PROJECT REPORT

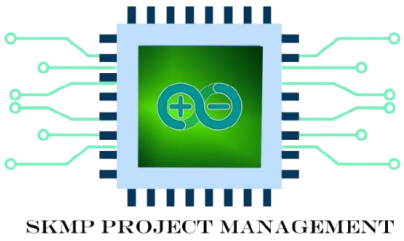
ON

"RFID Smart Home Security & Automation System"

THIS PROJECT & RESEARCH REPORT HAS BEEN INDEPENDENTLY DEVELOPED BY ME AND IS NOT SUBMITTED TO ANY COLLEGE OR UNIVERSITY FOR ACADEMIC EVALUATION

Developed by

Name:-Suzen Kumar Mohanty (**Reg.No**.2421331063)



SKMP PROJECT MANAGEMENT

DEPARTMENT OF IOT

POLISHLINE.BALASORE, ODISHA, INDIA

MAY -2026

“Dedicated to my beloved parents ,and teachers who have worked hard throughout my education”

SKMP PROJECT MANAGEMENT

CERTIFICATE

*This is to certify that the project entitled "**RFID Smart Home Security & Automation System**"*

Has been independently developed and completed by Suzen Kumar Mohanty for the purpose of enhancing technical knowledge, skills, and practical understanding.

This project is a self-initiated work carried out with person al interestand research. It has not been submitted to any college, university, or institution for the award of any degree or diploma.

The work presented in this project is genuine and has been completed by the developer himself.



Suzen Kumar Mohanty

(Project Developer)

Date: 29/05/2026

Place:-Balasore,Odisha,India

SELF ATTESTATION

I here by declare that I have personally worked on the project entitled "**RFID Smart Home Security & Automation System**"All the data, analysis, and implementation presented in this project are the result of my own efforts and genuine work .Any external sources of information, if used, have been properly acknowledged.

This project is created solely for learning , skill development ,and professional improvement, and has not been submitted to any institution for academic purposes.



Suzen Kumar Mohanty

(Project Developer)

Date: **29/05/2026**

Place:Balasore,Odisha,India

SKMP PROJECT MANAGEMENT

DECLARATION

I hereby declare that the project titled "**RFID Smart Home Security & Automation System**"is an original work carried out by me based on my own idea, research, and implementation.

This project that has not been submitted previously ,in part or in full, to any college, university, or institution for the award of any degree, diploma, or certification.

I confirm that all the information presented in this project is true to the best of my knowledge. Any references or sources used have been properly acknowledged.

I take full responsibility for the authenticity and originality of this work.

SKMP PROJECT MANAGEMENT

Name: Mr. Suzen Kumar Mohanty

Branch: Computer Science And Engineering

Institution:[Srinix Collage Of Engineering ,Independent]

Date:[**29/05/2026**]

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to everyone who contributed, directly or indirectly, to the development of this project, "**RFID Smart Home Security & Automation System**."

This project is the result of my personal interest, dedication, continuous learning, and exploration of electronics, automation, sensor technology, and control systems.

I am thankful to the developers of Arduino, the creators of open-source hardware and software resources, and the technical communities whose documentation, tutorials, and knowledge-sharing platforms helped me understand and implement the concepts used in this project.

I would also like to acknowledge the importance of self-learning, practical experimentation, and problem-solving throughout the development process. These experiences helped me strengthen my technical knowledge and improve my understanding of real-world automation systems.

Finally, I am grateful to everyone who supports innovation, DIY engineering, and independent technical projects. This work reflects my enthusiasm for learning, creating, and exploring new possibilities in technology.

Developed By:

Suzen Kumar Mohanty

ABOUT MYSELF



I am Mr. Suzen Kumar Mohanty , a passionate and dedicated Web Developer and SOC Analyst (Level 1) from the field of Computer Science and Engineering, with strong expertise in HTML, CSS, JavaScript, and I specialize in building scalable, responsive, and high-performance web applications that deliver seamless user experiences across all devices and screen sizes.

With a keen eye for detail, I focus on writing clean, maintainable, and well-structured code. My development approach is centered around Creating intuitive user interfaces, ensuring both functionality and aesthetic quality. I follow modern front-end development practices such as component-based architecture, responsive design principles, and performance optimization techniques to build efficient and user-friendly applications.

Beyond web development, I actively work on IoT-based solutions, where I integrate hardware and software to create smart, real-world systems. I have hands-on experience with Arduino Uno and various sensors, enabling me to develop projects such as environmental monitoring systems, smart automation solutions, and real-time data tracking applications.

One of my key strengths lies in connecting IoT devices with web technologies. I build interactive dashboards that allow real-time data visualization, giving users the ability to monitor, analyze, and control devices remotely. My work focuses on bridging the gap between the physical and digital world by transforming raw sensor data into meaningful insights.

I am deeply interested in developing innovative, data-driven solutions that combine web technologies with embedded systems. My goal is to create impactful applications that solve real-world problems while improving efficiency, automation, and user experience.

With a strong passion for continuous learning and innovation, I consistently explore new tools, frameworks, and technologies to enhance my skills and deliver high-quality, future-ready solutions.

Name: Mr. Suzen Kumar Mohanty

Branch: Computer Science And Engineering

MyPortPolioLink:-https://suzen-kumar-mohanty-8fdv.vercel.app/

ABSTRACT

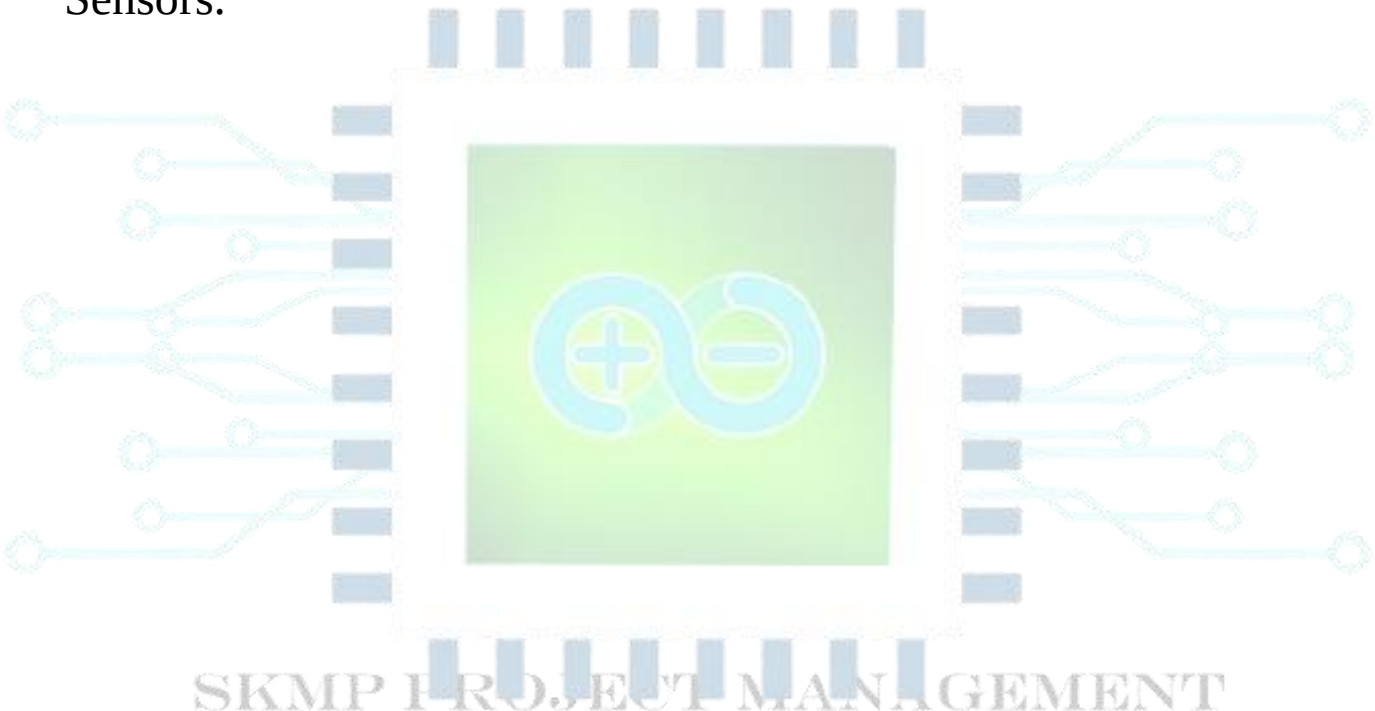
The rapid growth of the Internet of Things (IoT) has enabled the development of intelligent homes that improve security, convenience, and energy efficiency. This project presents the design and implementation of an **RFID-based Smart Home Security and Automation System** that provides secure keyless entry and automated control of household appliances. The system uses an RFID reader and authorized RFID cards or tags to authenticate residents and control the main door lock. When a valid card is scanned, the microcontroller verifies the identification and activates an electric lock or servo motor to grant access; an invalid card triggers an alert and denies entry. Similar RFID-based access-control systems have been widely implemented using microcontrollers, electronic locks, and real-time access logging.ejournal.uin-suska.ac+1

In addition to security, the system supports home automation through sensors and wireless connectivity. A PIR motion sensor can activate lighting when movement is detected, while a temperature and humidity sensor can control a fan or air-conditioning system for comfort and energy savings. Users can monitor and control connected devices remotely through a mobile application or web dashboard connected through Wi-Fi. IoT-based smart-home systems commonly combine RFID door access, automatic lighting, appliance control, and remote monitoring to create a more secure and efficient living environment.publisher.uthm.edu+1

The proposed system also includes safety features such as buzzer alarms, status indicators on an LCD display, and optional

notifications for unauthorized access attempts. Access records can be stored or displayed to help track entry and exit activity. By integrating RFID authentication, sensor-based automation, and IoT communication, the system reduces dependence on physical keys, improves household security, and offers a low-cost, scalable solution for modern smart homes.arxiv+1

Keywords: RFID, Smart Home, Home Automation, IoT, Security System, Door Access Control, Microcontroller, Sensors.



