank security systems, including improved efficiency, reliability, and cost-effectiveness.The results of the performance evaluation will be presented to demonstrate the effectiveness of the proposed system in enhancing the security

of the bank premises. Overall, the proposed bank security system that utilizes IoT technology and embedded systems provides a comprehensive approach to bank security that ensures the safety of the bank premises and its customers. The system's reliability, cost-effectiveness, and ease of installation make it an ideal solution for banks of various sizes.

LITERATURE SURVEY

[1] A bank security system using Arduino Uno and Keypad can be implemented by using various technical details. The Arduino Uno can be used to control the system's sensors, alarms, and other devices. A keypad can be used to allow authorized access to the bank's premises. Additionally, RFID technology can be integrated into the system to provide secure identification for bank employees. The system can be further strengthened by incorporating encryption and secure communication protocols to ensure that sensitive information is protected.

[2] A bank security system using Arduino Uno and a keypad servo typically involves the use of a password-protected access control system to regulate entry into the bank's secure areas. The system may also include an alarm system to detect unauthorized entry and alert security personnel. Technical details may include programming the Arduino Uno board to interact with the keypad and servo, configuring the alarm system to trigger at the appropriate threshold, and setting up the necessary hardware components for the system to function effectively. Other considerations may include ensuring the system is resistant to tampering and incorporating fail-safe mechanisms in case of technical failures.

[3] Fingerprint-based bank security systems using Arduino Uno and a fingerprint sensor have become increasingly popular due to their high level of security. The system consists of an Arduino Uno board, a fingerprint sensor, and a GSM module for sending alert messages to the bank's security team. The fingerprint sensor scans the user's fingerprint and verifies it with a database of authorized fingerprints.The system is highly reliable and can provide an additional layer of security to protect sensitive banking information.

[4] IoT-based bank automation systems using Raspberry Pi have been gaining attention for their versatility and cost-effectiveness. The system uses Raspberry Pi, a credit card-sized computer, to run various IoT devices, such as sensors, cameras, and smart ATMs, to automate bank operations. These devices are connected to a central network and can provide real-time data analysis to help banks make informed decisions. The system also enables customers to access banking services remotely through their mobile devices.

[5] IoT-based centralized bank security systems using NodeMCU, IR sensors, and ultrasonic sensors have been gaining popularity for their ability to improve bank security. The system uses NodeMCU, an open-source firmware and development board, to connect various IoT devices, such as IR and ultrasonic sensors, to a central network. These sensors detect intruders and trigger alarms, which are then sent to the bank's security team. The system also enables remote monitoring of the bank's premises using cameras connected to NodeMCU. Overall, IoT-based centralized bank security systems can help banks enhance their security, reduce costs, and provide a safe banking environment to customers.

[6] The Advanced Bank Security System using Raspberry Pi, Camera module, Image processing, and IoT platform involves the use of a Raspberry Pi board, a camera module, and image processing techniques to capture images and detect potential security threats. The system can be connected to an IoT platform for real-time monitoring and alerts. The system uses OpenCV library for image processing and can detect suspicious activities like unauthorized access, theft, or unusual behavior in the bank. The system also includes features like face recognition and license plate detection.

[7] A Bank Security System using a Web camera with Machine learning and Face detection involves the use of a web camera to capture live video streams and detect potential security threats. The system uses machine learning algorithms and face detection techniques to identify individuals and flag suspicious activities like unauthorized access, theft, or unusual behavior in the bank. The system can send live video streams to a central monitoring station for real-time monitoring and alerts. The system uses OpenCV and TensorFlow libraries for machine learning and can integrate with other security systems like alarms and access control systems.

[8] The IoT-Based Centralized Bank Security System with Live Video Transmission uses Raspberry Pi, KEYPAD, RFID, and IR sensors to detect potential security threats and transmit live video streams to a central monitoring station. The system uses IoT technology to integrate different security components and provide real-time monitoring and alerts. The system can authenticate access using RFID and KEYPAD and detect intrusions using IR sensors. The system uses OpenCV library for image processing and can detect suspicious activities like unauthorized access, theft, or unusual behavior in the bank.

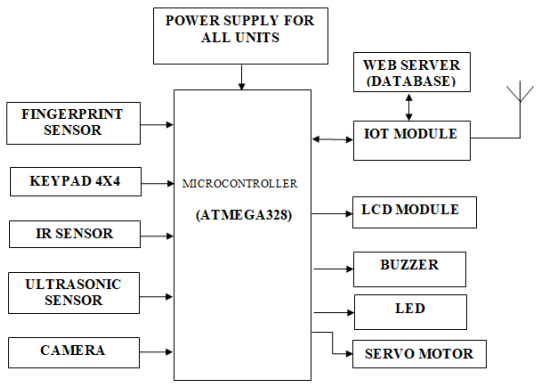
[9] An IoT-based bank security system with PIR sensor, temperature sensor, buzzer, and keypad involves the integration of various hardware components and software systems. The PIR sensor detects motion, while the temperature sensor monitors the ambient temperature. The buzzer is activated when unauthorized access is detected. A keypad is used for user authentication. Raspberry Pi serves as the central processing unit, and the system communicates via MQTT protocol. The collected data is stored in a database for further analysis and monitoring.

[10] A bank security system using IoT technology with Arduino Uno, keypad, NodeMCU, and Cayenne IoT platform API involves the integration of various hardware and software components. The system employs a keypad for user authentication and NodeMCU for wireless communication. The Arduino Uno serves as the central processing unit, while Cayenne IoT platform API facilitates data visualization and analysis. The system can detect unauthorized access and notify security personnel via email or SMS. The collected data is stored in the cloud for further analysis and monitoring.

