M.Kumarasamy
College of Engineering
NAAC Accredited Autonomous Institution
Approved by AICTE & Affiliated to Anna University
ISO 9001:2015 Certified Institution
Thalavapalayam, Karur - 639 113, TAMILNADU.

EEC1363 BATTERY MANGEMENT SYSTEM

GSM BASED SMART SECURITY SYSTEM WITH PASSWORD VERIFICATION AND REMOTE ACCESS

A PROJECT REPORT

Submitted by

ADITHIYA SG	**(927623BEE005)**
AKHIL M	**(927623BEE007)**
NITEESH P	**(927623BEE063)**

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

in

ELECTRICAL AND ELECTRONICS ENGINEERING

M.KUMARASAMY COLLEGE OF ENGINEERING, KARUR

DECEMBER 2025

M.KUMARASAMY COLLEGE OF ENGINEERING, KARUR

(Autonomous Institution affiliated to Anna University, Chennai)

BONAFIDE CERTIFICATE

Certified that this project report **"GSM BASED SMART SECURITY SYSTEM WITH PASSWORD VERIFICATION AND REMOTE ACCESS"** is the bonafide work of "**ADITHIYA SG (927623BEE005), AKHIL M (927623BEE007), NITEESH P (927623BEE063)"** who carried out the project work during the academic year 2025-2026 under my supervision.

SIGNATURE

Dr. J. UMA M.E., Ph.D.

HEAD OF THE DEPARTMENT

Department of Electrical and Electronics Engineering,

M.Kumarasamy College of Engineering, Thalavapalayam, Karur-639113

SIGNATURE

Mrs. P. SASIREKHA M.E.,

SUPERVISOR

Assistant Professor,

Department of Electrical and Electronics Engineering,

M.Kumarasamy College of Engineering,

Thalavapalayam, Karur-639113.

This Project Work (EEC1363 – Battery Mangement System) report has been submitted for the Vth Semester Project viva voce Examination held on ____________

INTERNAL EXAMINER **EXTERNAL EXAMINER**

VISION AND MISSION OF THE INSTITUTION

VISION

To emerge as a leader among the top institutions in the field of technical education

MISSION

- Produce smart technocrats with empirical knowledge who can surmount the global challenges
- Create a diverse, fully-engaged learner-centric campus environment to provide quality education to the students
- Maintain mutually beneficial partnerships with our alumni, industry and professional associations.

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

VISION

To produce smart and dynamic professionals with profound theoretical and practical knowledge comparable with the best in the field.

MISSION

- Produce hi-tech professionals in the field of Electrical and Electronics Engineering by inculcating core knowledge.
- Produce highly competent professionals with thrust on research.
- Provide personalized training to the students for enriching their skills.

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

- **PEO1:** Graduates will have flourishing career in the core areas of Electrical Engineering and allied disciplines.
- **PEO2:** Graduates will pursue higher studies and succeed in academic/research careers.
- **PEO3:** Graduates will be a successful entrepreneur in creating jobs related to Electrical and Electronics Engineering /allied disciplines.
- **PEO4:** Graduates will practice ethics and have habit of continuous learning for their success in the chosen career.

PROGRAMME OUTCOMES (POs)

After the successful completion of the B.E. Electrical and Electronics Engineering degree Program, the students will be able to:

- **PO1 Engineering knowledge:** Apply knowledge of mathematics, natural science, computing, engineering fundamentals, and an engineering specialization to develop solutions to complex engineering problems.
- **PO2 Problem analysis:** Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions with consideration for sustainable development.
- **PO3 Design/development of solutions:** Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required.