SKMP PROJECT MANAGEMENT
SKMP PROJECT MANAGEMENT

LIST OF FIGURES

Figure No.	Figure Title	Page No.
01	RFID SMART HOME SECURITY	01
02	OBJECTIVE IMAGE	03
03	ARDUINO UNO BOARD	11
04	HC-SR04 ULTRASONIC SENSOR	12
05	REGISTER 220 OHM	12
06	BREAD BOARD	13
07	SERVO MOTOR (SG 90)	14
08	JUMPER WIRES	15
09	LED	16
10	USB CABLE	17
11	POWER SUPPLY 9V BATTERY WITH CONNECTOR	18
12	RFID CARD	18
13	CIRCUIT DIAGRAM	36
14	CIRCUIT REAL IMAGE	37

SKMP PROJECT MANAGEMENT
SKMP PROJECT MANAGEMENT

INDEX

Sl. No.	Contents / Chapter Name	Page No.
1	Introduction	1
1.1	Background	1
1.2	Problem Statement	2
1.3	Proposed Solution	2
2	Objectives	3
2.1	Primary Objectives	4
2.2	Secondary Objectives	4
3	Literature Review	5
3.1	RFID Technology	5
3.2	RFID Frequency Bands	5
3.3	MFRC522 RFID Reader	6
3.4	Smart Home Automation	7
4	System Overview	8
4.1	System Architecture	8
4.2	Core Working Principle	9
5	Hardware Components	10
5.1	Arduino UNO Board	10
5.2	HC-SR04 Ultrasonic Sensor	11
5.3	220Ω Resistor	12
5.4	Breadboard	13
5.5	Servo Motor (SG90)	13
5.6	Jumper Wires	14
5.7	LED	15
5.8	USB Cable	16
5.9	Power Supply (9V Battery with Connector)	17

5.10	RFID Card	18
5.11	Main Controller	19
5.12	RFID Access Module	19
5.13	Door Lock and Actuation	20
5.14	Security and Safety Sensors	21
5.15	User Interface and Connectivity	21
6	Software Architecture	22
6.1	Firmware Modules	22
6.2	User Roles	23
6.3	Mobile Application Features	23
6.4	Complete Arduino Source Code	24
7	Detailed Working Process	34
7.1	Authorized Entry	34
7.2	Unauthorized Entry Attempt	34
7.3	Fire or Gas Emergency	35
7.4	Automation Scenario	35
8	Circuit Design	36
8.1	RFID Reader to ESP32 Connection	37
8.2	Sensor Connections	38
9	Security Design	39
9.1	RFID Security Risks	39
9.2	Security Controls	39
9.3	Privacy and Data Protection	40
10	Testing Plan	41
10.1	Functional Testing	41
10.2	Security Testing	41
10.3	Reliability Testing	42
11	Market Analysis	43
11.1	Market Opportunity	43
11.2	Target Customers	43

11.3	Competitive Advantage	44
12	Advantages	44
13	Limitations	45
14	Conclusion	46
15	Future Scope	47
15.1	Biometric Authentication	47
15.2	AI-Based Security Intelligence	48
15.3	Edge Computing and Offline Intelligence	48
15.4	Advanced Mobile and Cloud Platform	49
15.5	Smart Home Ecosystem Integration	49
15.6	Energy Management and Sustainability	50
15.7	Enhanced Safety and Emergency Response	51
15.8	Advanced Access Management	51
15.9	Stronger Cybersecurity	52
15.10	Commercial Expansion	53
15.11	Long-Term Vision	54
16	References	55
17	Project Link	58

SKMP PROJECT MANAGEMENT

Introduction

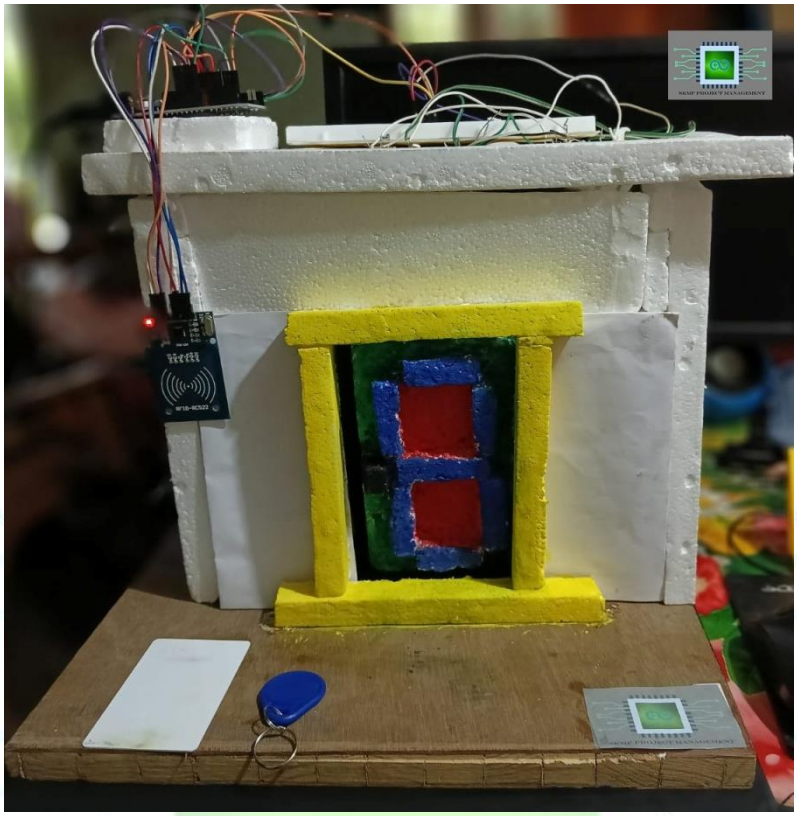


Fig-01

1.1 Background

Traditional mechanical locks depend on physical keys, which can be lost, duplicated, or stolen. They also provide limited visibility into who entered the property and when. RFID-based access control replaces or supplements mechanical keys with electronic credentials that can be issued, revoked, time-restricted, and logged centrally.mikroe+1

A smart home security system extends this capability by integrating door access with sensors, automation, alarms, and remote monitoring. For example,

an authorized RFID tap can unlock the main door, switch on entry lighting, disarm the intrusion alarm, and record the entry event.github+1

1.2 Problem Statement

Many households and small commercial premises face the following problems:

- Loss, theft, or unauthorized duplication of physical keys
- No reliable record of entry and exit activity
- Difficulty granting temporary access to guests, domestic workers, delivery personnel, or tenants
- Delayed awareness of unauthorized entry, fire, gas leakage, or abnormal motion
- Manual operation of lights, fans, and appliances
- Poor integration between door locks, alarms, and mobile notifications
- High cost and complexity of professionally installed commercial security systems

1.3 Proposed Solution

The proposed system provides a low-cost, modular, and scalable smart-security platform. It uses RFID authentication as the primary access method, supported by a keypad/PIN or mobile app as a backup. It also integrates motion detection, door-status sensing, gas and fire detection, automated lighting, and cloud-based event logging.github+2

The system can operate in three modes:

Mode	Description
Standalone mode	RFID authentication and lock control work locally without internet dependency.

Mode	Description
Connected mode	The system syncs access logs, alerts, and controls with a mobile app or cloud dashboard.
Emergency mode	Fire, gas-leak, tamper, or forced-entry events trigger alarms and notifications even if normal automation is disabled.

2. Objectives



Fig 2

2.1 Primary Objectives

- Develop an RFID-based smart door-lock system for secure residential access.
- Authenticate users through RFID cards, key fobs, or NFC-enabled devices.
- Automatically unlock the door only for authorized credentials.
- Maintain a digital entry and exit log with date, time, user identity, and access result.
- Detect unauthorized access attempts and trigger local and remote alerts.
- Automate lights, fans, appliances, and entry lighting based on occupancy or access events.
- Provide remote monitoring and control through a mobile application or web dashboard.
- Ensure the system continues to operate during internet or cloud-service failure.

2.2 Secondary Objectives

- Add multi-user access management, including admin, family member, guest, and service-person roles.
- Support temporary access validity for visitors, deliveries, cleaners, and maintenance staff.
- Integrate fire, smoke, gas-leak, motion, and door-tamper detection.
- Reduce electricity wastage through automated lighting and appliance control.
- Create a scalable design that can support multiple doors, rooms, or buildings.
- Keep the bill of materials affordable for mass deployment in India.