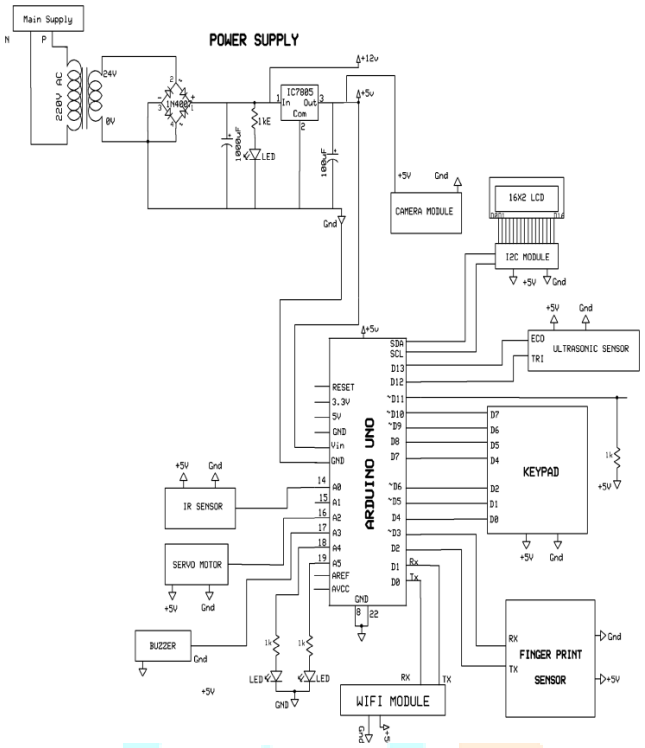
EXISTING SYSTEM:

They are using Microcontrollers with different sensors (PIR, Smoke or Fire) as observatory to recognize or perceive intruder or unpredictable activities inside the bank. The Existing security system will save the pictures at whatever point the development will be recognized that can be used in future for examination. These are all very low level Security system.

BLOCK DIAGRAM



CIRCUIT DIAGRAM



PROPOSED SYSTEM:

The proposed system for bank security utilizes a combination of IoT technology and a range of devices, including Nodemcu, biometric authentication systems, IR and ultrasonic sensors, keypad systems, ESP32 camera modules, LCD, Buzzer, and webserver. The system provides a multi-layered approach to bank security, ensuring the safety of the bank's premises, assets, and customers. The system utilizes Arduino UNO and Nodemcu, a microcontroller board that is equipped with Wi-Fi capabilities, to enable remote monitoring and control of the security system. The Nodemcu is connected to the bank's network, allowing for real-time data transmission and analysis.

The system also incorporates biometric authentication systems, such as fingerprint and facial recognition systems, to control access to restricted areas. The biometric authentication systems ensure that only authorized personnel can access the restricted areas, minimizing the risk of security breaches.

In addition to biometric authentication systems, the proposed system also utilizes IR and ultrasonic sensors to detect any unusual activity or unauthorized access to restricted areas. The sensors can detect environmental changes, such as changes in temperature or humidity, which can indicate a security breach. Keypad systems are also integrated into the proposed system to provide an additional layer of security. These systems require the input of a unique code or password to gain access to restricted areas. The use of keypad systems ensures that only authorized personnel can access the restricted areas, further minimizing the risk of security breaches.

Furthermore, the system incorporates ESP32 camera modules to provide real-time video feeds of the bank's premises. The cameras are equipped with high-resolution lenses and night vision capabilities, making them ideal for use in low-light conditions. The ESP32 camera modules are connected to the bank's network, allowing for remote monitoring and control of the security system. The system also incorporates LCD and Buzzer systems to provide real-time feedback and alerts. The LCD displays information related to the security system, while the buzzer generates an alarm in case of any security breach. Finally, the system utilizes a web server to provide a user-friendly interface for remote monitoring and control of the security

system. The web server allows authorized personnel to monitor the security system, receive alerts, and take appropriate action in case of any security breach.

METHODOLOGY:

The methodology for a Bank Security System involves both hardware and software components.

HARDWARE EXPLANATION:

The system provides a multi-layered approach to bank security, ensuring the safety of the bank's premises, assets. The proposed system for bank security utilizes a combination of IoT technology and a range of devices, including Nodemcu, biometric authentication systems, IR and ultrasonic sensors, keypad systems, ESP32 camera modules, LCD, Buzzer, and webserver.

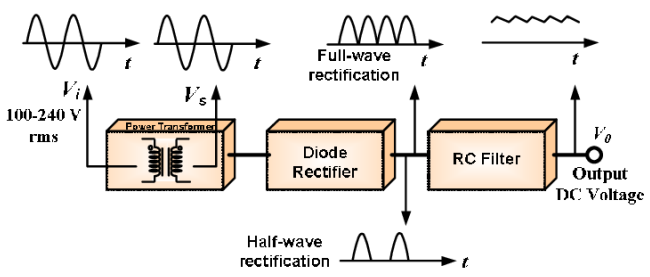
COMPONENTS LIST:

- Power supply system
- Arduino Uno
- Nodemcu
- Finger Print sensor
- RFID Reader and Tag
- LCD Module
- I2C Module
- Keypad
- IR sensor
- Ultrasonic Sensor
- Camera Module
- Servomotor
- Buzzer
- LED

HARDWARE COMPONENTS DESCRIPTION:

POWER SUPPLY SYSTEM:

A power supply system is an electrical system that converts one form of electrical energy to another form that is suitable for powering electronic devices. In particular, a 230V to 5V power supply system is an AC to DC converter that takes high voltage AC input from a mains power source and converts it into low voltage DC output suitable for powering electronic devices that require 5V DC voltage. The 230V to 5V power supply system typically consists of four major components, namely the transformer, rectifier, capacitor, and voltage regulator.