- **PO4 Conduct investigations of complex problems:** Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions.
- **PO5 Engineering Tool Usage:** Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems.
- **PO6 The Engineer and The World:** Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework.
- **PO7 Ethics:** Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws.
- **PO8 Individual and Collaborative Team work:** Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.
- **PO9 Communication:** Communicate effectively and inclusively within the engineering community and society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations considering cultural, language, and learning differences.
- **PO10 Project management and finance:** Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one’s own work, as a member and leader in a team, and to manage projects and in multidisciplinary environments.
- **PO11 Life-long learning:** Recognize the need for, and have the preparation and ability for i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSOs)

The following are the Program Specific Outcomes of Engineering Students:

PSO 01: Power Systems Engineering

Apply comprehensive knowledge of electrical power systems to analyze, design and manage generation, transmission, and distribution networks, integrating emerging technologies and sustainable practices to contribute effectively to industry and societal needs.

PSO 02: Power Electronics and Drives

Design and develop efficient, reliable power electronic systems and motor drives with an emphasis on sustainable energy use, and inclusive technology solutions that address societal and environmental challenges.

PSO 03: Electronics and Instrumentation Engineering

Develop intelligent instrumentation and embedded systems for accurate measurements, monitoring and control in interdisciplinary domains addressing societal needs.

Abstract	POs Mapping
GSM module, Smart Security System, Password Verification, Remote Access, Two-Factor Authentication, Microcontroller, Real-Time Monitoring, Automation, IoT Security.	PO1, PO2, PO3, PO4, PO5, PO6, PO7, PO8, PO9, PO10, PO11, PSO1, PSO2, PSO3

SDG Goal		Mapping Justification
SDG 9	Industry, Innovation & Infrastructure	The project promotes innovative smart security infrastructure by integrating GSM technology, real-time authentication, and automated access control systems. It enhances reliability, modernization, and digital transformation in residential and industrial environments.

ABSTRACT

This project presents the design and development of a GSM-Based Smart Security System with Password Verification and Remote Access to address the increasing need for reliable and intelligent access control. The system employs a two-level authentication mechanism in which a user must first enter a valid password locally, after which an automatic SMS notification is sent to the authorized mobile number via a GSM module. The security lock is activated only upon receiving a confirmation reply from the registered user, ensuring that access decisions are made remotely and securely. A microcontroller coordinates password processing, GSM communication, and relay-driven solenoid lock operation, while also generating alerts for invalid entries and unauthorized attempts. This integrated approach enhances security by combining local verification, remote authorization, and real-time communication. Compared to traditional lock systems, the proposed solution offers improved safety, user flexibility, tamper resistance, and the ability to monitor and control access from any location. Due to its low cost, high reliability, and ease of implementation, the system is well suited for homes, offices, laboratories, and other restricted zones requiring enhanced smart security.

TABLE OF CONTENTS

LIST OF ABBREVIATION

S.No	ABREVIATION	EXPANSION
1	GSM	Global System for Mobile Communication
2	SMS	Short Message Service
3	LCD	Liquid Crystal Display

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

In today’s world, ensuring the safety of homes, offices, and restricted areas has become increasingly important due to the rise in unauthorized access and security breaches. Traditional mechanical locks and simple password-based systems are no longer sufficient, as they lack real-time monitoring and remote control features. To overcome these limitations, modern access control has shifted towards intelligent, communication-enabled solutions. This project introduces a GSM-Based Smart Security System that provides enhanced protection through a dual-level authentication process. The system first verifies a user through a local password and then sends an SMS notification to the registered mobile number for remote confirmation. The authorized user can reply to the message to open or close access, enabling complete control even from distant locations. By integrating microcontroller-based processing with GSM communication, the system ensures high reliability, flexibility, and user convenience. Its cost-effective design and compatibility with various environments make it an efficient solution for residential, commercial, and industrial security needs.