SIMPLE PROJECT MANAGEMENT

3. Literature Review

3.1 RFID Technology

RFID, or Radio-Frequency Identification, is a wireless identification technology in which a reader communicates with a tag or card. The tag contains a microchip and antenna; the reader supplies energy through radio-frequency coupling and receives identifying data from the tag.scribd+1

RFID systems generally consist of:

- **Tag or transponder:** Card, key fob, sticker, or NFC-enabled device
- **Reader or interrogator:** Device that reads tag information
- **Antenna:** Enables radio communication between reader and tag
- **Controller:** Microcontroller or access-control panel that validates credentials
- **Actuator:** Electric strike, solenoid lock, motorized lock, or relay-controlled device
- **Software/interface:** Mobile app, web dashboard, database, or local displayambient+1

3.2 RFID Frequency Bands

SKMP PROJECT MANAGEMENT

Frequency band	Typical range	Common use	Suitability for home access
Low Frequency, 125 kHz	Short range	Legacy proximity cards	Low security; not recommended for new designs
High Frequency,	Short	MIFARE, NFC,	Best fit for residential

Frequency band	Typical range	Common use	Suitability for home access
13.56 MHz	range	access cards	smart locks
Ultra High Frequency, 860–960 MHz	Longer range	Vehicle tags, logistics, warehouse tracking	Useful for gates, not ideal for door locks

Modern access-control readers commonly operate at 13.56 MHz using ISO/IEC 14443-compliant smart cards. For new secure designs, MIFARE DESFire EV2 or EV3 credentials with AES-128 mutual authentication are recommended, whereas legacy 125 kHz EM4100 or HID Prox credentials lack cryptographic protection.mikroe+1

3.3 MFRC522 RFID Reader

The MFRC522 is a widely used low-cost RFID reader module for prototypes and educational systems. It operates at 13.56 MHz, supports ISO/IEC 14443A and MIFARE communication, and commonly interfaces with microcontrollers through SPI.cdn.aui+2

Key characteristics include:

- Operating frequency: 13.56 MHz
- Typical reading distance: approximately 3–5 cm, depending on antenna and tag quality
- Communication interface: SPI, with I2C and UART support in some configurations
- Supported tags: MIFARE Classic 1K/4K and compatible ISO 14443A tags
- Supply voltage: 3.3 V logic level, requiring careful interfacing with 5 V microcontrollerscdn.aui+2

SKMP PROJECT MANAGEMENT

For a production-grade product, the MFRC522 is suitable for basic UID-based access, but a more secure reader supporting MIFARE DESFire EV2/EV3, such as PN5180 or ST25R3916-based hardware, is preferable.mikroe

3.4 Smart Home Automation

Smart home automation uses sensors, microcontrollers, relays, communication modules, and cloud platforms to monitor and control household devices. Common functions include motion-activated lighting, remote appliance control, temperature and humidity monitoring, gas-leak alerts, fire detection, and security notifications.github+2

An ESP32-based implementation is especially suitable because it provides Wi-Fi connectivity, sufficient processing capability, multiple GPIO pins, and support for cloud and mobile application integration.github+1

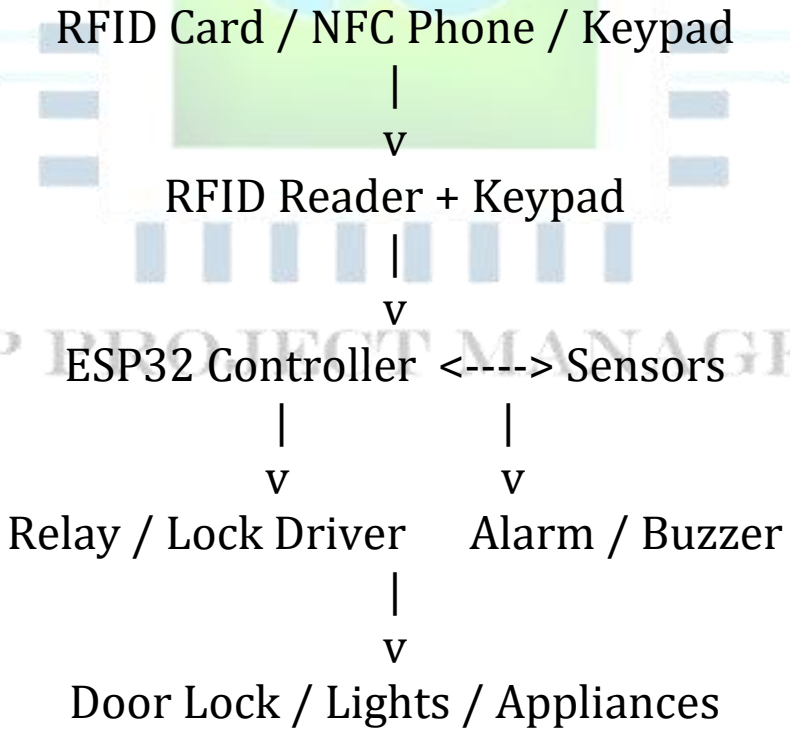
SKMP PROJECT MANAGEMENT

4. System Overview

4.1 System Architecture

The proposed system has five major layers:

1. **Credential layer:** RFID cards, key fobs, NFC phones, PIN keypad, and mobile app
2. **Sensing layer:** PIR motion sensor, magnetic reed switch, gas sensor, flame/smoke sensor, temperature/humidity sensor
3. **Control layer:** ESP32 microcontroller or equivalent edge controller
4. **Actuation layer:** Relay modules, electric strike/solenoid lock, buzzer, LED indicators, lights, and appliances
5. **Communication layer:** Wi-Fi, Bluetooth, cloud database, mobile application, and optional GSM module



SKMP PROJECT MANAGEMENT

|
v
Wi-Fi / Cloud / Mobile App

4.2 Core Working Principle

1. The user brings an RFID card or key fob near the reader.
2. The reader captures the tag's unique identifier and sends it to the microcontroller.
3. The controller checks whether the ID is authorized, active, and within its permitted time window.
4. If valid, the controller activates the relay or lock driver to release the door lock.
5. The system records the event, switches on entry lighting, disarms the indoor alarm if configured, and sends a notification.
6. If invalid, the controller denies access, activates a buzzer, logs the failed attempt, and can send an alert after repeated failures.

SKMP PROJECT MANAGEMENT

5.Hardware Components

● Arduino UNO Board

- The Arduino UNO is an open-source microcontroller development board based on the ATmega328P microcontroller. It is widely used in electronics, robotics, automation, and embedded system projects. It allows users to connect various electronic components, such as sensors, LEDs, motors, displays, and other devices, to develop interactive electronic applications.
- The Arduino UNO board has 14 digital input/output pins, of which 6 can be used as PWM outputs, 6 analog input pins, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button.
- It can be programmed using the Arduino IDE with a simple programming language based on C and C++. The board receives instructions from the program and controls connected devices according to the given commands.

SKMP PROJECT MANAGEMENT

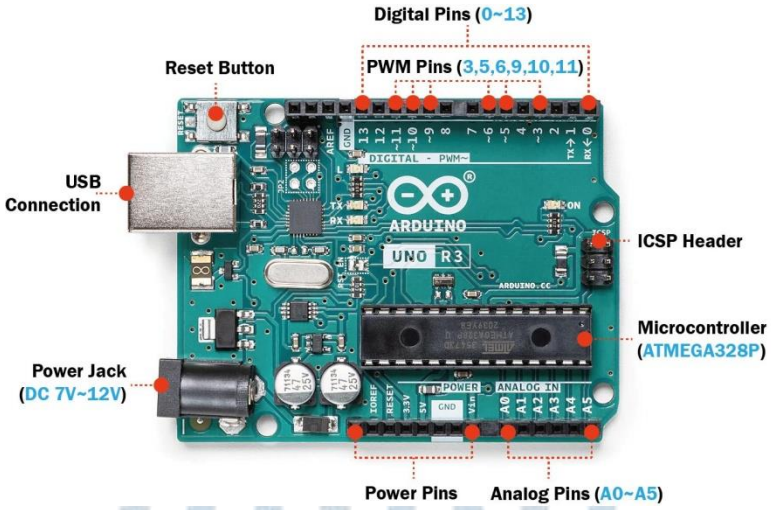


Fig -03

- ***HC-SR04 Ultrasonic Sensor***

- The HC-SR04 Ultrasonic Sensor is an electronic distance-measuring sensor that uses ultrasonic sound waves to detect objects and measure the distance between the sensor and an object. It operates by transmitting high-frequency ultrasonic waves (approximately 40 kHz) and receiving the reflected waves (echo) from an object.
- The sensor consists of two main ultrasonic transducers: one acts as a transmitter (Trig), which sends ultrasonic waves, and the other acts as a receiver (Echo), which detects the reflected waves. The distance is calculated by measuring the time taken for the ultrasonic waves to travel to the object and return to the sensor.
- The HC-SR04 sensor is commonly used with microcontrollers such as Arduino UNO for distance measurement, obstacle detection, robotics, and automatic control systems.

SMART PROJECT MANAGEMENT



Fig -04

. Resistor 220ohm

- A 220-ohm (220Ω) Resistor is a passive electronic component used to limit or control the flow of electric current in an electronic circuit. It provides a specific resistance of 220 ohms and helps protect sensitive electronic components from excessive current that may cause damage.
- In Arduino-based projects, a 220Ω resistor is commonly used to limit current flowing through LEDs and other electronic components. It helps maintain safe operating conditions and improves the reliability of the electronic circuit.
- The resistor works according to Ohm's Law, which describes the relationship between voltage, current, and resistance.