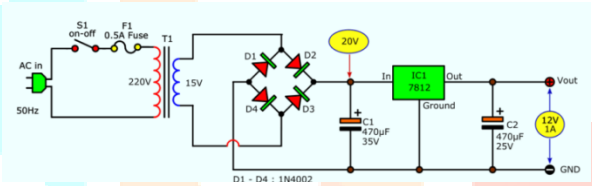


Transformer: The transformer is the first component in the power supply system. It takes in the 230V AC voltage input from the mains power source and steps it down to a lower AC voltage suitable for rectification. The transformer consists of two coils of wire wrapped around an iron core.

Rectifier: The rectifier is the second component in the power supply system. Its function is to convert the AC voltage from the transformer to DC voltage. The rectifier is made up of diodes arranged in a bridge configuration. It allows the current to flow in only one direction, resulting in a pulsating DC voltage output.

Capacitor: The capacitor is the third component in the power supply system. Its function is to filter the pulsating DC voltage from the rectifier and convert it into a smooth, stable DC voltage. The capacitor charges up during the positive half-cycle of the pulsating DC voltage and discharges during the negative half-cycle, resulting in a constant DC voltage output.

Voltage Regulator: The voltage regulator is the fourth and final component in the power supply system. Its function is to regulate the output voltage to a constant 5V DC voltage. The voltage regulator uses a feedback mechanism to adjust the output voltage to a constant value, even if the input voltage or load current changes.



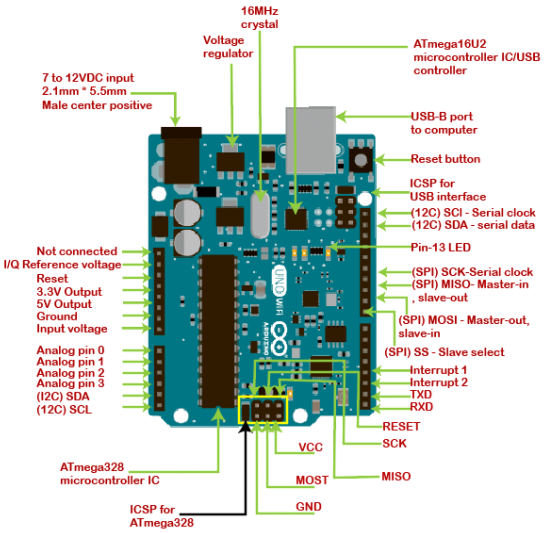
The working of the 230V to 5V power supply system involves the following steps:

- The AC voltage is stepped down by the transformer to a lower voltage level.
- The rectifier converts the AC voltage to a pulsating DC voltage.
- The capacitor filters and smooth's the pulsating DC voltage into a stable DC voltage.
- The voltage regulator regulates the output voltage to a constant 5V DC voltage.
- The output voltage is then used to power electronic devices that require a 5V DC voltage.

In summary, the 230V to 5V power supply system is an essential component in the design and development of electronic devices. The transformer, rectifier, capacitor, and voltage regulator are the key components that enable the conversion of high voltage AC input to low voltage DC output, suitable for powering electronic devices that require a 5V DC voltage.

ARDUINO UNO:

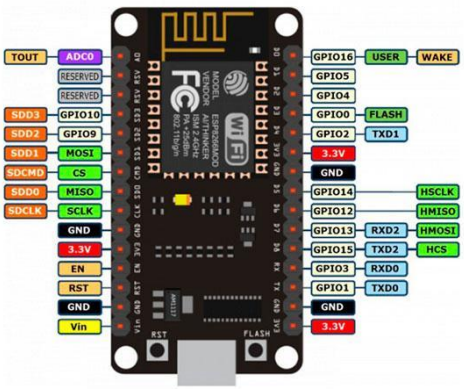
Arduino Uno is a main Brain of the Project. It has 14 digital input/output pins, 6 analog inputs, a 16 MHz quartz crystal oscillator, and a USB connection. The ATmega328P microcontroller has 32 KB of flash memory, 2 KB of SRAM, and 1 KB of EEPROM. The digital input/output pins are grouped into two sets of 8 pins each, with each set capable of being configured as either input or output. The analog inputs can read signals in the range of 0 to 5 volts, and are converted to a 10-bit digital value by the on-board analog-to-digital converter. The board can be powered either by connecting it to a computer via the USB cable, or by connecting it to a 9-volt battery or an external power supply.



The board also has a power jack and an ICSP header for programming the microcontroller using an external programmer. The board is programmed using the Arduino Integrated Development Environment (IDE), which is a free software tool that provides a user-friendly interface for writing, compiling, and uploading code to the board. The IDE supports the C++ programming language and provides a large library of pre-written code, making it easy for beginners to get started with programming the board.

NodeMCU:

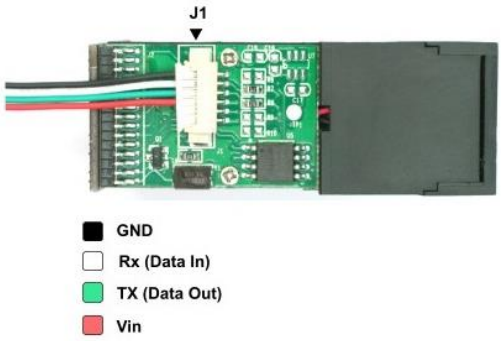
NodeMCU is a low-cost open-source firmware and development board based on the ESP8266 Wi-Fi module. The board has an 80 MHz 32-bit Tensilica CPU, 4 MB flash memory, and integrated Wi-Fi connectivity, which allows it to connect to the internet and exchange data with other devices. The board also features 11 digital input/output pins and one analog input pin, which can be used to interface with a variety of sensors and actuators. The NodeMCU firmware is based on the Lua scripting language and can be programmed using the NodeMCU Lua API. It also has support for the Arduino IDE, allowing it to be programmed using the familiar C++ programme ng language. Additionally, the NodeMCU supports the MicroPython programming language, which is a popular choice for IoT projects.



