UTTARA UNIVERSITY

Department of Electrical & Electronics Engineering

Project On

‘‘GSM BASED DOOR SECURITY SYSTEM’’

In Partial fulfilled requirements for the B.Sc Degree of Electrical & Electronics Engineering

Author’s Name	ID
POLLOB KUMAR BISWAS	2221171001
MD.MAHAMUD HASAN	2221171027
MOST.SHAGORIKA BEGUM	2221171024
BOBYRUN NAHAR JIM	2221171023

This book is for the partial fulfilment of B.Sc in Electrical and Electronic Engineering from Uttara University

Date of Submission: February- 2025

DECLARATION

I hereby declare that this project, titled **"GSM Based Door Security System,"** is the result of my original work conducted independently in the laboratories of the Department of Electrical and Electronic Engineering at **Uttara University**.

This project is submitted in partial fulfillment of the requirements for the degree of **Bachelor of Science in Electrical and Electronic Engineering**. It has not been submitted, either wholly or in part, for any other academic award, diploma, or qualification at this or any other institution. I affirm that the project work was carried out with due diligence, adhering to the highest standards of academic integrity. I have ensured that all relevant ethical and safety guidelines were followed during the course of this research. I take full responsibility for the content, originality, and reliability of the information and findings presented in this document.

Signature of the Supervisor

Subah Karnine

lecturer

Department of Electrical and ElectronicEngineering

Uttara University

Signature of the Author's

Name	ID	Signature
POLLOB KUMAR BISWAS	2221171001	
MD.MAHAMUD HASAN	2221171027	
MOST.SHAGORIKA BEGUM	2221171024	
BOBYRUN NAHAR JIM	2221171023	

APPROVAL

The project entitled **"GSM Based Door Security System"** submitted by POLLOB KUMAR BISWAS ID: 2221171001**,** MD.MAHAMUD HASAN ID: 2221171027**,** MOST.SHAGORIKA BEGUM ID: 2221171024, BOBYRUN NAHAR JIM ID: 2221171023 has been done under my supervision and accepted as adequate in partial fulfillment of the requirements for the degree of **Bachelor of Science in Electrical and Electronic Engineering** in **February, 2025**

_____

Subah Karnine

Lecturer

Department of Electrical and Electronic Engineering
Uttara University

ACKNOWLEDGEMENT

First and foremost, we express our heartfelt gratitude to **Almighty Allah** for His guidance and blessings throughout the completion of our final-year project.

We are deeply thankful to **Subah Karnine**, Lecturer in the Department of Electrical and Electronic Engineering at **Uttara University**, for his invaluable support, mentorship, and encouragement. His profound knowledge and dedication to the field of **"GSM Based Door Security System"** greatly enriched our work. His constructive feedback and unwavering guidance were instrumental in the successful execution of this project. We also extend our sincere gratitude to our classmates for their collaborative spirit, thought-provoking discussions, and shared enthusiasm, which significantly contributed to our learning and the development of this project. Finally, we would like to thank our parents for their unwavering support, encouragement, and belief in us throughout our academic journey. Their love and motivation have been our greatest strength.

On behalf of

Mahamud Hasan

ID: 2221171027

ABSTRACT

The" GSM Based Door Security System" is an innovative solution designed to enhance access control and security for residential, commercial, and industrial applications. This project integrates modern GSM communication technology with a microcontroller-based system to provide efficient and remote management of door access. The system employs an Arduino Nano as the central processing unit, paired with a SIM800L GSM module for communication. An IR sensor detects the presence of individuals near the door, triggering the system to initiate an authentication process. System status, prompts, and alerts are displayed on a 16x2 Liquid Crystal Display (LCD), providing an intuitive interface for users. In case of unauthorized access or a security breach, the GSM module sends real-time alerts to a predefined phone number via SMS. A Li-Ion battery with a booster module and a charging circuit ensures uninterrupted power supply, while a 5-volt adapter provides external power for consistent operation. This integration of hardware components ensures reliability and efficiency in various scenarios. The "GSM-Based Door Security System" offers several advantages, including enhanced security, real-time monitoring, and remote control capabilities, making it suitable for diverse environments. The project demonstrates the potential of combining GSM technology with microcontroller-based systems to develop cost-effective and scalable security solutions.

Table of Content's

CHAPTER ONE
INTRODUCTION

1.1 Introduction

In today's fast-evolving world, security has become a paramount concern in both residential and commercial spaces. Conventional door security systems, while effective, often lack the ability to provide real-time monitoring and control, especially in cases of unauthorized access. To address this limitation, advancements in technology have enabled the development of innovative solutions that combine hardware components with wireless communication systems, ensuring enhanced security and convenience. The **GSM Based Door Security System** is one such solution designed to offer robust access control with remote monitoring capabilities.

The system employs **Global System for Mobile Communication (GSM)** technology to deliver real-time alerts and control over door access. By integrating a GSM module, the system enables users to receive notifications and manage the door remotely through text messages. This feature not only enhances security but also provides flexibility, allowing the user to monitor their property from any location. Additionally, the use of microcontroller-based control ensures reliability and scalability for various applications. Key components such as the Arduino Nano**,** SIM800L GSM module, and IR sensor work cohesively to detect movement near the door and authenticate access attempts. Unauthorized access triggers alerts sent via the GSM module, while the system status and authentication prompts are displayed on an LCD interface for ease of use. Power stability is ensured through the incorporation of a Li-Ion battery**,** booster module, and charging circuit, making the system reliable even during power outages. This project bridges the gap between traditional lock-and-key mechanisms and modern wireless technologies. By leveraging GSM communication and sensor-based detection, it provides a cost-effective, scalable, and efficient solution to ensure the safety of properties. Such systems are particularly suited for environments where enhanced access control is critical, such as homes, offices, warehouses, and other restricted areas.

The **GSM Based Door Security System** represents a significant step towards the automation of security processes, combining simplicity with advanced features. This project aims to demonstrate how GSM communication, in conjunction with compact and low-power hardware components, can redefine the way door security is perceived and implemented.

1.2 Problem Statement

Traditional door security systems, such as mechanical locks and keys, often fail to provide adequate protection against unauthorized access or break-ins. These systems lack the ability to alert property owners in real-time about security breaches, leaving homes and businesses vulnerable to intrusions. Additionally, they offer no mechanism for remote monitoring or control, which limits their effectiveness in situations where immediate action is required. Moreover, modern lifestyles demand solutions that are not only secure but also convenient and adaptable to various scenarios. The absence of a cost-effective and scalable system that integrates advanced technology with user-friendly operation creates a gap in the security market. Many existing solutions are either too expensive, complex to install, or depend heavily on constant power supply, which limits their applicability in power-sensitive environments. To address these issues, the need arises for a smart, affordable, and reliable door security system that incorporates real-time communication and remote control capabilities. The '**GSM Based Door Security System'** aims to solve this problem by providing an efficient and accessible solution that enhances security through GSM communication, sensor technology, and microcontroller-based automation. This project focuses on bridging the limitations of conventional security systems by enabling real-time alerts, remote management, and reliable performance, ensuring the safety and convenience of users in a variety of settings.

1.3 Background of the Study

Security concerns have always been a priority for individuals and organizations alike. In Bangladesh, the rapid urbanization and population growth over the last few decades have led to significant changes in living standards and infrastructure. Alongside these developments, the need for enhanced security solutions has become increasingly evident. Traditional security measures, such as mechanical locks and manual surveillance, are often inadequate in preventing unauthorized access or addressing modern security challenges.

In recent years, Bangladesh has experienced a surge in property crimes, including theft and burglary, particularly in urban areas such as Dhaka, Chattogram, and Sylhet. These incidents highlight the limitations of conventional security systems in safeguarding homes, offices, and businesses. Moreover, the growing adoption of modern living spaces, gated communities, and high-rise apartments has created a demand for advanced security technologies that can provide both convenience and reliability. The rise of mobile communication and digital technologies has opened new avenues for enhancing security measures. Bangladesh, with its rapidly expanding mobile network and high penetration of GSM-enabled devices, offers a fertile ground for

integrating mobile communication into security systems. GSM (Global System for Mobile Communication) technology, widely used in mobile phones, has emerged as a practical solution for real-time communication and remote monitoring, enabling users to receive alerts and control systems from anywhere. With the increasing affordability and accessibility of microcontroller-based systems such as the Arduino Nano, along with sensors and GSM modules, it has become feasible to design cost-effective and scalable solutions tailored to the needs of Bangladeshi households and businesses. The inclusion of components such as IR sensors for motion detection, LCD displays interfaces for user interaction, and backup power solutions like Li-Ion batteries ensures reliability and ease of use, even in areas prone to power outages. The "GSM Based Door Security System" builds on these advancements to address security challenges specific to Bangladesh. This system is designed to provide real-time alerts via SMS and enable users to remotely monitor and control door access. The ability to detect unauthorized access and notify users instantly makes it particularly effective in combating the rising threat of property crimes. Furthermore, the project offers a practical alternative to expensive commercial security systems, making it accessible to a wider audience, including middle-income households and small businesses.

Historically, Bangladesh has faced challenges in adopting high-tech solutions due to economic constraints and a lack of technological awareness. However, recent government initiatives to promote digitalization under the "Digital Bangladesh" campaign have significantly boosted the adoption of smart technologies. Projects like this not only align with the country's vision of technological progress but also contribute to enhancing safety and improving the quality of life for its citizens. By combining modern technology with practical design, the GSM Based Door Security System aims to redefine security standards in Bangladesh. This system addresses local challenges such as frequent power outages, affordability concerns, and the need for reliable communication, ensuring that it is both effective and adaptable to the unique needs of the country. Through this project, we aim to contribute to the broader efforts of ensuring safety and security in Bangladesh, empowering individuals and businesses to adopt smarter, more secure living and working environments.