SKMP PR NAGEMENT

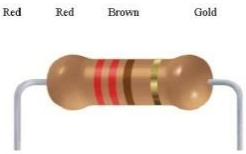


FIG-5

• Breadboard

- A Breadboard is a reusable electronic prototyping board used to build, test, and develop electronic circuits without soldering. It provides a convenient platform for connecting different electronic components using jumper wires.
- A breadboard contains several small holes arranged in rows and columns, which are internally connected through conductive metal clips. These connections allow electronic components such as resistors, LEDs, sensors, and microcontrollers to be connected easily.
- In Arduino-based projects, a breadboard is commonly used to connect components such as the Arduino UNO, HC-SR04 ultrasonic sensor, SG90 servo motor, and resistors. It helps users assemble and modify circuits quickly during the testing and development process.

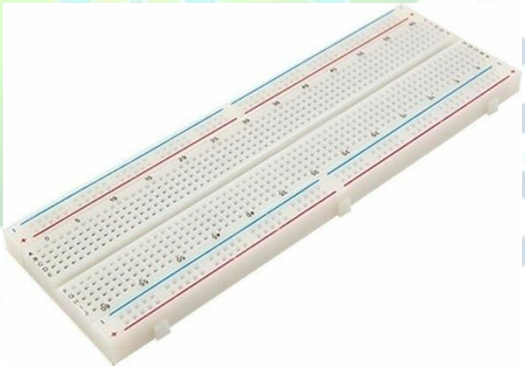


Fig-06

SKMP PROJECT MANAGEMENT

• Servo Motor (SG90)

- The SG90 Servo Motor is a small, lightweight, and compact rotary actuator used to control angular position with high precision. It is commonly used in robotics, automation, and Arduino-based electronic

projects. The SG90 is a micro servo motor that can rotate approximately 180 degrees, allowing accurate control of its shaft position.

- The SG90 servo motor consists of a DC motor, a gear mechanism, a position feedback system, and an electronic control circuit. It operates based on Pulse Width Modulation (PWM) signals received from a microcontroller such as the Arduino UNO. By varying the width of the control pulse, the motor shaft can be positioned at a desired angle.
- The SG90 servo motor is widely used in projects requiring controlled movement, such as robotic arms, automatic doors, obstacle-avoiding robots, and digital measurement systems.



Fig -07

• *Jumper Wires*

SKMP PROJECT MANAGEMENT

- Jumper Wires are electrical connecting wires used to establish temporary connections between different electronic components, sensors, and microcontroller boards. They are commonly used in electronics prototyping, Arduino projects, and embedded system development.
- Jumper wires are used to connect components such as Arduino UNO, ultrasonic sensors, servo motors, breadboards, LEDs, and other electronic modules without requiring soldering. They provide an easy and flexible

method of transferring electrical power and signals between different components.

- Jumper wires are generally available in three types: Male-to-Male, Male-to-Female, and Female-to-Female. They are commonly insulated with different colours to help identify power supply, ground, and signal connections.



Fig -08

• *LED*

- An LED (Light Emitting Diode) is a semiconductor electronic component that produces light when an electric current flows through it in the forward direction. It is a type of diode that converts electrical energy into light energy through a process known as electroluminescence.
- LEDs are widely used in electronic circuits as visual indicators to display the operating status of a system. They are available in different colours, such as red, green, blue, yellow, and white.

SKME PROJECT MANAGEMENT

- In Arduino-based projects, LEDs are commonly connected to digital output pins to indicate different operating conditions. The Arduino UNO controls the LED by switching it ON or OFF according to the programmed instructions.

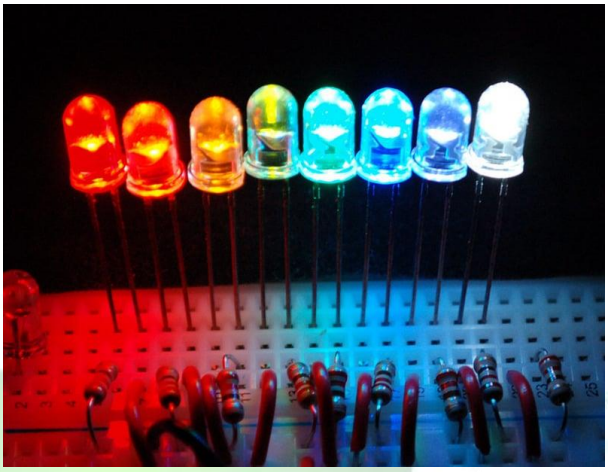


Fig-09

• *USB CABLE*

- A USB (Universal Serial Bus) Cable is an electrical communication cable used to establish a connection between electronic devices for data transmission and power supply. In Arduino-based projects, a USB cable is commonly used to connect the Arduino UNO board to a computer or laptop for programming, uploading code, and supplying electrical power.
- The USB cable allows communication between the computer and the Arduino UNO microcontroller. It transfers program instructions from the Arduino IDE to the board and also supports serial communication for monitoring sensor readings and debugging the project.

- The Arduino UNO R3 commonly uses a USB Type-B cable for connecting to a computer. One end of the cable connects to the Arduino board, while the other end connects to the computer's USB port.



Fig -10

• *Power Supply (9V Battery with connector)*

- A 9V Battery with Connector is a portable DC power source used to provide electrical energy to electronic circuits and microcontroller-based projects. It consists of a 9V battery and a battery connector that allows easy connection to the power input terminals of an electronic circuit or Arduino UNO board.
- In Arduino-based projects, the 9V battery is commonly connected to the Arduino UNO through its DC barrel jack using a 9V battery snap connector with a suitable DC plug. It supplies electrical power to the microcontroller and connected electronic components when a computer or external power adapter is not available.
- The Arduino UNO has an onboard voltage regulator that converts the input voltage into a suitable operating voltage for the board. The 9V battery provides portability and makes the project suitable for standalone operation.

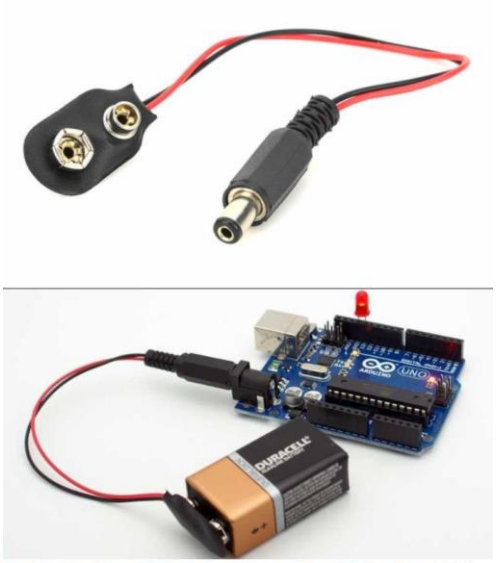


Fig -`11

• *RFID Card*

➢ An **RFID (Radio-Frequency Identification) card** is a contactless smart card that uses radio waves to transmit data between an embedded microchip and a reader device without requiring physical contact or a direct line of sight



Fig -`12

SKMP PROJ GEMENT

5.1 Main Controller

Component	Recommended option	Purpose
Microcontroller	ESP32 DevKit V1	Main processing, Wi-Fi connectivity, sensor control, cloud communication
Alternative controller	Raspberry Pi Pico W / Arduino Nano ESP32	Suitable for lower-cost or specialized designs
Power supply	12 V DC adapter, 5 V regulator, battery backup	Powers controller, lock, sensors, and relays
Real-time clock	DS3231 RTC module	Maintains accurate access timestamps during power interruptions

The ESP32 is recommended because it can manage RFID reading, relay control, sensor inputs, Wi-Fi communication, local storage, and mobile/cloud integration in a single low-cost platform.

5.2 RFID Access Module

Component	Specification	Function
RFID reader	MFRC522, 13.56 MHz	Reads RFID cards and key fobs
RFID tags	MIFARE Classic 1K cards/key fobs	User identification credentials
Secure upgrade option	PN5180 or ST25R3916 reader with DESFire EV2/EV3 cards	Stronger cryptographic authentication
NFC option	NFC-enabled smartphone	Mobile-based access

SKMD PROJECT MANAGEMENT

Component	Specification	Function where supported

The RC522 module is appropriate for a prototype or budget product. For a commercial security product, it should be paired with encrypted credentials and secure key management rather than relying only on readable tag UIDs.mikroe+1

5.3 Door Lock and Actuation

Component	Function	Notes
12 V electric strike	Releases door latch on authorization	Suitable for wooden/metal doors with compatible frame
12 V solenoid lock	electronically locks/unlocks door	Common in low-cost access-control systems
Motorized smart deadbolt	Physically extends/retracts deadbolt	Better security and door-status control
Servo motor	Prototype-only latch movement	Not recommended as final security lock
Relay module	Switches lock power and appliances	Must be rated for lock current
Door reed switch	Detects open/closed door state	Prevents false “locked” status

A servo motor is useful for demonstrating the concept, but a certified electric strike, electromagnetic lock, or motorized deadbolt is preferable for real-world deployment. The lock should fail securely according to the site’s safety requirements; for example, a fire-exit door must not trap occupants during an emergency.

SKMT PROJECT MANAGEMENT

5.4 Security and Safety Sensors

Sensor	Function	Automation response
PIR motion sensor	Detects human movement	Turns on lights, activates alarm in armed mode
Magnetic reed switch	Detects door/window opening	Sends tamper or intrusion alert
MQ-2 gas sensor	Detects LPG/smoke-related gases	Activates alarm, exhaust fan, and notification
Flame sensor	Detects flame presence	Triggers fire alert and alarm
DHT11/DHT22	Measures temperature and humidity	Supports environment monitoring and automation
Vibration/shock sensor	Detects forced entry or tampering	Raises high-priority security alert
Current sensor	Detects appliance status or abnormal load	Supports energy monitoring and fault alerts

PIR, gas, flame, ultrasonic, relay, RFID, and buzzer modules are commonly combined in ESP32-based smart-home prototypes, demonstrating the feasibility of this integrated architecture.