The board can be powered using a micro-USB cable or an external power supply, and can be programmed and debugged using a USB-to-serial converter. The NodeMCU firmware provides a range of networking protocols, including HTTP, HTTPS, MQTT, and Web Socket, which makes it an ideal choice for IoT applications that require cloud connectivity. NodeMCU is widely used for a range of IoT applications, such as home automation, weather stations, robotics, and wireless sensor networks. The open-source nature of NodeMCU means that it has a large community of developers who have created libraries, tools, and resources to help users get started with their projects. Overall, NodeMCU is a versatile and powerful development board that offers an affordable solution for IoT projects.

FINGERPRINT SENSOR:

The R307 fingerprint sensor is a compact and reliable fingerprint recognition module that can be used in a variety of applications such as access control, time and attendance systems, and personal identification. It is equipped with an optical sensor that can capture high-resolution images of fingerprints and can recognize and match fingerprints with a high degree of accuracy. The sensor has a built-in processor that can perform various functions such as image processing, feature extraction, and template generation.

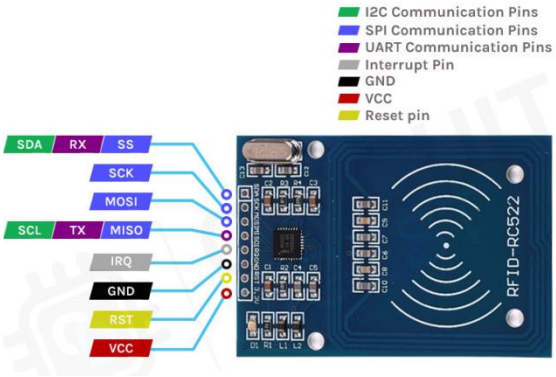


To connect the R307 fingerprint sensor to an Arduino Uno, by using Serial communication protocol. The sensor uses a UART interface for communication with microcontrollers such as the Arduino. The UART interface has two pins, TXD (Transmit Data) and RXD (Receive Data). To connect the sensor to the Arduino, To connect the TXD pin of the sensor to the RX pin of the Arduino, and the RXD pin of the sensor to the TX pin of the Arduino. To connect the VCC pin of the R307 sensor to the 5V pin of the Arduino, and the GND pin of the sensor to the GND pin of the Arduino.

Once the R307 sensor is connected to the Arduino can start sending commands to the sensor to perform various operations such as fingerprint enrolment, fingerprint recognition, and template storage. The sensor has a simple and easy-to-use command set that can be accessed through the serial interface.

RFID READER:

The RC522 RFID reader is a popular integrated circuit (IC) used for reading RFID tags. RFID stands for Radio Frequency Identification, and it is a technology that uses radio waves to communicate information between a tag and a reader. The RC522 RFID reader operates at a frequency of 13.56 MHz, which is a commonly used frequency range for RFID systems. The RC522 RFID reader consists of an antenna, a radio frequency module, and a control unit. The antenna receives the radio waves from the RFID tag and converts them into electrical signals. The radio frequency module amplifies and demodulates the signals, and the control unit processes the signals and communicates with the host system.

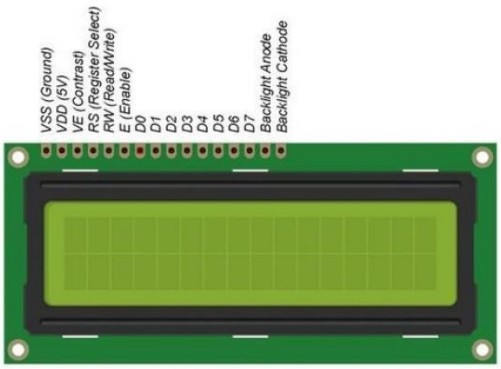


The RC522 RFID reader can read and write data to RFID tags that are compliant with ISO/IEC 14443A/MIFARE standard. The reader can detect tags within a range of up to 10 cm, depending on the size and type of the antenna used. The RC522 RFID reader supports both MIFARE Classic and MIFARE Ultralight tags, which are commonly used in access control systems, public transportation, and payment systems. The RC522 RFID reader communicates with the host system using a serial interface, such as SPI or I2C. The control unit of the RC522 RFID reader provides a command interface for controlling the reader and accessing the data stored on the RFID tags. The command interface includes commands for initializing the reader, selecting and authenticating a tag, reading and writing data to the tag, and setting the configuration of the reader.

The RC522 RFID reader includes built-in security features, such as a 48-bit unique ID number for each device and support for encryption and authentication protocols. These features ensure the security and privacy of the data stored on the RFID tags and prevents unauthorized access to the system.

LCD MODULE 16X2:

The LCD 16x2 is a display module that can show up to 16 characters per row with a total of 32 characters across the entire display. It uses liquid crystal display (LCD) technology for low power consumption and high contrast. The display is typically controlled by an integrated circuit (IC) driver, such as the HD44780, which communicates with a microcontroller or other digital device. The LCD 16x2 module typically requires 16 pins to be connected to a microcontroller or other digital device, which are used for power, ground, and data communication. The data communication is typically done using a parallel interface, where eight data pins are used to transmit the character data, along with other control pins for selecting the display row and column. The LCD 16x2 display can be programmed to display text, symbols, and even simple graphics, and the backlight can be turned on or off to improve visibility in different lighting conditions.



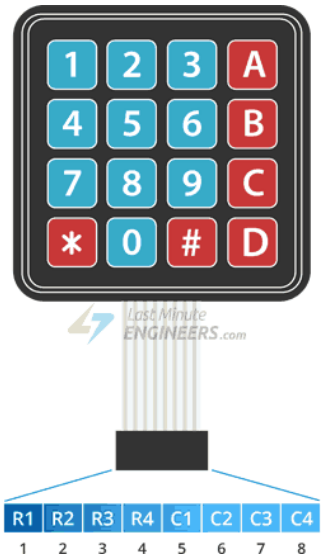
.