1.4 Objective

The **"GSM Based Door Security System"** project is designed with specific goals to address the challenges of modern security needs in residential, commercial, and industrial environments. The primary objectives of this project are as follows:

- **Enhance Security:** Improve safety by integrating a GSM-based alert system that sends real-time notifications to users in case of unauthorized access attempts, helping to prevent

security breaches.

- **Enable Remote Monitoring:** Provide users with the ability to monitor and control door access from anywhere using SMS alerts and commands, ensuring continuous surveillance and easy control.
- **Instant Alerts for Unauthorized Access:** Incorporate a real-time alert mechanism that sends instant SMS notifications to users whenever the system detects an unauthorized access attempt, enhancing the response time to security breaches.
- **Affordable and Accessible Solution:** Offer a cost-effective security system that can be easily deployed by households, small businesses, and offices, making modern security technology accessible to a wide range of users.
- **User-Friendly Interface:** Use an LCD display to provide users with clear feedback and system status messages, making it easy to understand the system's status and authentication process.
- **Power Reliability:** Ensure the system operates without interruption by incorporating a Li-Ion battery**,** booster module, and charging circuit, providing backup power in case of power failures.
- **Adaptability to Local Needs:** Design a system tailored to the unique challenges of Bangladesh, such as frequent power outages and affordability, ensuring it meets local demands effectively.
- **Future Scalability:** Provide a flexible design that can be upgraded with additional features such as RFID or biometric authentication systems, allowing for easy expansion and customization of the security system as technology evolves.

1.5 Methodology

The GSM Based Door Security System is developed using a methodical approach that combines both hardware and software components to achieve a fully functional security solution. The project begins with the identification of the system's primary objectives, such as enabling remote monitoring via GSM, ensuring real-time alerts for unauthorized access, and providing a user-friendly interface for operation. Based on these requirements, the necessary components, including the Arduino Nano**,** SIM800L GSM module**,** IR sensor**,** LCD display, and Li-Ion battery, are selected to form the core of the system. The first step in the methodology involves the design of the hardware architecture, which includes wiring and connecting the components to the Arduino Nano. The IR sensor is used for motion detection near the door, while the GSM module facilitates communication between the system and the user by sending SMS notifications. The LCD displa**y**

is incorporated to provide feedback on the system's status, such as security prompts or alerts(SMS and GSM for alerts). The Li-Ion battery is connected to ensure the system operates efficiently even during power failures, with a booster module used to stabilize the voltage for reliable performance. The software development phase follows, where the Arduino Nano is programmed to control the interactions between the hardware components. The code is designed to detect and validate password entries sent via SMS. The system verifies whether the entered password is correct, granting or denying access to the door accordingly. In case of unauthorized attempts, the system triggers the GSM module to send real-time SMS alerts to the designated phone number, notifying the user of a potential security breach. The LCD provides visual feedback on the status of the system, guiding the user through the process. Once the hardware and software are developed, the system is integrated and tested. During testing, the IR sensor is calibrated to ensure it accurately detects movement near the door, while the GSM module is checked to verify that SMS notifications are sent reliably. The system is tested for performance under various conditions, including simulated power outages and multiple incorrect password attempts, to ensure stability and responsiveness. Finally, the entire system is optimized for efficiency, focusing on minimizing power consumption and ensuring long battery life. This comprehensive approach ensures that the GSM Based Door Security System provides a reliable, cost-effective, and scalable solution for enhanced security in various application.

1.6 Implementation Schedule

Month / ***Items***	***Jan 2024***	***Feb 2024***	***Mar 2024***	***Apr 2024***	***May 2024***	***Jun 2024***	***Jul 2024***	***Aug 2024***	***Sep 2024***	***Oct 2024***	***Nov 2024***	***Dec 2024***
Literature Review												
Algorithm Development												
System Design												
Lab Prototype												
Testing and Thesis												

Table 1.1: Roadmap of the implementation schedule of the project report

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The rapid development of security technologies has significantly transformed the way we approach safety and protection in various environments. In recent years, advancements in communication systems, microcontrollers, and sensor technology have led to the creation of smarter, more efficient security systems. This chapter presents a comprehensive review of existing literature related to door security systems, focusing on the integration of GSM technology, sensor-based detection, and microcontroller-based automation. Traditional security systems, which often rely on mechanical locks, have limited functionality in terms of real-time monitoring, remote control, and integration with modern communication technologies. While these systems can provide some level of protection, they lack the ability to send alerts or respond to security breaches in real-time. This limitation has prompted the need for more sophisticated solutions that offer greater convenience, enhanced safety, and improved reliability. Several studies have explored the use of GSM technology in security applications. The GSM network, originally designed for mobile communication, has been effectively utilized to send short messages (SMS) as a means of alerting users about security events. GSM-based systems are particularly beneficial because they allow for remote monitoring and control, making them highly suitable for both residential and industrial security. Furthermore, advancements in microcontroller technology, particularly the use of low-cost microcontrollers like Arduino, have made it possible to design cost-effective, reliable, and scalable security systems. The integration of sensors, such as IR sensors, for detecting movement or unauthorized access, further enhances the functionality of these systems. The use of LCD displays provides real-time feedback, improving the user experience and making the system more intuitive to operate.

This chapter, will examine key research and developments related to these technologies, focusing on how they have been applied in the design of GSM-based security systems. By understanding the strengths and limitations of existing solutions, the literature review will provide a solid foundation for the design and implementation of the GSM Based Door Security System. The review will also highlight the practical implications of integrating GSM technology with microcontroller-based systems, sensor detection, and power management to create a reliable, secure, and user-friendly security solution.

2.2 Related Research

Recent research highlights several innovative systems for enhancing security and safety in electrical systems, particularly those integrating GSM technology for real-time alerts and remote monitoring. Several studies have focused on improving system access control, managing unauthorized access attempts, and ensuring timely responses to security threats. The following research works explore the integration of GSM technology, sensors, and microcontrollers in security applications, which align closely with the **GSM Based Door Security System** developed for this project.

2.2.1 GSM-Based Home Security System with Real-Time Notification

A study by Ahmed and Karim (2020) proposed a **GSM-based home security system** that provides real-time alerts for unauthorized access. The system integrates motion sensors and a GSM module to send SMS notifications to the homeowner whenever a security breach is detected. The researchers found that GSM technology is highly effective in ensuring remote monitoring of security systems, even in areas with limited or no internet access. Their system allowed for immediate user intervention, which is crucial in preventing potential thefts or intrusions. The study demonstrated the feasibility of using GSM communication for low-cost, reliable security solutions, particularly in residential settings where real-time alerts and remote control are essential for effective security management [1].

2.2.2 Arduino-Based GSM Security System for Smart Homes

In a study by Rahman et al. (2021), an **Arduino-based GSM security system** was designed for smart home applications. This system utilized infrared (IR) sensors to detect motion near entry points and GSM technology to notify homeowners via SMS when motion was detected. The researchers emphasized the cost-effectiveness of using Arduino microcontrollers in conjunction with GSM modules, which allowed for the creation of a customizable and scalable security system. The system's integration with an LCD display provided real-time feedback to users, helping them track the status of the system and receive alerts. The study concluded that GSM-based systems offer a practical and affordable solution for enhancing security in residential and small business environments [2].

2.2.3 Real-Time Security Alert System Using GSM and SMS Technology

A study by Hossain et al. (2022) introduced a **real-time security alert system** based on **GSM and SMS technology**. The researchers developed a system that monitored the entry of unauthorized individuals into a secured area using **IR sensors** and sent immediate SMS alerts to a mobile phone upon detecting motion. The system incorporated **password protection** for authorized entry, and

an SMS notification was sent for every unauthorized access attempt. The findings showed that such systems are particularly effective in providing quick notifications to users, enabling them to take timely actions to secure their premises. This research supports the implementation of **GSM communication** as a reliable method for remote monitoring and control of security systems, especially in environments where continuous internet access may not be available.[3]

2.2.4 Smart Door Security System Using GSM and Remote Control

Verma and Singh (2021) presented a **smart door security system** using **GSM** and remote control technologies. Their system utilized **IR sensors** to detect motion and a **GSM module** to send SMS alerts about unauthorized access attempts. The study demonstrated that the integration of **remote control features** allowed users to lock or unlock doors from anywhere using SMS commands. By using a **GSM-based communication protocol**, users could also receive notifications for specific events, such as incorrect password entries or sensor activations. The research highlighted that GSM technology, combined with **microcontrollers** like **Arduino**, offers an affordable yet robust solution for door security systems, especially in residential and office environments.[4]

2.3 Security Measures in Electrical Systems

In modern electrical systems, integrating security measures is essential to ensure the safety of both electrical devices and users. As technology evolves, systems become more complex, and safeguarding them against unauthorized access, faults, and malicious activities becomes a priority. Electrical systems, whether in homes, offices, or industrial environments, need protection to prevent mishaps like equipment damage, data breaches, and even personal injury. This section will explore the importance of security in electrical systems, examine the types of security measures employed, and discuss the challenges faced in implementing effective security protocols.

2.3.1 Importance of Security in Electrical Systems

The importance of security in electrical systems cannot be overstated, particularly in the context of smart homes, industrial automation, and critical infrastructure. Unauthorized access, system malfunctions, or cyberattacks in these systems can result in significant financial loss, operational downtime, and even safety hazards. In smart homes, electrical systems control everything from lighting to security alarms, and any breach could lead to unauthorized control or disabling of essential devices. Additionally, as electrical systems become more interconnected with the Internet of Things (IoT), the need to protect these systems from cyber threats grows. Proper security measures ensure the safe operation of devices, protect sensitive data, and prevent accidents like electric shocks or fires caused by tampering.