5.5 User Interface and Connectivity

Component	Purpose
16x2 LCD or OLED display	Shows access status, time, system mode, and error messages
Buzzer	Provides audible success, denial, alarm, and tamper alerts

Component	Purpose
LEDs	Indicate power, Wi-Fi status, access granted, access denied, and alarm state
4x4 membrane keypad	PIN-based backup access and admin configuration
Wi-Fi module	Built into ESP32 for cloud and app connectivity
GSM/GPRS module	Optional SMS/call alerts during internet failure
SD card module	Optional offline event logging
Mobile application	Remote monitoring, access management, and alerts

6. Software Architecture

6.1 Firmware Modules

The device firmware should be divided into the following modules:

- **RFID authentication module:** Reads tag UID, performs credential validation, and manages anti-passback rules
- **Access-control module:** Checks user role, access schedule, door status, and lock commands
- **Lock-driver module:** Controls relay, electric strike, motorized lock, and auto-relock timer
- **Sensor-monitoring module:** Reads PIR, door, gas, flame, temperature, humidity, and tamper inputs
- **Alarm module:** Manages buzzer, siren, notification priority, and alarm reset
- **Automation module:** Controls lights, fans, plugs, and appliances based on rules

SKOUR PROJECT MANAGEMENT

- **Communication module:** Connects to Wi-Fi, cloud database, MQTT broker, or mobile application
- **Logging module:** Stores access events locally and synchronizes them when internet is available
- **OTA update module:** Enables secure remote firmware updates
- **Configuration module:** Allows admin to add/remove users, set time windows, and configure alerts

END

6.2 User Roles

Role	Permissions
Owner/Admin	Add/remove users, view all logs, change settings, unlock remotely, receive all alerts
Family member	Regular access, limited settings, personal entry history
Guest	Temporary access for a defined period
Domestic worker	Access only during approved hours and days
Delivery personnel	One-time or short-duration access
Maintenance staff	Restricted access to specific doors and time slots
Security guard	Monitoring, alarm acknowledgment, and limited override permissions

CAMP PROJECT MANAGEMENT

6.3 Mobile Application Features

The mobile application should include:

- Live door status: locked, unlocked, open, tampered
- Remote lock/unlock with secure authentication

- RFID user registration and deletion
- Temporary guest-access generation
- Access-history dashboard
- Intrusion, fire, gas-leak, and tamper alerts
- Appliance and lighting control
- Automation scheduling
- Emergency contacts and panic button
- Offline event synchronization
- Admin audit trail

6.4 Complete Arduino Source Code

```
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

// ========================================
// RFID PINS
// ========================================
#define SS_PIN 10
#define RST_PIN 9

// ========================================
// OUTPUT PINS
// ========================================
#define BUZZER_PIN 8
#define SERVO_PIN 7
#define WHITE_LED 5
```

```
#define RED_LED 6

// ======================================
// OBJECTS
// ======================================
MFRC522 rfid(SS_PIN, RST_PIN);
Servo myServo;

// LCD ADDRESS
LiquidCrystal_I2C lcd(0x27, 16, 2);

// ======================================
// AUTHORIZED RFID UID
// ======================================
String authorizedUIDs[] = {
  "b5 6c f2 06",
  "8d 2f 65 06"
};

int numberOfAuthorizedUids =
sizeof(authorizedUIDs) / sizeof(authorizedUIDs[0]);

// ======================================
// SETUP
// ======================================
void setup() {

  Serial.begin(9600);
```

```
// RFID START
SPI.begin();
rfid.PCD_Init();

// ======================================
// SERVO SETUP
// ======================================
myServo.attach(SERVO_PIN);

// Door Closed
myServo.write(0);

delay(1000);

// Servo OFF
myServo.detach();

// ======================================
// PIN MODES
// ======================================
pinMode(BUZZER_PIN, OUTPUT);
pinMode(WHITE_LED, OUTPUT);
pinMode(RED_LED, OUTPUT);

// ======================================
// LED INITIAL STATE
// HIGH = ON
// LOW = OFF
// ======================================
```

```
  digitalWrite(WHITE_LED, LOW);
  digitalWrite(RED_LED, LOW);

  // ======================================
  // LCD START
  // ======================================
  lcd.begin();
  lcd.backlight();

  lcd.setCursor(0, 0);
  lcd.print(" RFID DOOR ");

  lcd.setCursor(0, 1);
  lcd.print("Scan Card");

  Serial.println("Scan your RFID card...");
}

// ======================================
// LOOP
// ======================================
void loop() {

  // WAIT FOR RFID CARD
  if (!rfid.PICC_IsNewCardPresent()) {
    return;
  }

  // READ RFID CARD
```

```
  if (!rfid.PICC_ReadCardSerial()) {
    return;
  }

  // ======================================
  // READ UID
  // ======================================
  String scannedUID = "";

  for (byte i = 0; i < rfid.uid.size; i++) {

    if (rfid.uid.uidByte[i] < 0x10) {
      scannedUID += "0";
    }

    scannedUID += String(rfid.uid.uidByte[i], HEX);

    if (i < rfid.uid.size - 1) {
      scannedUID += " ";
    }
  }

  scannedUID.toLowerCase();

  Serial.print("Scanned UID: ");
  Serial.println(scannedUID);

  // ======================================
  // CHECK AUTHORIZATION
```

```
// ======================================
bool isAuthorized = false;

for (int i = 0; i < numberOfAuthorizedUids; i++) {

  if (scannedUID == authorizedUIDs[i]) {

    isAuthorized = true;
    break;
  }
}

// ======================================
// ACCESS GRANTED
// ======================================
if (isAuthorized) {

  Serial.println("ACCESS GRANTED");

  lcd.clear();

  lcd.setCursor(0, 0);
  lcd.print(" ACCESS PASS ");

  lcd.setCursor(0, 1);
  lcd.print("WELCOME USER");

  // ======================================
  // LED CONTROL
```

```
    // ======================================
    digitalWrite(WHITE_LED, HIGH); // WHITE ON
    digitalWrite(RED_LED, LOW);   // RED OFF

    // ======================================
    // OPEN DOOR
    // ======================================
    myServo.attach(SERVO_PIN);

    // OPEN DOOR 120 DEGREE
    myServo.write(120);

    // BUZZER BEEP
    tone(BUZZER_PIN, 1000);
    delay(300);
    noTone(BUZZER_PIN);

    // DOOR OPEN TIME
    delay(5000);

    // ======================================
    // CLOSE DOOR
    // ======================================
    myServo.write(0);

    delay(1000);

    // SERVO OFF
    myServo.detach();
```

```
  // WHITE LED OFF
  digitalWrite(WHITE_LED, LOW);

  lcd.clear();

  lcd.setCursor(0, 0);
  lcd.print("DOOR CLOSED");

  lcd.setCursor(0, 1);
  lcd.print("Scan Again");

  delay(2000);
}

// ======================================
// ACCESS DENIED
// ======================================
else {

  Serial.println("ACCESS DENIED");

  lcd.clear();

  lcd.setCursor(0, 0);
  lcd.print("ACCESS DENIED");

  lcd.setCursor(0, 1);
  lcd.print("DOOR LOCKED");
```

```
// ======================================
// LED CONTROL
// ======================================
digitalWrite(RED_LED, HIGH);   // RED ON
digitalWrite(WHITE_LED, LOW);  // WHITE OFF

// KEEP DOOR CLOSED
myServo.attach(SERVO_PIN);

myServo.write(0);

delay(500);

myServo.detach();

// ======================================
// BUZZER ALARM
// ======================================
for (int i = 0; i < 5; i++) {

  tone(BUZZER_PIN, 700);
  delay(200);

  tone(BUZZER_PIN, 1000);
  delay(200);
}

noTone(BUZZER_PIN);
```

```
  delay(2000);

  // ======================================
  // COUNTDOWN TIMER
  // ======================================
  for (int sec = 10; sec >= 1; sec--) {

    lcd.clear();

    lcd.setCursor(0, 0);
    lcd.print("TRY AGAIN IN");

    lcd.setCursor(0, 1);

    lcd.print(sec);
    lcd.print(" Seconds");

    delay(1000);
  }

  // RED LED OFF
  digitalWrite(RED_LED, LOW);
}

// ======================================
// RESET LCD
// ======================================
lcd.clear();
```

```
  lcd.setCursor(0, 0);
  lcd.print(" RFID DOOR ");

  lcd.setCursor(0, 1);
  lcd.print("Scan Card");

  // STOP RFID
  rfid.PICC_HaltA();
}
```

7. Detailed Working Process

7.1 Authorized Entry

1. The resident taps an RFID card or key fob on the reader.
2. The MFRC522 reads the credential and sends the identifier to the ESP32.
3. The controller checks the credential against the authorized-user database.
4. If valid, the relay activates the electric strike or motorized lock.
5. The door opens, the reed switch confirms the door state, and the system logs the event.
6. Entry lighting turns on automatically for a predefined period.
7. The indoor security alarm is disarmed if the user is authorized.
8. The mobile app displays “Access granted” and identifies the user.cdn.aui+2