I2C MODULE:

I2C, or Inter-Integrated Circuit, is a communication protocol commonly used in microcontroller-based systems.This allows multiple devices to be connected to the same bus, with each device having a unique address. An I2C module is a hardware module that provides support for the I2C protocol. It typically consists of an integrated circuit (IC) that interfaces with a microcontroller and handles the low-level details of I2C communication, such as generating clock pulses, transmitting and receiving data, and addressing devices on the bus. The I2C module allows for simple and efficient communication between multiple devices, making it useful in many applications such as sensor networks, displays, and memory devices. Its simplicity and low pin count make it a popular choice for embedded systems, especially for communication between sensors and microcontrollers.

KEYPAD:

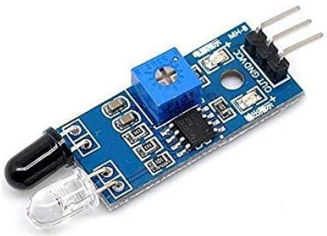
A 4x4 keypad is an input device that can be used to enter data or commands into a microcontroller, such as the Arduino Uno. It is made up of 16 keys arranged in a 4x4 matrix, with each key having a unique combination of rows and columns. This allows the keypad to be wired in a way that only requires 8 pins for connection to the microcontroller, rather than the 16 pins that would be needed if each key had its own dedicated pin. To connect a 4x4 keypad to an Arduino Uno, you will need to connect the keypad pins to the appropriate digital pins on the Arduino. The rows of the keypad are connected to four digital pins on the Arduino, while the columns are connected to another four digital pins. This allows the Arduino to determine which key has been pressed by sensing the voltage levels on the rows and columns.



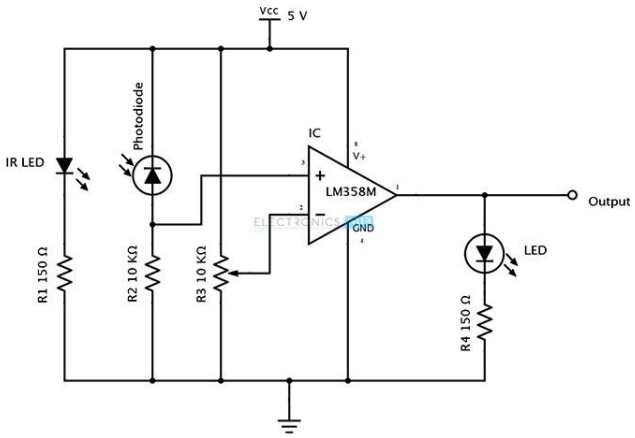
It is important to note that the pins used for the keypad can be changed in the code, but it is essential that the pins used for the rows and columns are connected to separate pins on the Arduino. This is because the rows and columns must be read and written to separately in order to detect key presses. In addition to its use as an input device, a 4x4 keypad can also be used for password authentication, security systems, or other applications that require user input.

IR SENSOR:

An infrared (IR) sensor is a device that detects the presence of objects or changes in temperature using infrared radiation. Infrared radiation is a type of electromagnetic radiation with a longer wavelength than visible light, and it is emitted by all objects with a temperature above absolute zero. IR sensors can be used in a wide range of applications, from motion detection to temperature sensing to communication systems. The basic working principle of an IR sensor is that it detects infrared radiation emitted by objects in its field of view. The sensor consists of an infrared source, which emits IR radiation, and an IR detector, which detects the radiation and converts it into an electrical signal. When an object enters the sensor's field of view, it absorbs some of the IR radiation emitted by the source. This causes a decrease in the amount of radiation detected by the detector, which in turn generates a change in the electrical signal. The sensor then processes this signal to determine the presence or absence of an object in its field of view.

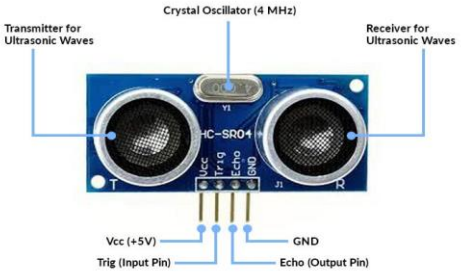


IR sensors are commonly available in two types: active and passive. Active IR sensors emit IR radiation and detect the reflection of the radiation off an object. Passive IR sensors, on the other hand, detect the radiation emitted by an object, which varies with the object's temperature. To connect an IR sensor to an Arduino board, you need to first identify the pins on the sensor. IR sensors typically have three pins: VCC, GND, and OUT. VCC is the power supply pin, GND is the ground pin, and OUT is the output pin that sends a signal to the Arduino when an object is detected. Once you have identified the pins, you can connect the IR sensor to the Arduino using jumper wires. Connect the VCC pin to the 5V pin on the Arduino, the GND pin to the GND pin on the Arduino, and the OUT pin to any of the digital input pins on the Arduino. To program the Arduino to read the output from the IR sensor, you need to use the appropriate library for the specific IR sensor you are using. The library provides functions that read the sensor output and perform the desired action based on the detected input.



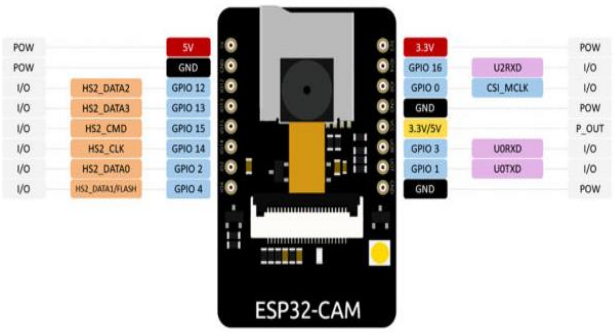
ULTRASONIC SENSOR:

The HC-SR04 is an ultrasonic sensor module that is commonly used for distance measurement applications in robotics and automation. It operates by emitting ultrasonic waves from a transmitter and detecting their reflection from nearby objects using a receiver. The time taken for the waves to travel to the object and back is measured, and this is used to calculate the distance to the object using the speed of sound in air. The sensor requires a 5V power supply and has four pins: Vcc (power), GND (ground), Trig (trigger), and Echo (echoed signal). To use the sensor, a trigger signal is sent to the Trig pin, and the resulting echo signal is received at the Echo pin. The distance to the object can then be calculated using the formula Distance = (Time * Speed of Sound) / 2. The HC-SR04 is a low-cost, easy-to-use, and accurate sensor that has become popular in many applications.