2.3.2 Types of Security Measures

Several security measures are employed in electrical systems to ensure their protection. These measures range from traditional physical security controls to advanced digital authentication mechanisms:

1. **Physical Security Measures**: Physical security measures are the first line of defense against unauthorized access to electrical systems. These measures aim to protect electrical devices and control panels from physical tampering, vandalism, or theft. Common methods include the use of locking enclosures to safeguard circuit breakers and control panels, preventing unauthorized personnel from accessing or modifying the system. Fencing around electrical installations and CCTV surveillance cameras are also employed to monitor and control physical access to sensitive areas. These physical barriers and monitoring systems are critical in environments like industrial plants or electrical substations, where the risk of unauthorized access is higher. By implementing these physical security measures, the safety of both the system and the surrounding area is enhanced.
2. **Password Protection and Access Control**: Password protection and access control are essential for limiting who can interact with and control electrical systems. This security measure requires users to input a valid password or PIN to gain access to critical system functions, such as turning electrical devices on or off. This approach is commonly used in systems like smart homes, circuit breakers, and electrical load controllers. In more advanced implementations, biometric authentication methods, such as fingerprint or facial recognition, are used to further secure access. By ensuring that only authorized individuals can interact with the system, this measure helps prevent tampering, theft, or misuse of electrical systems. Password protection and access control play a vital role in securing modern, automated electrical systems, particularly in residential and commercial environments.
3. **Remote Monitoring and Alerts**: Remote monitoring and alerts provide an advanced level of security by allowing real-time oversight of electrical systems and immediate notifications in case of unauthorized access or system malfunctions. Technologies such as **GSM-based alert systems** can send SMS notifications to users when an abnormal event occurs, such as an attempted unauthorized entry or an overload in the system. These remote capabilities ensure that users are informed of any critical events as soon as they occur, allowing for timely intervention to prevent damage or security breaches.

2.3.3 Challenges in Implementing Security Measures

Implementing security measures in electrical systems comes with several challenges. A primary concern is the **cost** of deploying advanced technologies, such as biometric systems and IoT-based monitoring, which can be prohibitively expensive for large-scale applications. Integration with existing systems is another challenge, especially when older infrastructures are incompatible with modern security solutions, necessitating costly upgrades. User compliance and training are crucial, as users must understand how to properly use security features like passwords and access controls. Without proper training, these measures may be ineffective. Reliability is another issue; any failure in the monitoring system or password protection can leave the system vulnerable to tampering or failure. Moreover, the rise in cybersecurity threats means that IoT-based systems are increasingly susceptible to hacking, requiring more robust protective measures. To overcome these challenges, proper planning, technology selection, and continuous user education are essential.

2.4 GSM-Based Security Systems

GSM-based security systems use the **Global System for Mobile Communications (GSM)** technology for remote communication and alert capabilities. By integrating GSM modules, such as the **SIM800L**, these systems send SMS notifications for security breaches, unauthorized access, or status updates, enabling remote monitoring and control. This makes GSM-based security systems a popular choice for security solutions, including door security systems.

2.4.1 Overview of GSM Technology in Security Systems

GSM technology plays a crucial role in modern security systems by enabling remote communication. It allows systems to send alerts, notifications, and updates to users through SMS, which can be received on mobile devices. The advantages of using GSM in security systems include its cost-effectiveness, wide coverage, and ease of implementation, which make it a reliable option for applications like door security systems. GSM enables users to stay informed and take action, even when they are far from the premises.

2.4.2 GSM Module Integration in Security Systems

The **SIM800L GSM Module**, used in your project, integrates seamlessly with the **Arduino Nano** to send SMS notifications when security breaches or unauthorized access attempts occur. The GSM module communicates with the microcontroller, ensuring real-time alerts. It plays a critical role in the system by enabling remote monitoring and communication, thereby enhancing the security of the system. This integration allows users to stay informed about potential security threats and take immediate actions when needed.

2.4.3 Applications and Benefits of GSM in Door Security

GSM technology enhances the functionality of door security systems by providing immediate notifications about access attempts, security breaches, or system status updates. Users can receive SMS alerts about events such as unauthorized access attempts or incorrect password entries, allowing for timely interventions. Additionally, GSM allows for remote control, such as unlocking the door or adjusting security settings via SMS commands, adding convenience and an extra layer of protection for the user. This integration ensures that security is not limited to physical proximity, offering peace of mind even when users are away.

2.5 Access Control and Authentication Technologies

Access control and authentication are critical components in securing electrical and security systems, particularly in systems where sensitive data or devices need protection. As digital and connected systems become more prevalent, the importance of ensuring that only authorized individuals can access or control specific functions of a system is paramount. This section will explore the various technologies used in access control and authentication for modern security systems, particularly in the context of your GSM-based door security system.

2.5.1 Password-Based Access Control

Password-based access control remains one of the most widely used methods for securing systems, both in residential and industrial applications. In this system, users are required to input a valid password or PIN to access critical functionalities such as turning devices on or off, unlocking doors, or accessing secure areas. While relatively simple, password-based systems can be highly effective when combined with other security measures, such as encryption and multi-factor authentication. The primary advantage of password-based access control is its ease of implementation and low cost. However, its security can be compromised if weak passwords are used or if they are not changed regularly.

2.5.2 Biometric Authentication

Biometric authentication is a more advanced method of access control, where an individual's unique biological traits, such as fingerprints, facial recognition, or retinal scans, are used to verify their identity. This technology offers a higher level of security compared to passwords because biological traits are difficult to replicate or steal. Biometric systems are increasingly being integrated into high-security applications, including access to restricted areas and secure systems. In door security systems, biometric authentication can be used in combination with traditional password systems to provide an added layer of security. For instance, a user might be required to enter a password first and then authenticate their identity using their fingerprint or facial recognition. This two-step verification process significantly reduces the unauthorized access.

2.5.3 RFID (Radio Frequency Identification) Access Control

Radio Frequency Identification (RFID) is another popular access control technology, especially in systems where convenience and speed are important. RFID systems use electromagnetic fields to automatically identify and track tags attached to objects or individuals. In security systems, RFID tags are used to control access to doors or secure areas by allowing only authorized RFID cards or fobs to unlock the door. RFID access control systems are often used in corporate offices, hotels, and industrial facilities, where quick and frequent access is necessary. The technology offers the benefit of convenience, as users only need to present an RFID tag to gain access, without the need for passwords or biometric scans. However, one of the challenges with RFID is ensuring that the tags cannot be duplicated or stolen, which makes encryption and other security measures essential.

2.6 Summary

This chapter provided a comprehensive review of the security measures essential for modern electrical and security systems, with a particular focus on the "GSM Based Door Security System." The importance of safeguarding electrical devices from unauthorized access, faults, and cyber threats was emphasized, especially in environments like smart homes and industrial settings. It highlighted key security measures such as physical security, password protection, and remote monitoring, which are critical to ensuring the safety and reliability of systems like the GSM-based door security system. Additionally, the chapter explored the role of GSM-based security systems in enhancing remote communication and real-time monitoring. GSM technology allows users to receive SMS alerts, providing instant notifications about security breaches or unauthorized access attempts, making it a valuable tool for door access control. This integration of GSM modules enables immediate response and effective management of security events.

Lastly, the chapter discussed various access control and authentication technologies, including password-based systems, biometric authentication, and RFID. These technologies ensure that only authorized individuals can access sensitive areas or control critical functions, thus strengthening the security of the "GSM Based Door Security System" and similar systems. The combination of these advanced technologies forms a multi-layered approach to safeguarding electrical and security systems.

CHAPTER THREE

DESIGN AND DEVELOPMENT

3.1 Introduction

The design and development of the **"GSM Based Door Security System"** aim to deliver a modern, efficient, and secure solution for controlling and monitoring door access using GSM technology. This chapter details the technical framework, design methodology, and development process, focusing on key components such as the Arduino Nano microcontroller, SIM800L GSM module, IR sensor, 16x2 LCD display, and the door locking mechanism. The primary goal is to ensure secure access control while offering flexibility and convenience through remote monitoring and notifications. At the core of the system is the Arduino Nano, which processes inputs from the IR sensor, communicates with the GSM module, and manages the locking mechanism based on user commands. The SIM800L GSM module enables real-time SMS notifications to inform users of access attempts and system status, providing remote control capabilities. Users can monitor the system and send SMS commands to unlock the door, ensuring accessibility and security even when they are not physically present. This chapter also highlights the hardware components that were carefully selected to ensure reliability and efficiency. The Arduino Nano was chosen for its compact size and versatility, while the SIM800L GSM module offers robust communication capabilities. The 16x2 LCD display provides clear feedback, such as system status and operational messages, ensuring an intuitive interface for users. The IR sensor detects motion near the door, serving as the system's trigger to initiate monitoring and communication processes. The development process integrated these components into a seamless system, with a focus on security, usability, and reliability. Software development involved programming the Arduino Nano to handle data processing, SMS communication, and access control. Testing was performed to validate system functionality, including real-time command verification, remote control, and SMS-based notifications. The door locking mechanism was evaluated for secure and consistent operation By combining robust hardware and efficient software, the GSM Based Door Security System is designed to be a practical and scalable solution for secure door access management. This system is suitable for both residential and commercial applications. The integration of hardware and software ensures a cohesive, efficient, and secure solution that meets modern security standards. Leveraging GSM technology, the system provides real-time communication and remote control, enhancing the user experience through its intuitive monitoring and operation features.