7.2 Unauthorized Entry Attempt

SAMP PROJECT MANAGEMENT

1. An unknown RFID card is presented.
2. The reader sends the tag ID to the controller.
3. The controller identifies it as unauthorized.
4. The buzzer sounds and the red LED turns on.
5. The event is stored with timestamp and tag identifier.
6. If multiple failed attempts occur, the system enters lockout mode and sends an intrusion alert.
7. If the door is forced open without valid authentication, the reed switch and vibration sensor trigger a high-priority alarm.repository.najah+1

7.3 Fire or Gas Emergency

1. The gas sensor detects a dangerous concentration of combustible gas, or the flame sensor detects fire.
2. The controller activates the buzzer/siren immediately.
3. The system sends an emergency notification to the owner and selected contacts.
4. The exhaust fan may turn on automatically in a gas-leak scenario.
5. The system can unlock designated emergency-exit doors, subject to fire-safety design requirements.
6. All events are logged for later review.github+2

7.4 Automation Scenario

When an authorized user enters the home:

- Entry light switches on

- Security alarm disarms
- Fan or air conditioner may switch on based on temperature
- Geyser, television, or other appliances can activate through predefined scenes
- Door automatically relocks after a defined delay
- The system records energy-use and access data

When the last authorized user leaves:

- Lights and non-essential appliances switch off
- Security system arms automatically
- Door locks after confirmation
- The owner receives a “home secured” notification

8. Circuit Design

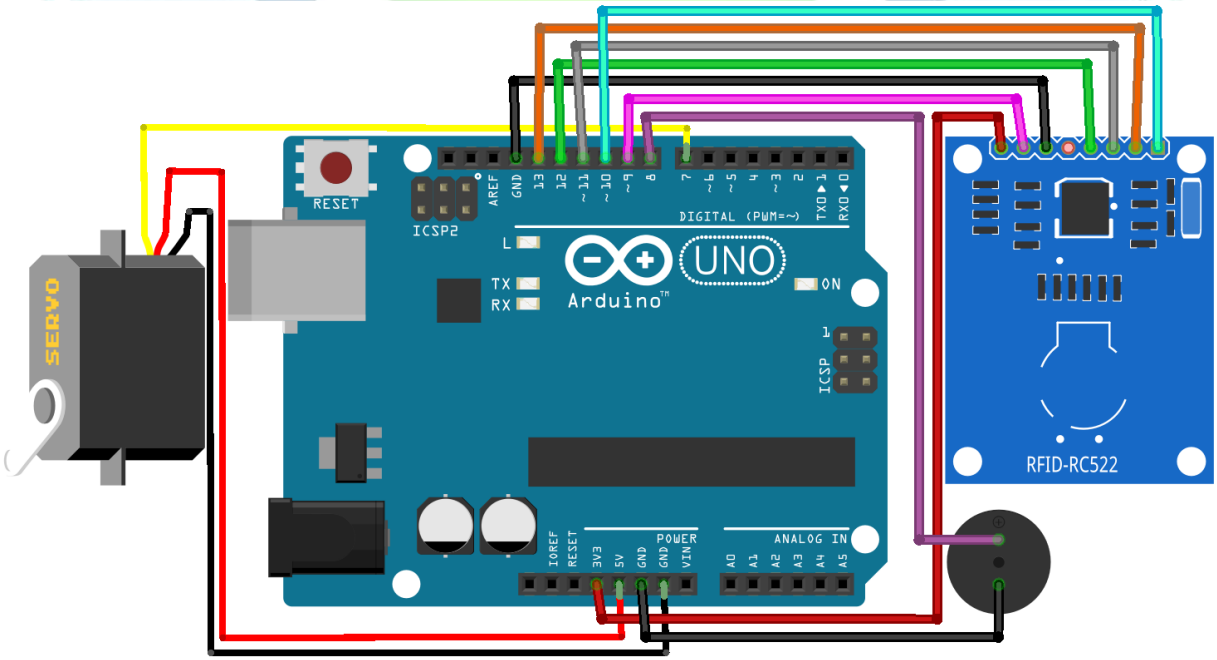


Fig:13

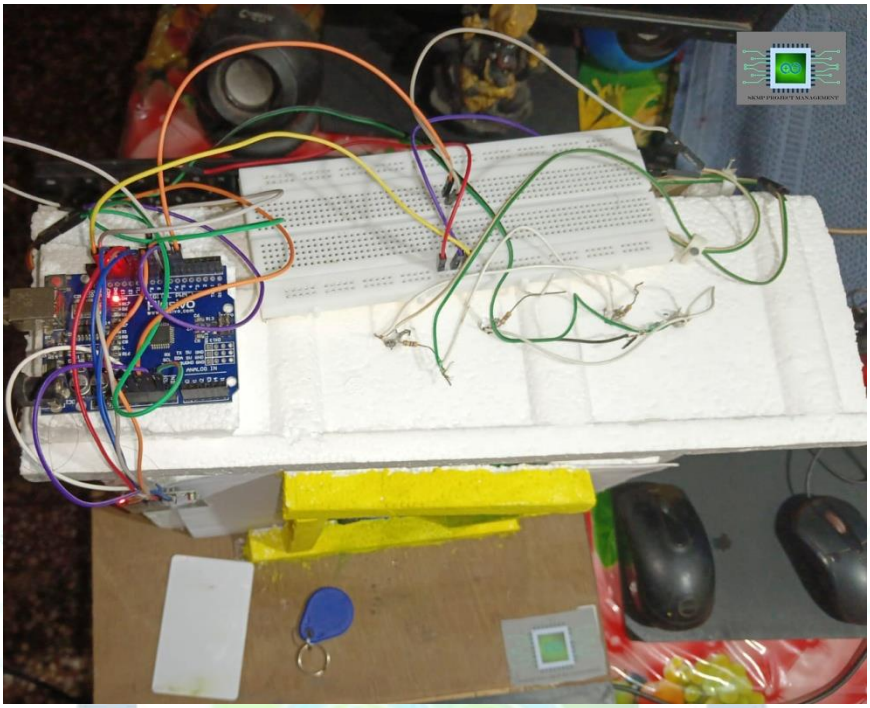


Fig:14

8.1 RFID Reader to ESP32 Connection

The MFRC522 commonly uses SPI communication. A typical ESP32 connection is:

SKMP PROJECT MANAGEMENT

MFRC522 Pin	ESP32 Pin
SDA/SS	GPIO 21
SCK	GPIO 18
MOSI	GPIO 23
MISO	GPIO 19
RST	GPIO 22

MFRC522 Pin	ESP32 Pin
GND	GND
VCC	3.3 V

The RC522 must be powered at 3.3 V; connecting it directly to 5 V can damage the module. The SPI pins may vary depending on the ESP32 board and software library used.cdn.aui+1

8.3 Sensor Connections

Sensor	Connection type	Controller input
PIR motion sensor	Digital output	GPIO input
Reed switch	Digital input with pull-up/pull-down resistor	GPIO input
Gas sensor	Analog output	ADC input
Flame sensor	Digital/analog output	GPIO or ADC input
DHT11/DHT22	Single-wire digital protocol	GPIO data pin
Buzzer	Digital output through transistor/driver	GPIO output
Relay module	Digital output	GPIO output

SKMP PROJECT MANAGEMENT

9. Security Design

9.1 RFID Security Risks

Basic RFID systems that rely only on a readable UID can be vulnerable to tag cloning, replay attacks, and unauthorized reading. Therefore, UID-only authentication should not be treated as high-security authentication.mikroe+1

Major risks include:

- Cloning of low-security RFID cards
- Replay of captured credential data
- Unauthorized reading of card data
- Compromise of Wi-Fi credentials or cloud account
- Physical tampering with the lock or controller
- Relay attacks in certain contactless systems
- Loss or theft of RFID cards or smartphones
- Power failure affecting electronic locks

9.2 Security Controls

Risk	Recommended control
Tag cloning	Use MIFARE DESFire EV2/EV3 with AES-128 mutual authentication
Replay attack	Use challenge-response authentication, timestamps, and session keys
Unauthorized reading	Limit read range, shield reader electronics, and avoid storing sensitive data in plaintext
Cloud compromise	Use HTTPS/TLS, strong passwords, MFA, role-based

SKMP PROJECT MANAGEMENT

Risk	Recommended control
	access, and encrypted storage
Physical tampering	Use tamper switches, secure enclosures, anti-pry hardware, and tamper alerts
Lost card	Provide instant card revocation through the admin app
Power failure	Use battery backup and mechanical override where appropriate
Internet failure	Keep local authentication and event logging functional
Unauthorized remote unlock	Require app login, device binding, OTP/2FA, and audit logging

Modern secure access-control designs should use 13.56 MHz credentials with cryptographic mutual authentication, and OSDP v2 with Secure Channel where a separate access-control panel is used.mikroe+1

9.3 Privacy and Data Protection

The system should collect only necessary data, including user identity, access time, door location, and security events. Access logs should be encrypted at rest and in transit, retained only for a defined period, and accessible only to authorized administrators.