ESP32 CAMERA MODULE:

The ESP32 camera module is a small camera unit that can be integrated with the ESP32 microcontroller for a wide range of applications. The module features a 2 megapixel OV2640 camera sensor with a resolution of 1600 x 1200 pixels, capable of capturing JPEG images and video up to 640 x 480 pixels at 60 frames per second. It also includes a built-in lens with a 120-degree field of view, making it suitable for applications such as surveillance cameras, video streaming, and facial recognition systems.



The camera module is connected to the ESP32 via a standard SPI interface, requiring a minimum of 4 GPIO pins for operation. It also includes an SD card slot for storing images and video. The module can be powered using a 3.3V power supply and consumes approximately 100mA of current during operation. It also includes a sleep mode for low power consumption when not in use.

The pin details of the ESP32 camera module are as follows:

- 3V3: 3.3V power supply pin
- GND: Ground pin
- CS: Chip select pin, used to enable the camera module
- SCK: Serial clock pin for SPI communication
- MOSI: Master out slave in pin for SPI communication
- MISO: Master in slave out pin for SPI communication
- XCLK: External clock pin, used to control the sensor clock
- PWDN: Power down pin, used to turn off the camera sensor when not in use
- RESET: Reset pin, used to reset the camera module
- D7: Data pin for camera control

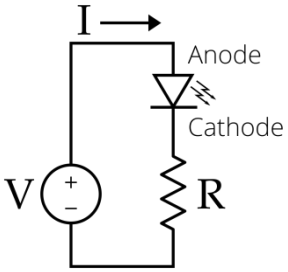
These pins can be connected to the appropriate GPIO pins on the ESP32 microcontroller for operation. The ESP32 camera module can be programmed using the Arduino IDE or the ESP-IDF development framework, which provides a range of libraries and tools for developing applications on the ESP32**.**

BUZZER:

A buzzer is a device that generates sound, typically used to provide audible alerts or signals in electronic devices. Buzzer modules are commonly used in electronic projects and can be found in a variety of shapes and sizes. A buzzer typically consists of a metal or plastic housing that contains an electromagnetic coil and a spring-mounted armature. When an electrical current is passed through the coil, it creates a magnetic field that pulls the armature towards the coil. This movement of the armature causes the device to vibrate, producing a sound. Buzzer modules are typically driven by a digital signal from a microcontroller or other digital device. The sound produced by the buzzer can be controlled by varying the frequency and duration of the digital signal. Buzzer modules can produce a wide range of sounds, from simple beeps and tones to more complex melodies. Some buzzers have built-in sound generators, allowing them to produce a variety of pre-programmed sounds or music.

LED (LIGHT EMMITING DIODE):

LEDs are commonly used in a wide range of applications, from indicator lights on electronic devices to decorative lighting in homes and buildings. The basic working principle of an LED is that it converts electrical energy into light energy. The LED consists of a p-n junction, which is formed by doping two regions of a semiconductor with different types of impurities. When a voltage is applied across the p-n junction, electrons and holes combine, releasing energy in the form of photons. This energy causes the LED to emit light.



To connect an LED to an Arduino board, you need to first identify the polarity of the LED. LEDs have two leads: the anode (positive) and cathode (negative). The anode is usually the longer lead or has a flat edge, while the cathode is the shorter lead or has a rounded edge. Connect the anode of the LED to a digital output pin on the Arduino using a resistor. The resistor limits the current flowing through the LED to prevent it from burning out. The value of the resistor depends on the specific LED and the desired brightness. A common value is 220 ohms. Connect the cathode of the LED to the GND pin on the Arduino. To program the Arduino to control the LED, you can use the digitalWrite() function to set the output pin to HIGH or LOW, depending on whether you want to turn the LED on or off. You can also use pulse-width modulation (PWM) to control the brightness of the LED by varying the duty cycle of the output waveform.

SERVO MOTOR:

The SG90 servo motor is a small, low-cost motor commonly used in hobbyist and educational projects. It can be controlled by a microcontroller or other digital device using a pulse width modulation (PWM) signal.

The SG90 servo motor has three pins:

- Power pin (usually red wire): This pin is used to supply power to the motor. It typically operates at 5V DC and draws a current of around 100mA.
- Ground pin (usually brown or black wire): This pin is used to connect the motor to the ground or negative terminal of the power supply.
- Control pin (usually yellow or orange wire): This pin is used to send the PWM signal to the motor to control its position.The duty cycle of the PWM signal determines the position of the motor's output shaft.

It is important to note that the SG90 servo motor should not be directly powered by a microcontroller or other digital device, as it requires more power than these devices can provide. Instead, it should be powered by a separate power supply with sufficient current capacity.

SOFTWARE DESCRIPTION:

ARDUINO IDE:

Arduino IDE (Integrated Development Environment) is a software tool used for programming and development of Arduino boards.

The main features of the Arduino IDE include:

- **Code Editor:** The code editor is the main interface of the Arduino IDE where you can write, edit and upload code to the Arduino board. It includes features such as syntax highlighting, auto-completion, and code snippets to make programming easier.