3.2.1 Designed Model block diagram

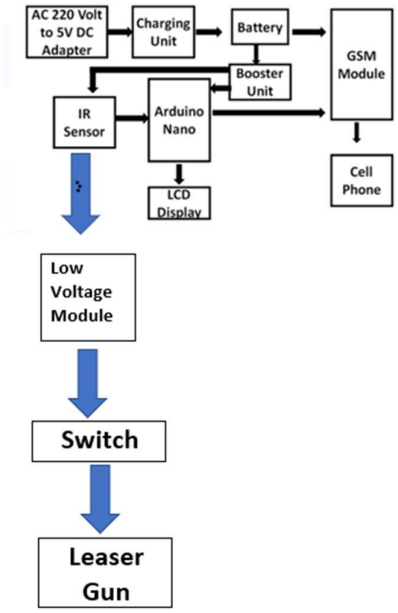

Figure 3.1: Designed model block diagram

The block diagram of the **"GSM Based Door Security System"**, shown in Fig. 3.1, illustrates the system's structure and functionality. The design integrates key components such as the **Arduino Nano**, **SIM800L GSM module**, **IR sensor**, **16x2 LCD display**, and the power supply system. At the core of the design is the Arduino Nano, which processes inputs and coordinates the system's operations. It receives signals from the IR sensor to detect user presence and communicates with the GSM module to send and receive SMS for remote monitoring and control. The **16x2 LCD display** provides real-time feedback to users, showing system status and operational messages such as access granted or denied. The inclusion of this display ensures an intuitive and user-friendly experience, enabling users to understand the system's responses clearly. The SIM800L GSM module allows the system to notify users about access attempts and receive remote commands for unlocking the door, adding a layer of convenience and security. The power system is designed for reliability, incorporating a Li-Ion battery**,** charging circuit**,** booster module**,** and a 5V adapter to provide stable power to all components. This ensures uninterrupted functionality even during power outages, making the system suitable for both residential and commercial environments. The block diagram demonstrates how these components interact to create an efficient and secure door access system, leveraging GSM technology to meet modern security needs.

3.2.2 Circuit Diagram

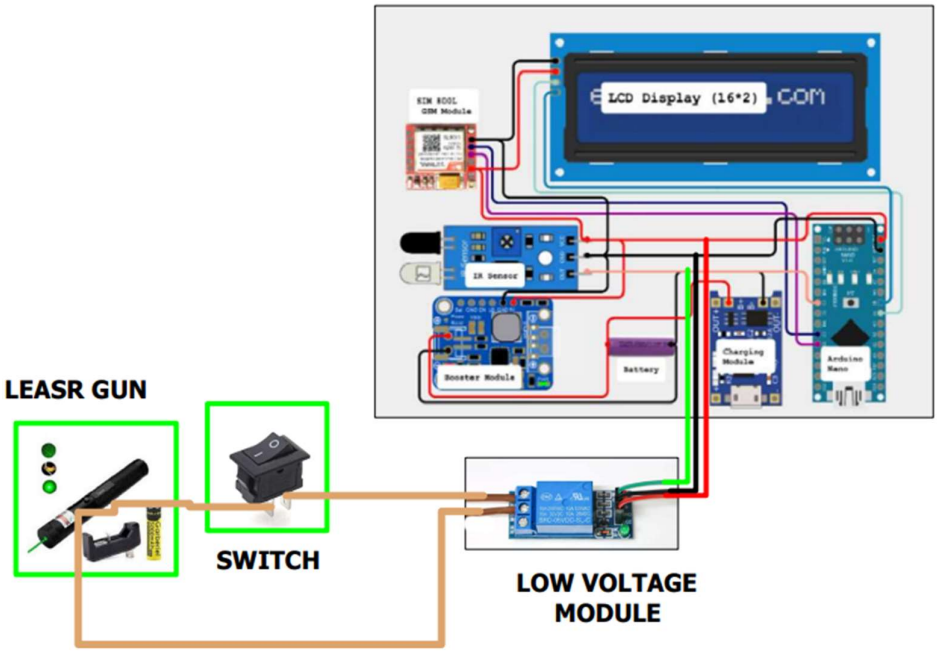

Figure 3.2: Designed model circuit diagram

The circuit diagram for the **"GSM Based Door Security System"** (Fig-3.2) outlines the key components and their interconnections to provide a secure access control solution. At the heart of the system is the **Arduino Nano**, which acts as the central controller, interfacing with several important components: the **IR sensor**, **SIM800L GSM Module**, **16x2 LCD display**, and the **Li-Ion battery**. The IR sensor detects motion and triggers the system to take action when someone approaches the door. The SIM800L GSM Module is used to send SMS notifications to the user in real-time, alerting them about access attempts or system status updates. The **16x2 LCD display** provides visual feedback to the user, displaying relevant information, such as the system status or a message about unauthorized access attempts, enabling quick assessment of the system's security. Powering the system is a **Li-Ion battery**, managed by the **booster module** and a **charging circuit** to ensure a stable power supply. The **5V adapter** provides an external power source, keeping the system operational even during battery charging. This circuit design ensures a reliable and secure access control mechanism for doors, suitable for both residential and industrial use, with all components integrated seamlessly for efficient operation.

3.2.3 List of the components

- Arduino Nano
- LCD Display
- Project board
- 220v to 5-volt adaptor
- IR sensor
- Charging circuit
- Booster circuit
- Battery
- GSM
- Jumper wire
- Connecting wire

3.3 Arduino Nano

The **Arduino Nano**, shown in Fig. 3.3, is a compact microcontroller board powered by the **ATmega328P**, providing a robust yet space-efficient solution for embedded systems and breadboard applications. Designed to offer the core functionality of larger Arduino boards, the Nano is particularly well-suited for projects requiring a minimal footprint. Operating at 5V with an input voltage range of 7-12V, it can connect to various power sources via the **Mini-B USB port** for easy programming and power. The board includes 14 digital I/O pins, 6 of which are capable of **Pulse Width Modulation (PWM)**, enabling versatile control over connected devices like LEDs, motors, and other actuators. Additionally, 8 analog input pins make it suitable for monitoring sensors and other analog inputs, providing an adaptable interface for a variety of real-world applications.

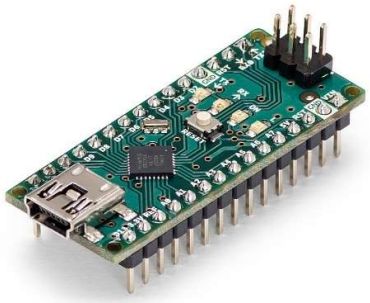

Figure 3.3: Arduino uno

Fig. 3.3 illustrates the **Arduino Nano's** compact design, which also includes 32 KB of flash memory (with 2 KB allocated for the bootloader), 2 KB of SRAM, and 1 KB of EEPROM. With a **16 MHz clock speed**, the Nano delivers reliable processing power for time-sensitive tasks, ensuring smooth control and interaction with peripherals. Unlike some larger Arduino boards, it lacks a dedicated DC power jack, but its size and functionality make it ideal for portable or space-

constrained applications. Its open-source architecture and extensive community support further add to its appeal, making the Arduino Nano a popular choice for projects that demand reliability in a small form factor.

SPECIFICATIONS:

Operative Voltage: 5V (5V model) or 3.3V (3.3V model)

Input Voltage: 7-12V for both models (recommended range)

Digital I/O Pins: 14 Pins (6 with PWM capability)

Analog Input Pins: 8 Pins

DC Current per I/O Pin: 40 mA

Flash Memory: 32 kB (2 KB is taken by bootloader)

SRAM: 2 Kbytes

EEPROM: 2 Kbytes

Clock Speed: 16 MHz (5V model) and 8 MHz (3.3V model)

Table 3.1: ARDUINO NANO Configuration

Pin Group	Pin Name	Description
POWER SOURCE	Vin, 5V, 3.3V, GND	**-Vin**: Input voltage (7-12V) from an external source - **5V**: Regulated 5V output to power the board and connected components - **GND**: Ground pins
Communication INTERFACE	UART(Serial0-erial3), I2C (SCL, SDA), SPI (MOSI, MISO, SCK)	-**UART**: One serial port (TX/RX) for communication -**SPI**: SPI communication pins (MOSI, MISO, SCK) - **I2C**: I2C protocol pins (SCL, SDA)
INPUT-OUTPUT PINS	D0 to D13	14 digital I/O pins, 6 of which support PWM output.
ANALOG INPUT PINS	A0 to A7	8 analog input pins with 10-bit resolution.

PWM	D3, D5, D6, D9, D10, D11	6 PWM pins providing 8-bit resolution.
RESET	RESET	Resets the controller.
EXTERNAL INTERRUPTS	D2, D3	Pins D2 and D3 provide hardware interrupt functionality.
ANALOG COMPARATOR	AIN0, AIN1	Internal analog comparator with input pins AIN0 and AIN1.

The Table 3.1 provides the accurate configuration details for the Arduino Nano, outlining its power source, communication protocols, digital and analog input/output capabilities, PWM outputs, reset function, external interrupts, and analog comparator feature.

3.4 Liquid Crystal Display (LCD) 16*2

The **16x2 Liquid Crystal Display (LCD)**, shown in Figure 3.4, is a popular component in Arduino and microcontroller projects, known for its ability to display data in a compact format. This LCD can show 16 characters per line across two lines, making it an ideal replacement for LEDs in many applications. The standard interface for these LCDs is based on the HD44780U controller chip, which facilitates communication between the microcontroller and the display.

The HD44780U controller allows the LCD to operate in either a 4-bit or 8-bit data mode. In 4-bit mode, the display requires a total of seven lines (three control and four data lines), while in 8-bit mode, it requires eleven lines (three control and eight data lines). This flexibility enables users to connect the LCD easily to a variety of microcontrollers.

