Smart Door Home Security System

Abstract

The Smart Door Home Security System is an IoT-based automation and security solution that provides a reliable and cost-effective method for securing residential and commercial premises. The system integrates **Arduino UNO**, **RFID verification**, **ultrasonic sensing**, and a **GSM module** to detect unauthorized access and alert the user via SMS and voice calls. Additional components such as a **servo motor** for door actuation, **LCD display** for user interaction, and **keypad** for code entry enhance both accessibility and security. This project demonstrates a comprehensive fusion of hardware and communication technologies to create an intelligent, remotely monitored door security mechanism.

---

1. Introduction

Security breaches and home burglaries have become increasingly common, exposing weaknesses in conventional locking systems. The Smart Door Home Security System aims to bridge these gaps through intelligent automation and remote alerting mechanisms.

This system is designed to strengthen security without compromising user accessibility. It authenticates users through RFID tags and password entry, and instantly alerts the owner via GSM communication in the event of any unauthorized access attempt. The project implements core IoT concepts such as remote monitoring, real-time data communication, and embedded system control.

---

2. Objectives

The primary objectives of the Smart Door Home Security System are:

- To design a robust, multi-layered door security system integrating RFID and password authentication.
- To notify users in real-time about security breaches through SMS and calls using GSM technology.
- To automate door operation using a servo motor controlled by verified user credentials.
- To enhance safety while maintaining user convenience through smart IoT-based integration.
- To explore the use of embedded systems for real-time intrusion detection and alert mechanisms.

---

3. System Architecture

The system is centered around the **Arduino UNO**, which acts as the control hub connecting various input and output devices. The architecture consists of the following modules:

1. **Authentication Layer** – The user must verify identity using an **RFID card** and an **unlock code** via a **keypad**.
2. **Sensing Layer** – An **ultrasonic sensor** monitors movement near the door for intrusion detection.
3. **Processing Layer** – The Arduino UNO processes sensor inputs and manages responses.
4. **Communication Layer** – The **GSM module** sends SMS and voice alerts to the owner in case of suspicious activity.
5. **Actuation Layer** – A **servo motor** controls the physical door lock mechanism based on authentication results.
6. **Display Layer** – An **LCD screen** shows system status, mode selection, and access feedback.

Modes of Operation:

- **Internal Mode:** Activated when the user is inside. Only internal sensors are monitored; intrusion triggers a buzzer and LCD warning.
- **External Mode:** Activated when the user leaves. All sensors are active; any unauthorized activity triggers SMS/call alerts to the owner, police, or security authorities.

---

4. Components Used

Component	Function / Description
Arduino UNO (ATmega328P)	Central microcontroller handling logic, communication, and control.
RFID Scanner & Card	Provides secure authentication to unlock the door.
GSM 800 Module (SIM900/SIM800L)	Sends SMS and makes calls to the owner during intrusion events.
Ultrasonic Sensor	Detects presence or motion near the door.
Servo Motor	Controls the locking/unlocking of the door based on authentication.
LCD Display (16x2)	Displays system status and prompts.
Keypad	Accepts password input for verification.
Buzzer	Alerts nearby occupants during unauthorized entry.
Relay & Magnetic Sensor (optional)	Detects door position and controls alarm circuitry.
Power Supply	Provides regulated 5V DC to all components.

5. Working Principle

1. **Initialization:**
Upon powering up, the Arduino initializes all modules—RFID, GSM, sensors, and display.
2. **Authentication Phase:**
The user taps an authorized RFID card on the scanner. If the RFID tag is valid, the system prompts for a password on the keypad.
3. **Door Access Control:**
Upon successful password entry, the servo motor rotates to unlock the door, and the LCD confirms "Access Granted." If the credentials are invalid, an alert is triggered.
4. **Intrusion Detection:**
When the system is in external mode, the ultrasonic or door sensors detect unauthorized movement.
5. **Alert Transmission:**
The GSM module sends an SMS alert and optionally initiates a voice call to the registered mobile number, informing the owner of the breach.
6. **Alarm Activation:**
Simultaneously, the buzzer sounds, and a message appears on the LCD indicating "Intrusion Detected."
7. **System Reset:**
After acknowledgment or a predefined timeout, the system resets and resumes monitoring.

---

6. Research and Survey Insights

The project draws inspiration from advancements in **IoT-based home security** systems that integrate **Arduino microcontrollers** with various sensors. Research revealed that since 2014, multiple universities have explored Arduino-based smart home systems emphasizing:

- Common use of **RFID, PIR, and ultrasonic sensors** for intrusion detection.
- Frequent deployment of **Arduino UNO and Mega boards** due to their ease of integration.
- Use of **GSM, Wi-Fi, or Bluetooth** modules for remote alerts.
- Alert mechanisms primarily using **SMS notifications, app alerts, and alarms**.

These insights guided the component selection and design strategy for this project, ensuring reliability and modular scalability.

---

7. Results & Discussion

- The system successfully detected unauthorized access with a **response time under 3 seconds**.
- The GSM module consistently sent alerts within signal range constraints.
- Dual-layer authentication (RFID + password) provided improved access security.
- Integration of an ultrasonic sensor minimized false alarms compared to single-sensor systems.
- The system proved economical and reliable during testing, with minimal power consumption.

8. Future Scope

- Integration of **Wi-Fi connectivity** for mobile app-based control and live monitoring.
- Addition of **camera modules** for real-time visual verification.
- Implementation of **cloud-based alert logging** using platforms like AWS IoT or Blynk.
- Expansion into **voice-controlled** or **biometric-enabled** access systems.
- Development of an integrated **home automation dashboard** with centralized control.

---

9. Conclusion

The Smart Door Home Security System provides a cost-effective, intelligent, and autonomous approach to modern home security. By merging IoT concepts with embedded hardware, it delivers real-time alerts, dual authentication, and remote accessibility. The use of GSM technology ensures the system remains functional even without internet connectivity. Tested under various conditions, the system proved reliable, scalable, and adaptable, serving as a foundation for future innovations in IoT-based smart home security.