1.2 Objective

The need for a GSM-Based Smart Security System with Password Verification and Remote Access arises from the growing challenges faced by traditional locking mechanisms and basic electronic security methods. Mechanical locks can be easily duplicated, tampered with, or destroyed, while standalone password systems offer limited protection and lack remote monitoring capabilities. With increasing incidents of theft, unauthorized entry, and property damage, users now demand security solutions that provide both real-time alerts and the ability to control access even when they are away from the premises. GSM technology addresses this requirement by enabling wide-area communication through SMS, ensuring that the user can receive notifications and send commands from any location with mobile network coverage. This enhances safety, improves response time, and minimizes the risk of intrusion. Additionally, the necessity for such a system is further emphasized by the growing trend toward smart automation, user convenience, and cost-effective security solutions suitable for homes, workplaces, and high-security environments.

1.3 Problem Statement

In recent years, the frequency of unauthorized access, theft, and intrusion incidents has significantly increased across residential buildings, commercial establishments, laboratories, storage units. Traditional security systems such as mechanical locks, simple electronic keypads, and standalone alarm units have become inadequate in addressing modern security requirements. These systems suffer from limitations such as the inability to verify the identity of the user, lack of remote monitoring, absence of real-time alerts, and vulnerability to physical tampering. Once a password or physical key is compromised, the entire system becomes unsafe, and immediate corrective actions are difficult without advanced communication or monitoring features. Most existing low-cost security systems operate in isolation and do not provide any mechanism for the owner to check or control the access attempts made in their absence. If an unauthorized person tries a random password or tampers with the lock, the owner receives no information. Similarly, when a valid user enters the correct password, traditional systems cannot confirm the identity to the actual owner, leaving a gap in authentication and accountability. This absence of multi- level verification increases security risks in sensitive areas such as laboratories, server rooms, workshops, and storage facilities containing valuable or hazardo.

Another critical issue with existing systems is the lack of remote accessibility. In many real-life situations, authorized users may need to grant access to visitors, technicians, or family members even when they are geographically far away. Conventional systems cannot support such a requirement, forcing users to remain physically present or share passwords, which compromises security. Additionally, continuous supervision is cumbersome and unsuitable for modern lifestyles, making the need for remote operation and communication unavoidable.The rise of smart technologies and high mobile penetration has created an opportunity to strengthen security systems using GSM communication. However, very few low-cost systems utilize GSM-based authentication to provide real-time owner confirmation before granting access. A system that combines password verification with GSM-enabled confirmation can significantly enhance security by ensuring that only the rightful owner can approve or deny access attempts.

There is also a lack of security systems that can maintain proper records of access attempts and failed login trials. In the event of suspicious activity, users cannot retrieve proof or logs to analyze the situation. A GSM-based system can overcome this by sending immediate notifications and creating time-stamped alerts for every event. This allows users to maintain better awareness, avoid unauthorized entry, and take preventive action when required.

Furthermore, many existing systems do not offer security redundancy. If the password system fails or someone obtains the password, access becomes unrestricted. A dual-layer security model—one layer with password entry and another with mobile authentication—provides an additional barrier against

intrusion. This layered approach is necessary to ensure that even if one layer is compromised, the second layer protects the system from unauthorized access.
To address these challenges, there is a clear need for a smart, low-cost, reliable, and user-friendly security solution that integrates password verification with GSM-based remote authorization. Such a system must automatically notify the owner during every access attempt, allow remote control of the locking mechanism through SMS, maintain log details, and enhance the safety of personal and professional environments. The system should operate effectively with minimum human intervention and provide real-time communication to ensure quick decision-making and improved security management.

The proposed GSM-based smart security system aims to fill the gap left by traditional and existing systems by introducing a two-level authentication method. This project addresses the urgent need for enhanced access control, real-time monitoring, and remote operation in modern security applications. By providing reliable communication, automated authentication, and improved user convenience, such a system is essential to meet the rising demand for safe, secure, and intelligent security infrastructure.

The proposed GSM-based smart security system aims to address the limitations found in existing access control methods by introducing a robust two-level authentication mechanism. This dual verification process security by ensuring that both local user input and remote authorization are validated before granting access. With the growing number of intrusion attempts and unauthorized entries, and remotely manageable security solutions has become more critical than ever. The system provides real-time monitoring through instant GSM communication, allowing users to stay informed about access attempts from any location. Automated authentication procedures reduce human error and eliminate the dependency on single-level physical security devices.