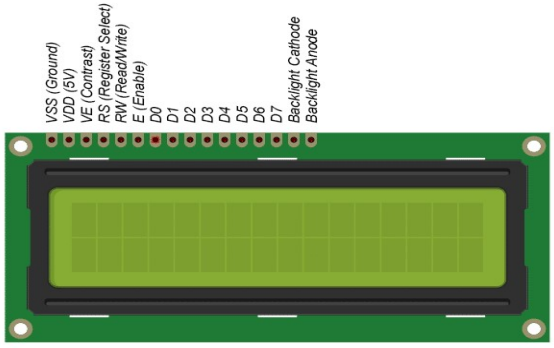

Figure 3.4: LCD 16*2

Features

- The presentation information RAM
- Character initiator ROM
- 160 different 57-dot matrix character patterns
- The display includes internal RAM for data storage and character generation ROM
- It supports 160 different 5x7 dot matrix character patterns
- Microcontrollers can access both display data RAM and character generator RAM
- The LCD offers various functions such as cursor positioning, display on/off, and character blinking.

Table 3.2: Pin symbol description

PIN	Sign	Function
1	VSS	GND
2	VDD	+5V
3	V0	Contrast Adjustment
4	RS	H/L Register select signal
5	R/W	H/L Read/write signal
6	E	H/L Enable signal
7	DB0	H/L Data bus line
8	DB1	H/L Data bus line
9	DB2	H/L Data bus line
10	DB3	H/L Data bus line
11	DB4	H/L Data bus line
12	DB5	H/L Data bus line
13	DB6	H/L Data bus line
14	DB7	H/L Data bus line
15	A	+4.2V for LED
16	K	Power supply for BKL (0V)

Table 3.2 shows the pin functions of a 16x2 LCD display. Pins 1 and 2 are for power (VSS for ground and VDD for +5V), while Pin 3 controls the contrast. Pins 4 to 6 manage the register selection, read/write control, and enable signals, and Pins 7 to 14 form the data bus lines. Pins 15 and 16 provide power for the LCD backlight.

3.5 Booster Circuit

A **booster circuit** or **DC-DC boost converter** is used to step up a lower input voltage to a higher, stable output voltage. In the **GSM-Based Door Security System**, the booster circuit ensures that critical components such as the **Arduino Nano**, **LCD display**, and **SIM800L GSM module** receive a reliable power supply, even if the input voltage fluctuates. The boost converter achieves this by using key components, including an **inductor**, **switch**, **diode**, and **capacitor**, which work together to increase and stabilize the voltage.

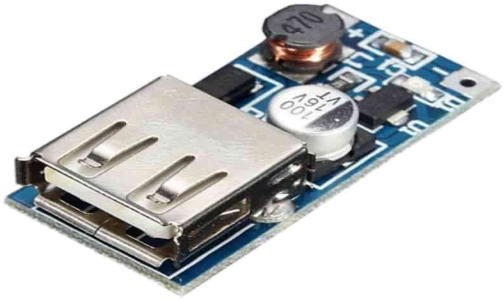

Figure3.5 Booster Circuit

3.6 Breadboard

A breadboard is a tool used for building and testing electronic circuits without soldering. It consists of rows of conductive strips where components like resistors, capacitors, and integrated circuits (ICs) are inserted. In the GSM Based Door Security System, the breadboard allows for the easy connection of the Arduino Nano, SIM800L GSM module, IR sensor, LCD display, and power components to form a prototype. It helps in testing the system's functionality, ensuring that all components work together as expected. The breadboard provides a flexible and efficient way to modify and troubleshoot the circuit before finalizing the design.

Figure 3.6: Breadboard

3.7 IR Sensor

The IR (Infrared) sensor, used in the **GSM Based Door Security System**, is a key component for detecting motion and presence near the door. It operates by emitting infrared light and detecting the reflection of that light from nearby objects or individuals. The sensor is commonly used for proximity detection, and it plays an essential role in activating the system when someone approaches the door. In this system, the IR sensor detects the presence of an individual near the door and triggers the Arduino Nano to activate the GSM module and relay. The sensor provides an output signal to the microcontroller, which processes it to control the door locking mechanism. The IR sensor is an efficient and reliable solution for enhancing the security of the system, enabling automatic responses to detect unauthorized access attempts and improve overall functionality.

Figure 3.7: IR Sensor

6.8 Battery

The 3.7V Li-ion battery is a rechargeable, compact power source widely used in portable electronics and embedded systems due to its high energy density and light weight. In the **GSM Based Door Security System**, this battery ensures continuous power supply, even during power outages, by providing backup energy to crucial components like the Arduino Nano, GSM module, and LCD display.

With a nominal voltage of 3.7V, the Li-ion battery is ideal for low-power applications, offering stable voltage for extended periods. Its rechargeable nature, along with a long life cycle, makes it both cost-effective and sustainable for projects that require uninterrupted operation. Additionally, its compact size allows easy integration into the system's design without significantly increasing the overall bulk of the project.

Figure 3.8: li-ion battery

3.9 GSM

The SIM800L GSM/GPRS module, used in the **GSM Based Door Security System**, is a compact, versatile communication device that supports a wide range of functionalities, including sending SMS messages, making phone calls, and connecting to the internet via GPRS. Operating in the 3.4V to 4.4V voltage range, it is suitable for battery-powered projects, making it an ideal choice for IoT applications. The module supports quad-band GSM frequencies, ensuring compatibility in various regions. It communicates with the microcontroller through UART at baud rates between 1200bps and 115200bps, with auto-baud recognition for easy configuration.

Figure 3.9: GSM

In the context of the GSM Based Door Security System, the SIM800L module plays a crucial role by enabling remote control of the door. Through SMS, users can receive notifications regarding access attempts and system status, as well as send commands to control the door lock. The module enhances the system's functionality by providing reliable wireless communication, making it an essential component for secure, remote monitoring and control of the door access system.

3.10 220v to 5-volt adaptor

A 220 to 5-volt adapter, often referred to as a power supply or charger, is a device that converts electrical voltage from 220 volts to a lower voltage of 5 volts. This type of adapter is commonly used to power or charge electronic devices that require a 5-volt power source, such as smartphones, tablets, USB-powered devices, and various small electronics. The adapter takes the higher input voltage of 220 volts (which is a standard voltage level in many parts of the world, including Europe and Asia) and steps it down to a safer and compatible 5 volts for the connected device. This is typically achieved through a transformer or other voltage conversion technology within the adapter.

Figure 3.10: 220v to 5-volt adaptor 220v to 5-volt adaptor

3.11 Charging Circuit

The charging circuit in the **GSM-Based Door Security System** is responsible for safely charging the 3.7V Li-ion battery. It converts the 5V input from the adapter to a stable 4.2V output required for charging the battery. The circuit controls the current to ensure safe and efficient charging, typically around 500mA to 1A, depending on the battery's specifications.

Figure 3.10: charging Circuit

It also includes protection features to prevent overcharging, over-discharge, and short circuits, ensuring the longevity and safety of the battery. With an integrated charging IC like TP4056, the circuit provides reliable charging, making it a crucial component for maintaining uninterrupted operation of the system.

3.12 Jumper wire

It is possible to connect two places without soldering using jumper wires, which are wires with connector pins on either end. With breadboards and other prototype equipment, jumper wires make it easy to change circuits as needed. Despite the variety of colors available for jumper wires, the hues don't hold much meaning. Three types of jumper wire are commonly available: male-to-male, male-to-female, and female-to-female. Every wire has an endpoint that distinguishes it from the others. Male ends have a pin sticking out, which can be used to plug into other items while female ends have a pin sticking out to be plugged into items.

Figure 3.11: Jumper wire

3.13 Design Specification

- **Microcontroller**: Arduino Nano, operating at 16 MHz, with 14 digital I/O pins (6 of which support PWM output) and 8 analog input pins. The Nano handles all input, output, and control operations within the system.
- **Display:** 16x2 Liquid Crystal Display (LCD), connected to the Arduino to display system status, password prompts, and feedback on operations.
- **Power Supply**: A combination of AC and DC sources. The AC source powers the load, while the DC source provides stable power to the Arduino and other components. A backup 3.7V Li-ion battery ensures uninterrupted operation during power outages.
- **Relay Module**: Single Channel Relay Module, designed to switch AC loads with low-power signals from the Arduino, allowing controlled on/off functionality.

- **Input Interface**: 4x4 Matrix Keypad, used for password entry to control access to the system.
- **Booster Circuit:** DC-DC booster circuit used to stabilize voltage levels, ensuring consistent performance across all system components.
- **Software**: Programmed using the Arduino IDE with C/C++ support, handling password verification, relay control, and display updates.
- **Housing**: Enclosure with basic protection against dust and accidental contact, suitable for indoor use in controlled environments.

3.14 Summarization

This chapter provided an in-depth overview of the components and design specifications for the GSM-Based Door Security System. It detailed the key hardware elements, including the Arduino Nano microcontroller, 16x2 LCD display, single-channel relay module, and the power supply system that ensures reliable operation. The chapter also discussed the role of the 4x4 matrix keypad for user input and the booster circuit for stabilizing voltage levels across the system. Additionally, the GSM module (SIM800L) and IR sensor were introduced as critical components for remote communication and motion detection, respectively. The system's power is supplied through a combination of AC and DC sources, with a backup Li-ion battery ensuring continuous operation. Software control, managed via the Arduino IDE, handles key functions such as password verification, relay control, and real-time system feedback. Finally, the design also considers the housing and protection of the system, ensuring durability and safety in everyday use. This chapter establishes the foundation for understanding the design and functionality of the system, integrating hardware and software elements to create a reliable, efficient, and secure door access control solution.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 Introduction

In this chapter, focuses on the results obtained from the implementation of the GSM-Based Door Security System and provides a detailed discussion on the system's performance, functionality, and reliability. It examines how effectively the system meets its objectives of providing secure access control and remote monitoring through GSM technology. The primary outcomes of the project include successful integration of hardware components such as the Arduino Nano, SIM800L GSM module, IR sensor, 16x2 LCD display, and relay module, along with their seamless interaction with the software. The chapter highlights key functionalities such as password-based access control, SMS-based notifications, and motion detection. Additionally, the role of the power supply, including the backup Li-ion battery and booster circuit, in maintaining system stability is evaluated. Through testing and observation, the chapter discusses the system's accuracy in verifying passwords, sending real-time SMS alerts, and controlling the door mechanism. Challenges encountered during development and deployment are addressed, along with the steps taken to resolve them. The chapter concludes by reflecting on the project's overall efficiency and areas for potential enhancement.