- **Sketches:** Arduino programs are referred to as "sketches" and can be easily created and saved within the IDE. The sketch contains two main functions: the setup() function, which is called once at the start of the program, and the loop() function, which is called repeatedly as long as the program is running.

- **Library Manager:** The Library Manager allows users to easily install and manage libraries for their Arduino projects. It is a collection of pre-built libraries that can be used to add functionality to your projects. Users can also create their own libraries and add them to the IDE.

- **Serial Monitor:** The Serial Monitor allows users to communicate with the Arduino board and monitor the data being sent and received through the serial port. This is particularly useful for debugging and troubleshooting.

- **Board Manager:** The Board Manager allows users to select the type of Arduino board they are using, configure settings, and install the necessary drivers. This is important because different Arduino boards may have different specifications and require different drivers.

- **Upload:** The Upload feature allows users to upload their sketches to the Arduino board and begin executing the program. Users can select the correct board and serial port before uploading the sketch.

- **Tools:** The Tools menu includes a range of options for configuring and customizing the IDE. This includes options for setting the board type, serial port, programmer, and other settings.

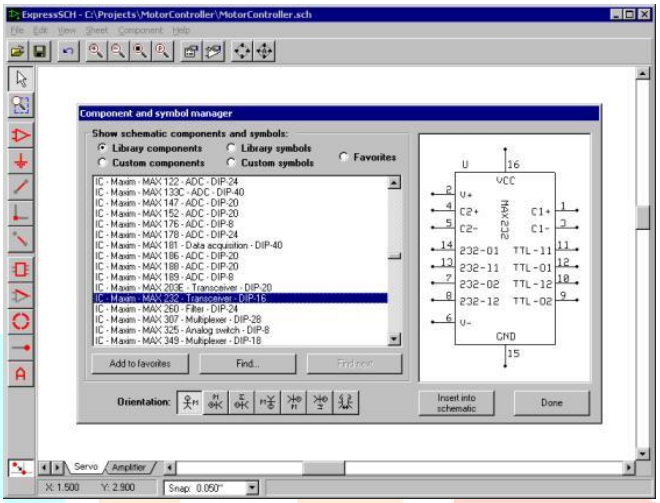
Overall, the Arduino IDE is a user-friendly software tool that simplifies the programming process for beginners and experienced users alike. It is compatible with a wide range of Arduino boards and shields, making it a versatile tool for a variety of applications. With its many features and community support, the Arduino IDE is an essential tool for anyone interested in electronics and programming.

In addition to the basic features listed above, the Arduino IDE also supports advanced features such as debugging and profiling tools, version control integration, and multiple file editing. The IDE can also be extended through plugins and add-ons, allowing users to customize the tool to their specific needs.

Additionally, the Arduino community provides a wealth of resources and tutorials to help users get started and troubleshoot any issues they may encounter.

EXPRESS PCB:

Express PCB is a free-to-use software program for designing printed circuit boards (PCBs). It is a simple and user-friendly tool that is ideal for beginners and hobbyists who want to design and create their own PCBs.



Some of the key features of Express PCB include:

- **Schematic Capture:** Express PCB allows users to create schematic diagrams of their circuits using a library of pre-built symbols. The software also provides a range of editing tools to help users create and modify their schematic diagrams.
- **Board Layout:** Express PCB includes a powerful board layout editor that allows users to place components on the board, route traces between components, and add text and graphics. The software also includes a range of design rules to ensure that the PCB meets the required specifications.
- **Gerber Export:** Once the board design is complete, Express PCB allows users to export the design as Gerber files, which can be used to manufacture the PCB.
- **Parts Library:** Express PCB comes with a large library of pre-built parts and components that users can use to create their designs. Users can also create their own custom parts library.
- **Auto-Router:** The software includes an auto-router feature that can automatically route traces between components on the board. This can save users a lot of time and effort, especially for complex designs.
- **3D Viewer:** Express PCB includes a 3D viewer that allows users to view their board designs in 3D, providing a realistic view of how the final product will look.

Overall, Express PCB is a powerful and user-friendly software tool that can help users design and create their own PCBs quickly and easily. The software is free to download and use, making it accessible to hobbyists and beginners who may not have a large budget for PCB design software. Additionally, Express PCB provides a range of tutorials and resources to help users get started and troubleshoot any issues they may encounter during the design process.

WEB SERVER:

The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capabilities. It can be used as a standalone microcontroller or as a Wi-Fi enabled communication module with other microcontrollers. One of its popular applications is to create a webserver page to control and monitor devices over the internet.

Here are the details on how to create a webserver page with ESP8266:

- Set up the ESP8266 with Arduino IDE and connect it to Wi-Fi.
- Import the required libraries such as ESP8266WiFi.h and ESP8266WebServer.h.
- Create a web server object using the ESP8266WebServer class.
- Define a callback function that will handle requests made to the webserver. The callback function can take inputs from HTML forms and execute specific actions on the ESP8266.
- Write HTML code for the web page that the user will see.
- Create a server.begin() statement in the setup() function to start the web server.
- In the loop() function, run the server.handleClient() method to handle incoming client requests.
- Upload the sketch to the ESP8266 and test the web page in a browser by entering the IP address of the ESP8266 in the browser address bar.

By following these steps, the ESP8266 can serve up a web page to control and monitor devices over the internet. This can be useful for remote control of home automation devices or other internet of things (IoT) applications.

CONCLUSION:

In conclusion, the proposed system for bank security utilizing Microcontroller, IoT technology, biometric authentication systems, sensors, keypad systems, camera modules, LCD, Buzzer, and webserver, provides a comprehensive and multi-layered approach to bank security. The Arduino UNO board acts as the central controller for the system, receiving inputs from the various sensors and IoT devices and processing the data to trigger appropriate actions in case of any security breaches. The system incorporates a webserver that can display real-time data related to the security status of the bank and send alerts to the security personnel and bank manager in case of any security breaches. The system ensures that only authorized personnel can access restricted areas, detects any unusual activity or security breaches, and provides real-time video feeds and alerts. The use of IoT technology and a range of devices ensure that the system is efficient, reliable, and effective in addressing the evolving security threats faced by banks today.