SIWP PROJECT MANAGEMENT

Users should be informed about:

- What data is collected
- Why it is collected
- How long it is stored
- Who can access it
- How to request deletion or correction
- How alerts and location-related data are handled

10. Testing Plan

10.1 Functional Testing

Test case	Expected result
Valid RFID card is tapped	Door unlocks, green LED turns on, success log is created
Invalid RFID card is tapped	Door remains locked, buzzer sounds, denial log is created
Expired guest card is tapped	Access denied and expiry event logged
Admin adds a new user	New RFID credential becomes active
Admin removes a user	Removed card is immediately denied
Door is opened without authorization	Tamper/intrusion alert is generated
PIR detects motion in armed mode	Alarm activates and notification is sent
Gas leakage is detected	Alarm, fan activation, and emergency notification occur
Internet fails	Local access control continues working
Power fails	Battery backup maintains essential security functions
Mobile app sends unlock command	Door unlocks only after authenticated admin action

10.2 Security Testing

- Attempt RFID cloning and verify rejection of unauthorized cloned credentials

SKMP PROJECT MANAGEMENT

- Test replay attacks using captured authentication data
- Test Wi-Fi encryption, certificate validation, and secure API access
- Test brute-force protection on PIN and app login
- Verify lockout after repeated failed attempts
- Test tamper-switch response
- Verify secure remote-unlock authentication
- Test data encryption in local storage and cloud transmission
- Conduct penetration testing before public deployment

10.3 Reliability Testing

- Continuous 72-hour operation test
- RFID read-range consistency test
- Relay and lock endurance test
- Sensor false-alarm test
- Wi-Fi reconnection test
- Battery-backup duration test
- Temperature and humidity endurance test
- Real-door installation test

SKMP PROJECT MANAGEMENT

11. Market Analysis

11.1 Market Opportunity

Security and access control are major entry points for smart-home adoption because cameras, doorbells, and smart locks provide immediate, visible value and can be installed without automating the entire home.

India's access-control market is projected to grow strongly, with card-based systems leading the market. This supports the commercial relevance of RFID-enabled residential and small-business security products.

11.2 Target Customers

Customer segment	Main need	Product positioning
Urban households	Convenient keyless entry and safety	Affordable smart lock with RFID and app control
Rental-property owners	Tenant access management	Temporary credentials and access logs
Hostels and PG accommodations	Controlled room access	Multi-user RFID access system
Small offices	Employee entry management	RFID attendance and door access
Shops and warehouses	Theft prevention and monitoring	Alarm, access control, and sensor integration
Gated communities	Visitor and resident management	RFID gate and door access
Senior-care facilities	Safe entry and	Caregiver access and

SKMP PROJECT MANAGEMENT

Customer segment	Main need	Product positioning
	emergency alerts	emergency notifications

11.3 Competitive Advantage

The proposed system can differentiate itself through:

- Local offline access control during internet outages
- Affordable RFID cards and fobs for all family members
- Temporary access for guests, tenants, and service staff
- Integrated fire, gas, motion, and tamper safety features
- Detailed access logs and alerts
- Modular design for homes, hostels, offices, and shops
- Support for Indian power conditions and battery backup
- Lower cost than fully imported premium smart-lock ecosystems

12. Advantages

- Eliminates dependence on physical keys
- Allows instant addition or removal of user access
- Supports temporary and scheduled access
- Maintains a complete entry/exit history
- Sends real-time security and emergency alerts
- Automates lighting and appliances
- Improves safety through fire, gas, motion, and tamper detection
- Works locally even when internet connectivity is unavailable
- Can be expanded to multiple doors and rooms
- Reduces unauthorized entry and improves accountability
- Provides a strong foundation for future AI-based security analytics

SKMP PROJECT MANAGEMENT

13. Limitations

- RFID cards can be lost, stolen, or shared with unauthorized persons
- Basic RFID UID systems are not sufficient for high-security applications
- Electronic locks require reliable power and backup arrangements
- Wi-Fi-dependent features may fail during internet outages
- Sensors can generate false alarms due to pets, insects, steam, or environmental interference
- Installation may require door modification and professional wiring
- Cloud services require ongoing maintenance, security updates, and data-protection compliance
- RFID alone should not replace certified mechanical locks in high-risk premises

SKMP PROJECT MANAGEMENT

CONCLUSION

The **RFID Smart Home Security & Automation System with Smart Lock** is a practical, scalable, and commercially relevant solution for modern residential and small-commercial security. It combines RFID access control, electronic locking, intrusion detection, environmental safety, automation, and mobile monitoring into a unified platform.mikroe+2

For a student prototype, an ESP32 with MFRC522, relay module, sensors, buzzer, and solenoid lock is sufficient. For a public-facing commercial product, the design should upgrade to encrypted MIFARE DESFire credentials, certified locking hardware, secure cloud architecture, tamper protection, battery backup, and rigorous security testing.mikroe+1

The project has strong potential in India because card-based access control already represents a major share of the access-control market, while smart-home adoption is increasingly driven by security and access-control products.

SKMP PROJECT MANAGEMENT

Future scope

The future scope of the **RFID Smart Home Security & Automation System** is to evolve from a basic RFID door-lock prototype into an intelligent, secure, interoperable home-security ecosystem. Future versions can combine RFID with biometrics, AI-based threat detection, edge processing, voice control, and cloud-managed access management.mordorintelligence+2

1. Biometric Authentication

The system can be upgraded with fingerprint, face recognition, iris recognition, and voice-based authentication. A multi-factor approach—such as RFID card plus fingerprint, or face recognition plus mobile confirmation—will provide stronger protection than RFID alone.securitysystemsnews+2

Future feature	Purpose
Fingerprint scanner	Adds a unique biometric credential for residents
Facial recognition camera	Enables touchless entry for authorized users
Voice recognition	Supports hands-free access and voice commands
Mobile biometric unlock	Uses smartphone fingerprint/Face ID before remote unlock
Multi-factor authentication	Combines RFID, PIN, biometric, and mobile approval

Biometric access control is expected to become increasingly mainstream, with fingerprint, facial, and voice recognition being integrated into more home-security products.securitysystemsnews+1

2. AI-Based Security Intelligence

SKMP PROJECT MANAGEMENT

Artificial intelligence can make the system proactive rather than only event-reactive. Machine-learning models can analyze access patterns, motion events, camera footage, and sensor data to distinguish normal household activity from suspicious behavior.brinkshome+2

Possible AI features include:

- Detection of unusual entry times or repeated failed RFID attempts
- Recognition of familiar residents and unknown visitors
- Differentiation between humans, pets, vehicles, and delivery activity
- Prediction of possible intrusion or tailgating attempts
- Automatic prioritization of critical alerts
- Reduction of false alarms through behavioral analytics
- Identification of abnormal appliance or energy usage patterns

AI-powered video analytics can identify routine deliveries versus suspicious loitering, while on-device processing can reduce cloud bandwidth use and improve privacy.researchandmarkets+1

3. Edge Computing and Offline Intelligence

Instead of sending all video, sensor, and access data to the cloud, the system can process critical events locally using an edge AI module. This improves response speed, reduces internet dependency, lowers data costs, and protects user privacy.researchandmarkets+2

SKMB PROJECT MANAGEMENT

Future edge functions may include:

- Local face recognition at the entrance
- On-device intrusion detection
- Local storage of access logs during internet failure
- Automatic alarm activation without cloud delay

- Secure synchronization with the cloud after connectivity is restored
- Privacy-preserving processing of camera footage within the home

4. Advanced Mobile and Cloud Platform

The mobile application can be expanded into a complete home-management platform. It can support remote door control, live camera viewing, user management, automation scheduling, emergency alerts, and detailed security analytics.kaisoresearch+2

Future app capabilities:

- Live video doorbell and two-way audio communication
- Remote lock/unlock with OTP or biometric approval
- Temporary digital keys for guests and service staff
- Family access calendar and permission scheduling
- AI-generated daily security reports
- Emergency SOS button with location sharing
- Multi-home and multi-door management
- Role-based admin dashboard for landlords and property managers

Cloud-managed access control is expected to expand beyond individual homes into rental properties, hostels, offices, hospitality, and managed facilities.researchandmarkets+1

SKMP PROJECT MANAGEMENT

5. Smart Home Ecosystem Integration

The system should support interoperability with major smart-home platforms and communication protocols. This will allow the RFID lock, cameras, lights, thermostats, alarms, and appliances to work together as one coordinated system.giiresearch+2

Potential integrations include:

- Amazon Alexa and Google Assistant voice control
- Apple HomeKit-compatible automation
- Matter-compatible smart devices
- Zigbee, Z-Wave, Wi-Fi, Bluetooth Low Energy, and Thread devices
- Smart lighting, fans, air conditioners, geysers, and plugs
- CCTV cameras and video doorbells
- Water-leak, smoke, gas, and fire-safety devices
- Solar inverters, energy meters, and battery systems

Interoperable systems that connect locks, lighting, HVAC, cameras, and voice assistants are a major direction for future smart-home security.globalsecuritymag+1

6. Energy Management and Sustainability

The system can use occupancy detection, access events, and environmental data to reduce electricity consumption. For example, lights and air conditioners can automatically switch off when the last resident leaves or when no motion is detected for a defined period.kaisoresearch+1

Future sustainability features:

- Solar-powered outdoor RFID gate reader
- Low-power sleep mode for battery-operated locks
- Energy-consumption dashboard for appliances
- Automatic load shedding during peak electricity hours
- Solar-battery monitoring and optimization
- Water-leak detection and automatic valve shutoff
- Eco-mode automation for vacant rooms

SMART PROJECT MANAGEMENT

Low-power wireless connectivity and energy-efficient smart-lock design are identified as important future development areas.researchandmarkets

7. Enhanced Safety and Emergency Response

The system can be connected to emergency services, family members, neighbors, security guards, and building management systems. During fire, gas leakage, medical emergency, or intrusion, it can automatically trigger the appropriate response.brinkshome+2

Future emergency features:

- Automatic call or SMS to emergency contacts
- Integration with local police, fire, and ambulance services
- Panic button for senior citizens and children
- Fall-detection sensors for elderly residents
- Smoke, CO, gas, and water-leak detection
- Automatic unlocking of emergency-exit routes during fire events
- Emergency lighting and evacuation guidance
- Location-based alerts for multiple family members

8. Advanced Access Management

Future versions can support more flexible and secure access policies for families, tenants, employees, and visitors. This is especially useful for rental homes, hostels, PG accommodations, offices, and shared properties.researchandmarkets+1

Feature	Benefit
Time-based access	Allows entry only during approved hours
Location-based access	Restricts access to selected doors or zones

Feature	Benefit
One-time digital key	Useful for deliveries and temporary visitors
QR-code visitor pass	Enables secure guest entry without physical cards
Anti-passback system	Prevents the same credential being used twice improperly
Tailgating detection	Identifies unauthorized entry following an authorized user
Access-score analysis	Flags abnormal user behavior
Centralized multi-site control	Manages several homes, rooms, or buildings from one dashboard

9. Stronger Cybersecurity

As the system becomes more connected, cybersecurity must become a core design requirement. Future development should include encrypted communication, secure credential storage, authenticated firmware updates, tamper detection, and resilient fallback access.giiresearch+1

Recommended future security upgrades:

- End-to-end encryption for cloud and mobile communication
- Secure Element or TPM-based key storage
- Certificate-based device identity
- Signed and encrypted OTA firmware updates
- Two-factor authentication for administrator accounts
- Anomaly detection for suspicious API or app activity
- Regular vulnerability scanning and penetration testing
- GDPR-style privacy controls and transparent data policies
- Mechanical key override for emergency fallback access

SRMP PROJECT MANAGEMENT

10. Commercial Expansion

The project can be developed into a commercial product line for different customer segments. Smart locks, RFID access control, video doorbells, connected cameras, and AI-based monitoring are expected to remain major drivers of smart-home security growth.kaisoresearch+2

Possible product versions:

Product version	Target market	Key features
Basic RFID Smart Lock	Budget homes and hostels	RFID, PIN, buzzer, local logs
Premium Smart Lock	Urban households	RFID, fingerprint, mobile app, camera
Rental Access System	Landlords and PG owners	Temporary keys, tenant logs, remote control
Office Access System	Small businesses	Employee RFID, attendance, admin dashboard
Society Gate System	Gated communities	Vehicle tags, visitor management, guard panel

SKMP PROJECT MANAGEMENT

Product version	Target market	Key features
Product version	Target market	Key features
Industrial Access System	Warehouses and factories	Multi-door control, shift-based access, safety alerts
AI Security Hub	Premium smart homes	AI camera, biometric lock, automation, cloud analytics

11. Long-Term Vision

The long-term vision is to create a **self-learning, privacy-respecting, and resilient smart-security ecosystem**. Such a system would recognize residents, understand daily routines, detect abnormal activity, automate home functions, prevent unauthorized access, and respond intelligently during emergencies.brinkshome+2

However, AI-based access decisions should include human oversight, clear privacy controls, secure data handling, and reliable fallback authentication. AI should support—not replace—strong authentication, physical safeguards, and emergency procedures.

SKMP PROJECT MANAGEMENT

REFERENCES

1. Mikroe. (2026). *RFID Readers for Access Control Systems (2026)*. Available at: https://www.mikroe.com/blog/rfid-reader-access-controlmikroe
2. Ambient.ai. (2026). *RFID Access Control Systems: How They Work & When to Use Them*. Available at: https://www.ambient.ai/learn/rfid-access-controlambient
3. Chalmers University of Technology. *Security in Access Control Systems Using RFID*. Master's thesis. Available at: https://odr.chalmers.se/server/api/core/bitstreams/8dc11bef-e52c-4d56-9802-28427b647311/contentscribd
4. Al Akhawayn University. (2023). *Smart Home Security System*, Capstone Project Report. Available at: https://cdn.aui.ma/sse-capstone-repository/pdf/spring-2023/SMART%20HOME%20SECURITY%20SYSTEM.pdf
5. IoT Smart Home ESP32. (2026). *Complete ESP32 Smart Home Project: Components and Implementation*. GitHub Repository. Available at: https://github.com/panchacharam/IoT-Smart-Home-ESP32
6. Smart Home Report. (2026). *RFID-Based Smart Home Automation and Security System Using ESP32*. Scribd. Available at: https://www.scribd.com/document/971639222/Smart-Home-Report
7. Project Report: IoT Prem. (2026). *RFID Door Lock and Smart Home Security System Using Arduino and RC522*. Scribd. Available at: https://www.scribd.com/document/961341924/Project-Report-iot-prem
8. India Smart Home Market Share, Companies & Trends Report 2026–2032. (2026). *Ken Research*. Available at: https://www.kenresearch.com/industry-reports/india-smart-homes-market

9. IMARC Group. (2026). *Indian Access Control Market Size, Share, Trends and Forecast by Component, Type, End User, and Region, 2026–2034*. Available at: https://pdf.marketpublishers.com/imarc/indian-access-control-market-report-by-component-controller-reader-locks-software-type-card-based-biometric-based-end-user-government-commercial.pdf
10. California State University, Northridge. *Smart Home Security and Automation System Using RFID, Sensors, and Microcontrollers*. ScholarWorks. Available at: https://scholarworks.calstate.edu/downloads/pn89d973h
11. An-Najah National University. *Smart Home Security System Using RFID, Reed Switch, Motion Sensor, and Alarm*. Institutional Repository. Available at: https://repository.najah.edu/server/api/core/bitstreams/560d9997-966a-48f8-a8d2-3b1b0a2a0a0a/contentodr.chalmers
12. Final Report, Prakash. (2025). *IoT-Based Smart Home Automation and Security System*. Scribd. Available at: https://www.scribd.com/document/857440963/Final-report-Prakash-EC23I2013
13. RFID Attendance System. (2015). *MFRC-522 RFID Reader Module and RFID Tags*. SlideShare. Available at: https://es.slideshare.net/slideshow/rfid-attendance-system-48338237/48338237
14. Smart Home Automation Prototype Design. (2026). *Design and Realization of a Prototype Using MIFARE RC522 Module*. Scribd. Available at: https://www.scribd.com/document/971740518/Design-and-realization-of-a-prototype-pdf
15. Arduino Documentation. *MFRC522 RFID Library and RC522 Module Interfacing*. Available at: https://docs.arduino.cc/ [General technical reference]

16. Espressif Systems. *ESP32 Technical Reference Manual and Wi-Fi/Bluetooth Development Documentation*. Available at: https://www.espressif.com/en/support/documents/technical-documents [General technical reference]
17. NXP Semiconductors. *MFRC522 Contactless Reader IC Data Sheet*. Available at: https://www.nxp.com/ [General technical reference]
18. NXP Semiconductors. *MIFARE DESFire EV2/EV3 Contactless IC Product Documentation*. Available at: https://www.nxp.com/ [General technical reference]
19. International Organization for Standardization. *ISO/IEC 14443: Identification Cards — Contactless Integrated Circuit Cards — Proximity Cards*. Available at: https://www.iso.org/ [General standards reference]
20. International Organization for Standardization. *ISO/IEC 15693: Identification Cards — Contactless Integrated Circuit Cards — Vicinity Cards*. Available at: https://www.iso.org/ [General standards reference]

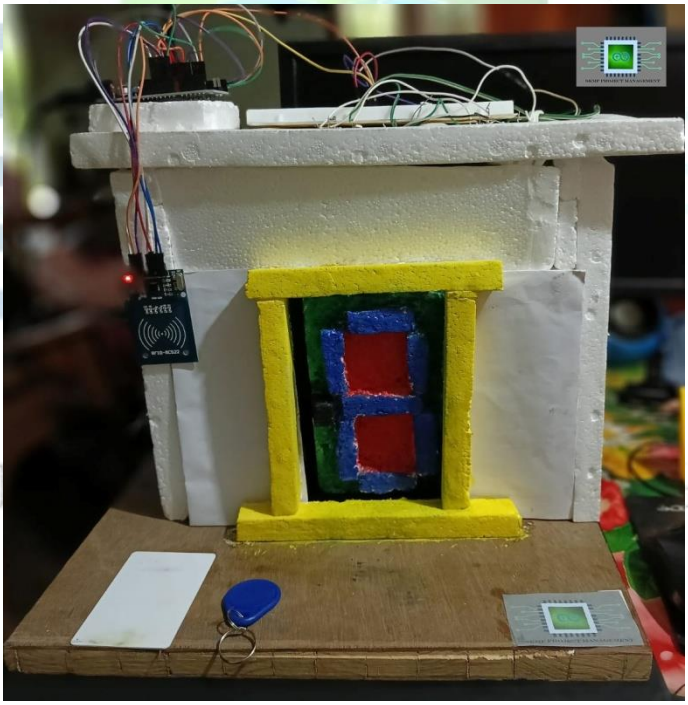
SKMP PROJECT MANAGEMENT

PROJECT LINK

Website lnk:-https://skmp-project-management.vercel.app/

Google Drive Link:-
https://drive.google.com/drive/folders/1OeDMJDswF44xzNG61_4TLy9eypoeNHJ4?usp=sharing

VideoLink:- https://youtu.be/s_0UQm30jz0?si=QIJ0tqWgkSwgop4O





SKMP PROJECT MANAGEMENT

SKMP PROJECT MANAGEMENT

==========

SKMPPROJECTMANAGEMENT

DEPARTMENT OF IOT