4.2 Result

Figure 4.1 shows the setup of the **GSM-Based Door Security System**, which includes the Arduino Nano**,** SIM800L GSM module**,** IR sensor**,** 16x2 LCD display**, and** relay module. The

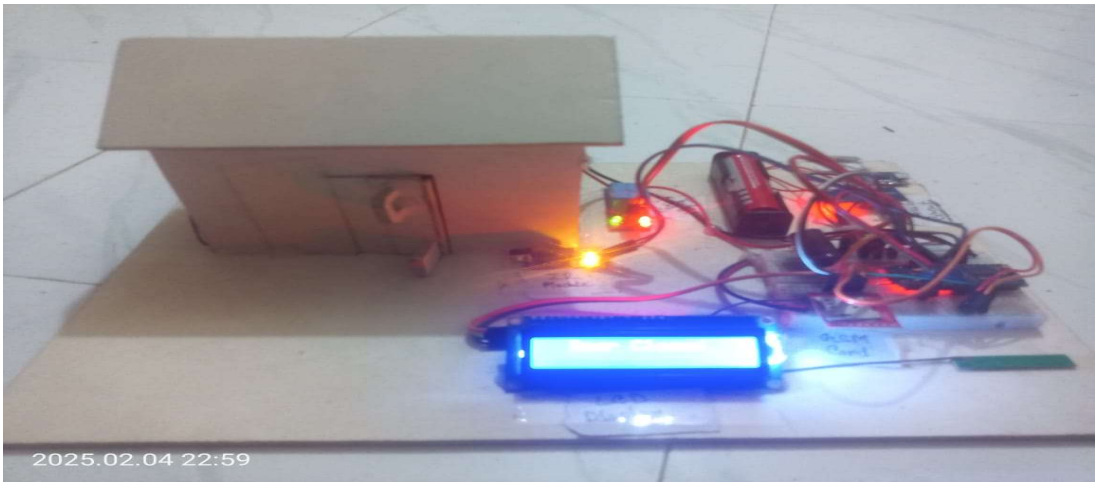

Figure 4.1: Project Picture

Arduino Nano controls the entire system, processing inputs from the IR sensor to detect motion and interacting with the GSM module to send SMS notifications. The LCD display provides real-time feedback, showing system status and access prompts. The relay module controls the door locking mechanism based on password verification. The setup also includes a reliable power supply with a Li-Ion battery and booster circuit to ensure stable operation, even during power outages. This setup effectively integrates hardware and software to provide secure and remote door access control.

4.3 Outcome Analysis

The results of the **" GSM-Based Door Security System "** project were thoroughly tested and analyzed through various scenarios to evaluate the system's functionality and performance.

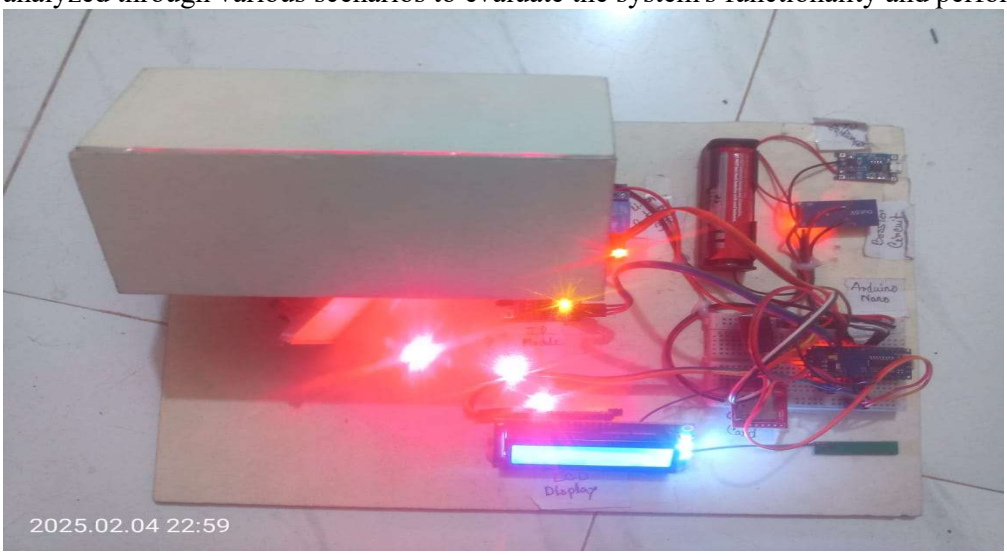

Figure 4.2: Door Open

This figure *(fig-4.2)* the state of the door when it is open, either during an active call or after a call has ended. The system, upon receiving the correct password via SMS, activates the **GSM module**, which communicates with the **Arduino Nano** to trigger the **relay module**. This opens the door, allowing access. The **IR sensor** may detect the user's presence to confirm the action. The **LCD display** will likely show a message like "Access Granted" or "Door Open" to indicate that the door has been successfully unlocked, and the system is in an active state.

In this image *(fig-4.3)*, the state of the door when it is closed and locked after the call or interaction has ended. After the user completes the action, the system reverts to its idle state, locking the door for security. The **relay module** is triggered to lock the door, and the **LCD display** may show a message such as "Door Locked" or "Call Ended" to inform the user that the door has returned to a secure state. This ensures that no unauthorized access occurs once the user has finished their

interaction with the system.

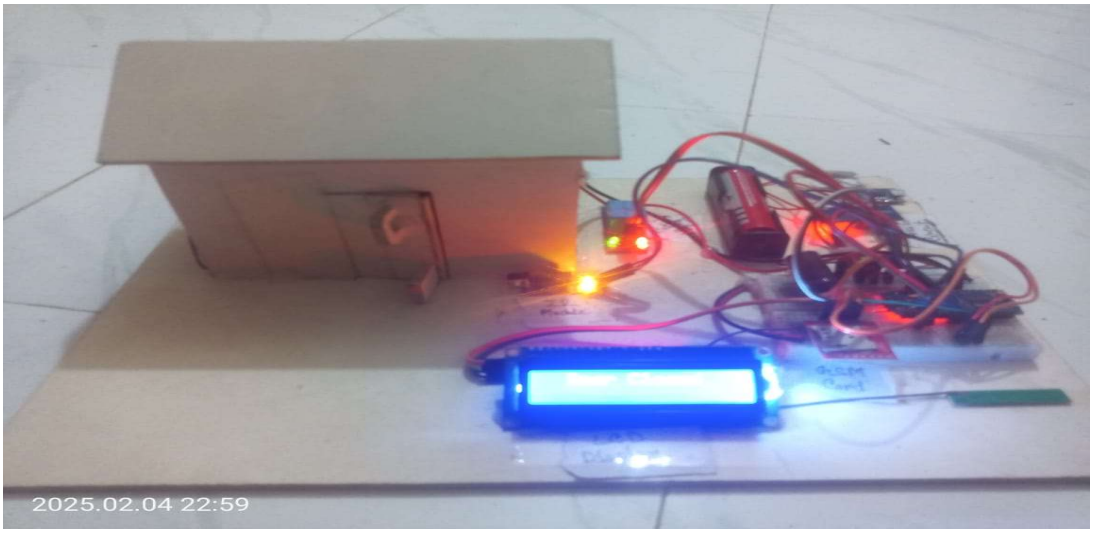

Figure 4.3: Door Closed

the outcome analysis demonstrates the GSM-Based Door Security System's effectiveness in providing secure access control and real-time notifications. The system successfully manages door operations through SMS communication, and remote control. It ensures that the door remains locked and secure when not in use, enhancing overall safety and reliability.

4.4 Advantages

- **Energy Efficiency:** The system optimizes power usage by enabling selective control of door mechanisms and notifications. By ensuring operations occur only when authorized, it reduces unnecessary energy consumption, contributing to lower power usage in security systems.
- **Remote Monitoring:** The GSM module enables real-time remote monitoring through SMS alerts, providing users with updates on the system's status and any security breaches. This feature enhances convenience and ensures users are informed, even when they are away from the premises.
- **Quick Response Capability:** Immediate notifications during unauthorized access or malfunctions allow users to act promptly. This proactive approach minimizes potential security risks and ensures quick resolution of issues.
- **User-Friendly Interface:** The system features an easy-to-read 16x2 LCD display for status updates and feedback, and the keypad offers straightforward password input. This intuitive interface ensures that users of all technical levels can operate the system effectively.