In summary, the proposed bank security system offers a comprehensive and reliable solution that can significantly improve the security of banks while reducing the workload of security personnel. The system can be easily implemented in existing bank security systems and can be customized to meet the specific security requirements of individual banks.

DISCUSSION:

The proposed bank security system using Embedded System and IoT Technology offers several advantages over traditional security systems used in banks. In this section, we will discuss the various advantages and limitations of the proposed system.

Advantages:

1. **Multi-layer security:** The proposed system incorporates multiple layers of security to ensure the safety of the bank.The IR sensor and ultrasonic sensor detect any suspicious activity, and the ESP32 camera module provides a visual record of all individuals who enter the bank.

2. **Real-time monitoring:** The proposed system utilizes a webserver to display real-time data related to the security status of the bank. This enables security personnel and bank managers to monitor the security status of the bank from anywhere.

3. **Cost-effective:** The proposed system is cost-effective and can be easily implemented in existing bank security systems. The use of open-source hardware and software reduces the cost of the system significantly.

4. **Customizable:** The proposed system is highly customizable and can be tailored to meet the specific security requirements of individual banks. The system can be expanded with additional sensors and IoT devices to improve the security of the bank further.

Limitations:

1. **Dependence on internet connectivity:** The proposed system relies on internet connectivity to provide real-time updates on the security status of the bank. Any disruption in internet connectivity can lead to a delay in receiving alerts related to security breaches.

2. **False alarms:** The proposed system may trigger false alarms in case of any technical glitches. The system must be regularly maintained and tested to ensure that it functions correctly.

3. **Privacy concerns:** The use of the ESP32 camera module raises privacy concerns since it captures images of all individuals who enter the bank. Proper measures must be taken to ensure that the images are stored securely and are not misused.

In conclusion, the proposed bank security system offers several advantages over traditional security systems used in banks. The system is cost-effective and highly customizable, making it a suitable security solution for banks of all sizes. However, the system also has certain limitations that must be addressed to ensure its effective functioning.

REFERENCE:

1. A bank locker equipped with fingerprint recognition technology and image capturing features was developed by Ambrish Kumar1, Anish Kumar2, Kushagra Gohil3, Laxit Porwal4, Manish Cheepa5, and Ankit Vijayvargiya6 from the Department of Electrical Engineering at SKIT in Jaipur, India (302033).

2. In 2017, Divya R.S presented a paper titled "Super Secure Door Lock System for Critical Zone" at the International Conference on Network and Advances in Computational Technology.

3. In 2014, Srinivatsan Sridharan from the Department of Computer Science at the International Institute of Technology in Bangalore, India, developed a system for authenticated and secure biometric-based access to bank safety lockers.

4. Amit Verma from the Department of Electronics and Communication Engineering (ECE) at Amity University in Noida, Uttar Pradesh, India, authored an IEEE paper in 2014 on the development of an intelligent system for bank security.

5. In 2016, Pradeep Kumar from the Department of Electronics and Communication Engineering (ECE) at Amity University developed an efficient multi-stage security system for user authentication.

6. In 2017, N. Anusha from the Department of Computer Science and Engineering at Sathyabama University in Chennai, India, developed a locker security system that utilizes facial recognition technology and OTP (one-time password) authentication.

7. In 2015, Sanal Malhotra from the Department of Electronics and Communication Engineering (ECE) at Amity University in Uttar Pradesh, India, developed a banking security system that utilizes hand gesture recognition.

8. In 2017, Avinash D. Harale from SKN Sinhgad College of Engineering in Korti, Maharashtra, India, conducted research on the use of iris recognition as a biometric for security systems.

9. X. Judong and W.-Y. Yau authored a paper titled "Fingerprint Minutiae Matching Based on Local and Global Structures" which was presented at the ICPR conference in 2000. The paper can be found in the conference proceedings on pages 1038-1041.

10. Robert T. Collins, Alan J. Lipton, Hironobu Fujiyoshi, and Takeo Kanade published a paper titled "Algorithms for Cooperative Multisensor Surveillance" in the IEEE Proceedings in October 2001. The paper can be found in Volume 89, Issue 10, and spans pages 1456-1477.

11. Piyush Mayank and Sudipta Mukhopadhyay presented a paper titled "Temporal Correlation and Probabilistic Prediction Based Face Detection Framework in Real Time Environment" at the 4th International Conference on Intelligent Human Computer Interaction, held in Kharagpur, India in December 2012. The paper was published in the IEEE Proceedings of the conference.

12. Weiming Hu, Tieniu Tan, Liang Wang, and Steve Maybank wrote a paper titled "A Survey on Visual Surveillance of Object Motion and Behaviors" which was published in the IEEE Transactions on Systems, MAN, and Cybernetics journal in August 2004. The paper can be found in Volume 34, Issue 3, and spans pages 334-351.

13. Sadeque Reza Khan authored a paper titled "Development of Low Cost Private Office Access Control System (OACS)" which was published in the International Journal of Embedded Systems and Applications in June 2012. The paper can be found in Volume 2, Issue 2.

14. The paper "Design and Implementation of Home Automation System" was authored by A. Alheraish and was published in the IEEE Transactions on Consumer Electronics in November 2004. The paper is available in volume 50, issue 4 and spans pages 1087 to 1092.

15. The paper authored by V. Vinoth Krishnan, M. Saianand, and J.S. Vimali, titled "Response Mechanism for Crisis Times from Social Networks," was published in the June 2016 issue of the International Journal of Pharmacy & Technology (IJPT). The volume number is 8, the issue number is 2, and the pages are 11958-11966.