- **Reduced Risk of Electrical Hazards:** Unauthorized attempts trigger alerts via SMS through the GSM module, ensuring immediate action can be taken. This safeguards sensitive areas and prevents tampering or unauthorized access.
- **Adaptability and Flexibility**: The system is designed to be implemented in various applications, from residential doors to office and industrial setups. The use of an Arduino-based platform allows for customizations to suit specific security requirements, making it a versatile choice.
- **Scalability**: The system can easily be expanded to include additional features such as multiple door control, biometric integration, or advanced security protocols. Its modular design and Arduino architecture support future upgrades and enhancements.
- **Ease of Maintenance**: The modular structure, including the GSM module, relay, and LCD, simplifies troubleshooting and component replacement. This ensures minimal downtime and extends the lifespan of the system.
- **Cost-Effective**: By utilizing readily available and affordable components, the GSM-Based Door Security System provides a budget-friendly solution without compromising functionality. Its low operational costs make it suitable for both small-scale and large-scale applications.
- **Backup and Stability**: The inclusion of a booster circuit and a 3.7V Li-ion battery ensures stable operation during voltage fluctuations or power outages. This reliability makes the system dependable in critical situations, maintaining continuous functionality.
- **Enhanced Security**: Password-protected access minimizes the risk of unauthorized entry. The GSM module provides real-time notifications, alerting the user to any security breaches or access attempts, enhancing overall safety in residential or industrial setups.

4.5 Disadvantages

- **Dependence on Power Supply:** While the system includes a backup battery, prolonged power outages or battery depletion could render the system inoperable, impacting its reliability.
- **Password Management:** Forgetting the password or unauthorized changes to the password could lock out legitimate users, creating inconvenience or the need for manual system reset.
- **Component Sensitivity:** Certain components, like the GSM module or relay, may be

sensitive to environmental conditions such as heat or humidity, which could affect their performance or lifespan.

- **Signal Reliability:** The GSM module relies on network connectivity to send alerts. Poor signal strength or network unavailability could delay or prevent critical notifications from being delivered
- **Limited Security Against Advanced Threats:** While the password-based mechanism enhances security, it may not be sufficient against advanced hacking techniques or physical tampering, requiring additional layers of protection for sensitive application.
- **Maintenance Requirements:** Over time, components such as the Li-ion battery or relay module may require replacement due to wear and tear, leading to periodic maintenance costs.
- **Initial Setup Complexity:** Setting up the system, including configuring the GSM module, assembling the hardware, and programming the microcontroller, may require technical expertise, which could be a barrier for non-technical users.
- **Limited Range of GSM Coverage:** The system's reliance on GSM technology means it may not function effectively in areas with weak or no GSM network coverage, limiting its applicability in remote or rural locations.

4.6 Cost Estimation

SL. No	Component's name	Price
1	Arduino Nano	1000
2	Liquid Crystal Display (LCD) 16*2	300
3	Project board	100
4	Booster Circuit	150
5	Single Channel Relay Module	100
6	IR Sensor	150
7	Battery	120
8	Jumper wire	100
9	220volt to 5volt Adaptor	150
10	Charging Circuit	100
11	GSM	500
12	Foam board	80
	Total Cost	**2850**

4.7 Discussion

This section, provides a detailed discussion on the key aspects of the "**GSM-Based Door Security System"**, focusing on component selection, system architecture, circuit design, and programming logic. The project integrates reliable components such as the Arduino Nano, IR sensor, GSM module, and LCD display to deliver an efficient and secure solution for door access control.

1. **Component Selection**: The components were chosen based on their compatibility, reliability, and efficiency. The Arduino Nano serves as the central control unit, managing inputs and outputs. The GSM module (SIM800L) facilitates remote communication, enabling SMS-based notifications. The IR sensor ensures the detection of unauthorized entry attempts, while the LCD display provides real-time feedback for user interaction. A booster circuit and Li-ion battery backup are included to maintain stable power supply during fluctuations or outages, ensuring uninterrupted system performance.

2. **System Architecture**: The system architecture integrates hardware and software seamlessly, with the Arduino Nano functioning as the core controller. The GSM module allows for communication with users via SMS, enabling alerts and remote control features. The IR sensor monitors entry points, and the LCD display provides a user-friendly interface to display system status and feedback. This structured design ensures a robust, interactive, and secure system.
3. **Circuit Design and Integration**: The circuit design focuses on efficient communication and power stability. The Arduino Nano is connected to the GSM module, IR sensor, and LCD display to form a control loop. The booster circuit stabilizes voltage levels, while the relay ensures secure switching of electrical connections. Careful isolation between high-power and low-power sections of the circuit ensures safety and prevents interference.
4. **Programming Logic**: The programming logic is designed to process user inputs, manage communication through the GSM module, and control system responses. The code facilitates password authentication and generates alerts for unauthorized access attempts. It also ensures real-time feedback via the LCD display and sends SMS notifications using the GSM module. This logic creates a reliable and secure system for door security management.

The design, and development of the **GSM-Based Door Security System** combine advanced components and efficient programming to create a secure access control system. By integrating the Arduino Nano, GSM module, IR sensor, and LCD display, the project delivers real-time feedback and remote communication capabilities. The structured system architecture and robust programming logic ensure dependable performance, addressing critical security needs for residential, commercial, and industrial applications.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATION

5.1 Conclusion

The GSM-Based Door Security System presents a modern and effective solution for controlling and monitoring door access, integrating key technologies such as GSM communication, motion detection, and microcontroller-based automation. By utilizing components like the Arduino Nano, SIM800L GSM module, IR sensor, and LCD display, the system successfully offers secure access control, enabling users to remotely monitor and control the door from anywhere through SMS commands. The system's design allows for real-time alerts in case of unauthorized access attempts, making it a significant improvement over traditional mechanical locks.

Incorporating a Li-Ion battery backup and a booster module ensures continuous operation, even during power failures, adding an extra layer of reliability. The system's compact design and user-friendly interface make it suitable for both residential and commercial environments. Through rigorous testing and development, the GSM-Based Door Security System has demonstrated its capability to provide secure, reliable, and scalable door access management. By combining hardware and software components seamlessly, the project highlights the potential for GSM technology to enhance traditional security systems, making them smarter, more convenient, and easier to manage remotely. Ultimately, the GSM-Based Door Security System not only meets its primary objectives of security and remote access but also sets a foundation for further advancements in smart security solutions. The system is cost-effective, energy-efficient, and adaptable to different environments, making it a promising solution for enhancing the security of homes, offices, warehouses, and other restricted areas.

5.2 Limitations of the Work

The "GSM-Based Door Security System" project, like any security system, has several limitations that need to be considered:

- **Environmental Sensitivity**: Key components such as the LCD display, keypad, and Arduino Nano may be vulnerable to environmental factors like moisture, dust, and temperature fluctuations. These conditions could impact the durability and reliability of the system, potentially leading to component failure or reduced performance over time, especially in outdoor or harsh industrial environments.
- **Communication Range**: The GSM module used in the system relies on cellular networks to send and receive SMS messages. As a result, the system's performance is dependent on

the availability and quality of the cellular network. In areas with weak or no network coverage, the system may experience delays or failures in sending SMS notifications, compromising its effectiveness in remote monitoring.

- **Limited Power Protection**: While the system includes a booster circuit and backup battery for power stability, it lacks a comprehensive surge protection mechanism. In the event of a high-voltage power surge, critical components like the relay or Arduino could be damaged, disrupting system functionality. Incorporating surge protection would enhance the system's resilience but would increase both cost and design complexity.
- **Scalability Constraints**: The current design, based on the Arduino Nano, is effective for single-load applications but may encounter processing or memory limitations if expanded to handle multiple loads or more complex functionalities. This limits its scalability for larger applications or environments requiring centralized control over several circuits.
- **Security Vulnerabilities:** Although the system incorporates password-based access control, there may still be security vulnerabilities, such as interception of SMS messages or brute-force attacks on the password. Enhancing the system's security with encryption or adding multiple layers of authentication would help mitigate these risks, but it would increase system complexity and processing demands
- **Maintenance Challenges**: Although the modular setup of the system allows for individual component replacement, diagnosing issues with the microcontroller or other electronic components may require specialized knowledge. Therefore, system maintenance may present challenges for non-technical users, who may need professional assistance or additional training..
- **Cost Constraints for Advanced Features**: Incorporating advanced features, such as surge protection, remote monitoring, or multi-user access, would increase both the cost and complexity of the system. While these improvements could enhance functionality, the added expense might limit the system's accessibility for budget-conscious users, particularly in residential or small-scale environments.
- **Limited Scalability**: The system is designed to control a single load. Expanding it to manage multiple loads or larger systems would require additional modifications, impacting both cost and design complexity.

5.3 Future Recommendation

To enhance the **GSM-Based Door Security System**, several future improvements are recommended. Firstly, integrating wireless communication, such as Wi-Fi or Bluetooth, would enable a more modern and flexible user experience. This would allow users to manage the system remotely via a mobile app or web interface, providing real-time notifications and control, without being limited to SMS-based communication. Furthermore, enhancing security features by adding multi-factor authentication (such as biometric verification or two-factor authentication) would strengthen the system's defense against unauthorized access. To cater to larger applications, the system could be upgraded to support multiple doors or entry points, particularly for commercial or industrial use. This could be achieved by integrating more powerful microcontrollers, such as the Arduino Mega or Raspberry Pi, enabling the management of several doors under one central control. In terms of reliability, additional power protection, including surge protection circuits, could be incorporated to prevent damage to components during power surges. Expanding the backup power system with higher-capacity batteries or even integrating solar power solutions would ensure uninterrupted operation, especially in areas with unreliable electrical supplies. For better security, upgrading the motion detection system with advanced technologies such as PIR sensors or cameras would provide more accurate and comprehensive monitoring.

Additionally, remote monitoring and alerts could be further enhanced by incorporating cloud-based systems, enabling users to monitor their system in real-time and access historical data through a mobile app or web portal. Finally, to improve the system's energy efficiency, optimizing power consumption by incorporating low-power components and intelligent sleep modes would extend battery life, reducing the need for frequent maintenance and charging. These recommendations, when implemented, would significantly improve the system's functionality, scalability, and security, making it a more versatile and reliable solution for both residential and commercial applications.

REFERENCES

[1] Ibrahim, Adnan, et al. "GSM based digital door lock security system." 2015 International Conference on Power, Instrumentation, Control and Computing (PICC). IEEE, 2015. https://doi.org/10.1109/PICC.2015.7455796

[2] Gayathri, M., P. Selvakumari, and R. Brindha. "Fingerprint and GSM based security system." *International journal of engineering sciences & research technology* 1.3 (2014): 4024-7.

[3] Al Rakib, M. A., Rahman, M. M., Rana, M. S., Islam, M. S., & Abbas, F. I. (2021). GSM based home safety and security system. *European Journal of Engineering and Technology Research*, *6*(6), 69-73..

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

[5] G. M. S. Mahmud Rana, A. A. Mamun Khan, M. N. Hoque and A. F. Mitul, "Design and implementation of a GSM based remote home security and appliance control system," 2013 2nd International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, 2013, pp. 291-295, doi: 10.1109/ICAEE.2013.6750350.

[6] R. Teymourzadeh, Salah Addin Ahmed, Kok Wai Chan and Mok Vee Hoong, "Smart GSM based Home Automation System," 2013 IEEE Conference on Systems, Process & Control (ICSPC), Kuala Lumpur, 2013, pp. 306-309, doi: 10.1109/SPC.2013.6735152.

[7] W. M. El-Medany and M. R. El-Sabry, "GSM-based remote sensing and control system using FPGA," 2008 International Conference on Computer and Communication Engineering, Kuala Lumpur, 2008, pp. 1093-1097, doi: 10.1109/ICCCE.2008.4580776.

[8] V. D. Vaidya and P. Vishwakarma, "A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation," 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, 2018, pp. 1-4, doi: 10.1109/ICSCET.2018.8537381.

[9] Huang, Huiping et al. "A remote home security system based on wireless sensor network and GSM technology," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Vol. 1, IEEE, 2010.

[10] Parab, Abhishek S., Amol Joglekar, and Abhishek S. Parab. "Implementation of home security system using GSM module and microcontroller." International Journal of Computer Science and Information Technologies, 6.3 (2015): 2950-2953.

[11] Bangali, Jayashri, and Arvind Shaligram, "Design and Implementation of Security Systems for Smart Home based on GSM technology," International Journal of Smart Home, 7.6 (2013): 201-208.

[12] Khan, Sadeque Reza et al., "Design and implementation of low cost home security system using GSM network," International Journal of Scientific & Engineering Research 3.3 (2012): 1.

[13] Ahmad, Arbab Waheed et al., "Implementation of ZigBee-GSM based home security monitoring and remote control system," 2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), IEEE, 2011.

[14] Ahmad, Arbab Waheed, et al. "Implementation of ZigBee-GSM based home security monitoring and remote control system." *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2011.

[15] Deva, Seelam Vasavi Sai Viswanada Prabhu, and Shyam Akashe. "Implementation of GSM based security system with IOT applications." *International Journal of Computer Network and Information Security* 9.6 (2017): 13. https://doi.org/10.2991/iccasp-16.2017.102

[16] Parab, Abhishek S., Amol Joglekar, and Abhishek S. Parab. "Implementation of home security system using GSM module and microcontroller." *International Journal of Computer Science and Information Technologies* 6.3 (2015): 2950-2953..
[17] Y. Zhao and Z. Ye, "Low cost GSM/GPRS BASED wireless home security system", IEEE Trans. Consumer Electron, vol. 56, no. 4, (2007) January, pp. 546-567.
[18] Z. Bing, G. Yunhung, L. Bo, Z. Guangwei and T. Tian, "Home Video Security Surveillance", Info-Tech and Infonet, 2001,Proceedings,ICII 2001-Beijing. 2001 International Conference, vol. 3, pp. 202-208.
[19] M. Meyer, M. Hotter and T. Ohmacht, "A new system for Video-based Detection of moving objects and its integration into digital networks", Security Technology 1996, 30th Annual 1996 International Carnahan Conference, (1996), pp. 105-110.
[20] Rana, G.M.S.M., Khan, A.A.M., Hoque, M.N. and Mitul, A.F. (2013) Design and Implementation of a GSM Based Remote Home Security and Appliance Control System. Proceedings of the 2nd International Conference on Advances in Electrical Engineering, Dhaka, 19-21 December 2013, 291-295.
[21] Ahmad, A.W., Jan, N., Iqbal, S. and Lee, C. (2011) Implementation of ZigBee—GSM Based Home Security Monitoring and Remote Control System. IEEE 54th International Midwest Symposium on Circuits and Systems, Seoul, 7-10 August 2011, 1-4.
[22] Golzar, M.G. and Tajozzakerin, H.R. (2010) A New Intelligent Remote Control System for Home Automation and Reduce Energy Consumption. 4th Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation, Kota Kinabalu, 26-28 May 2010, 174-180.
[23] Yuksekkaya, B., Kayalar, A.A., Tosun, M.B., Ozcan, M.K. and Alkar, A.Z. (2006) A GSM, Internet and Speech Controlled Wireless Interactive Home Automation System. IEEE Transactions on Consumer Electronics, 52, 837-843. http://dx.doi.org/10.1109/TCE.2006.1706478.
[24] Van Der Werff, M., Gui, X. and Xu, W.L. (2005) A Mobile-Based Home Automation System. Proceedings of the 2nd International Conference on Mobile Technology, Applications and Systems, Guangzhou, 15-17 November 2005, 1-5.
[25] Hwang, I.-K., Lee, D.-S. and Baek, J.-W. (2009) Home Network Configuring Scheme for All Electric Appliances using ZigBee-Based Integrated Remote Controller. IEEE Transactions on Consumer Electronics, 55, 1300-1307. http://dx.doi.org/10.1109/TCE.2009.5277992.
[26] Lee, H.-B., Park, J.-L., Park, S.-W., Chung, T.-Y. and Moon, J.-H. (2010) Interactive Remote Control of Legacy Home Appliances through a Virtually Wired Sensor Network. IEEE Transactions on Consumer Electronics, 56, 2241-2248. http://dx.doi.org/10.1109/TCE.2010.5681096.
[27] Zeyad, Mohammad, Susmita Ghosh, and SM Masum Ahmed. "Design prototype of a smart household touch sensitive locker security system based on GSM technology." *International Journal of Power Electronics and Drive Systems* 10.4 (2019): 1923..
[28] Falohun, A. S., et al. "DESIGN AND CONSTRUCTION OF A DOOR SECURRITY ALARM SYSTEM BASED ON SMS VERIFICATION AND VOICE RECOGNITION." *International Journal of Advanced Research in Computer Science* 12.3 (2021).
[29] Murthy, B. Rama, et al. "Development of gsm based advanced alert home locker safety security system using arduino uno." *International Journal of Scientific Research in Science and Technology (IJSRST)* 4.2 (2018): 1154-1160.
[30] Shawki, F., et al. "Microcontroller based smart home with security using GSM technology." *IJRET: International Journal of Research in Engineering and Technology* 4.06 (2015): 2319-1163.
[31] Usha, V., et al. "GSM based door open and closing system." *International Journal of*

Engineering & Technology 7.2.4 (2018): 97-100.

APPENDIX

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <SoftwareSerial.h>
// Define LCD address and size (e.g., 0x27 for a 16x2 display)
LiquidCrystal_I2C lcd(0x27, 16, 2);
// Define Software Serial pins for SIM800L
SoftwareSerial sim800(7, 8); // RX, TX for SIM800L
// Define IR Sensor and Buzzer pins
const int IR_SENSOR_PIN = 2;
const int BUZZER_PIN = 4;
// Phone number to call
String phoneNumber = "+8801743727172"; // Replace with your phone number
// Variable to store the last state of the IR sensor
int lastIrState = LOW;
void setup() {
  // Initialize LCD
  lcd.init();
  lcd.backlight();
    // Initialize Serial for debugging
  Serial.begin(9600);
    // Initialize SIM800L Serial
  sim800.begin(9600);
    // Set IR sensor and buzzer pins
  pinMode(IR_SENSOR_PIN, INPUT);
  pinMode(BUZZER_PIN, OUTPUT);
```

```
  // Display startup message
  lcd.setCursor(0, 0);
  lcd.print("Door Security");
    lcd.setCursor(0, 1);
  lcd.print("System Ready");
  delay(2000);
  lcd.clear();
}
void loop() {
  // Read IR sensor
  int irState = digitalRead(IR_SENSOR_PIN);

  // Check if IR sensor state has changed
  if (irState != lastIrState) {
    // Activate the buzzer for 1 second
    digitalWrite(BUZZER_PIN, HIGH);
    delay(1000);
    digitalWrite(BUZZER_PIN, LOW);
     // Update lastIrState
    lastIrState = irState;
     // Display corresponding message on LCD
    if (irState == HIGH) {
      lcd.setCursor(3, 0);
      lcd.print("Door Open");
      lcd.setCursor(0, 0);
      lcd.print("Calling......");
```

```
      // Call the phone number
      makeCall();
       // Wait until object is detected again
      while(digitalRead(IR_SENSOR_PIN) == HIGH) {
        delay(500);
      }
    } else {
      lcd.setCursor(2, 0);
      lcd.print("Door Closed");
    }
  }
delay(500); // Small delay to avoid excessive polling
}
// Function to make a call using SIM800L
void makeCall() {
  lcd.setCursor(0, 1);
  lcd.print("Calling...      ");
  sim800.print("ATD" + phoneNumber + ";\r"); // Send AT command to dial the number
  delay(10000); // Wait for 10 seconds (adjustable duration)
  sim800.print("ATH\r"); // Hang up the call
  lcd.setCursor(0, 1);
  lcd.print("Call Ended      ");
  delay(2000);
}
```