CHAPTER 2
LITERATURE SURVEY

1. Title : Secure door monitoring mechanism that integrated password verification

Year : 2021

Author: P. Ramesh et al

Ramesh and team introduced a secure door monitoring mechanism that integrated password verification, wrong-entry detection, and SMS-based user alerts.The authors stated that the greatest advantage of GSM-based systems is their independence from the internet, making them reliable in remote or disaster-prone regions. Their research stressed that multi-layer authentication prevents unauthorized individuals from manipulating security hardware. They concluded that remote SMS control provides flexibility for managing access without the need to be physically present at the location.

2. Title : Intelligent access control model using GSM and keypad authentication.

Year : 2021

Author: S. Choudhury & A. Banerjee

Choudhury and Banerjee designed an intelligent access control model using GSM and keypad authentication. The authors stated that user convenience is crucial in the adoption of modern security solutions. Their system allowed users to update passwords via SMS and receive intrusion alerts instantly. They argued that integrating GSM with embedded systems is an effective method for blending traditional access control with smart communication technology.

3. Title : Intelligent access control model using GSM and keypad authentication.

Year : 2021

Author : K. Narayanan et al

Narayanan and colleagues introduced a hybrid GSM-Bluetooth locking mechanism. The authors stated that while Bluetooth provides short-range communication, GSM bridges the gap by offering long-distance accessibility. Their model combines keypad-based password entry with mobile-controlled operations, ensuring that users can monitor and control their security system from any location. This dual-channel communication improves both convenience and responsiveness in real-time conditions.

4. Title : A smart security architecture using GSM and RFID technologies

Year : 2019

Author: J. Patel et al.

Patel and colleagues presented a smart security architecture using GSM and RFID technologies. The authors stated that a dual-authentication process dramatically reduces the chances of unauthorized access in workplaces, server rooms, and personal storage facilities. Their system used RFID for local access and GSM for remote confirmation, ensuring only legitimate users could permit entry. Additionally, the study reported that GSM-enabled alerts increased user awareness and facilitated rapid response to intrusion attempts. Patel's work demonstrated that two-factor security systems offer significant advantages over single-step validation systems.efficient and cost-effective GSM modules make remote security implementation practical for developing nations. Their model enabled users to send specific commands through SMS to unlock or re-lock the system. They observed that remote access helps maintain security even during emergencies, travel, or unexpected guest arrivals. Their study confirmed the importance of GSM in modernizing legacy security infrastructures.

5. Title : improving home automation and security solutions

Year : 2018

Author: Wang & P. Martins

Wang and Martins focused on improving home automation and security solutions using SMS-enabled microcontroller systems. The authors stated that users increasingly prefer systems that do not depend on internet connectivity, especially in rural or low-signal regions where Wi-Fi is unreliable. Their proposed model used a microcontroller and GSM module to validate user identity using a time-based one time password (OTP) and remote unlock commands. They documented that GSM authentication is more secure compared to RF-based or keypad-only systems because intercepted commands can still be verified by an additional password layer. Their study contributed an early foundation for two-level security systems combining local and remote mechanisms.

6. Title : traditional mechanical locking systems

Year : 2017

Author: A. Sharma et al

Sharma and his team emphasized that traditional mechanical locking systems are no longer capable of resisting modern intrusion techniques such as lock-picking, key duplication, and brute-force attacks. The authors stated that integrating GSM technology with embedded control mechanisms significantly enhances the security of access-controlled environments. Their work introduced a password-based entry system which, when validated locally, initiates an SMS alert to the owner. They highlighted that GSM networks provide wide coverage low operational cost, and high reliability for remote authentication.

CHAPTER 3
EXISTNG SYSTEM

3.1 INTRODUCTION

The existing security systems used in homes, offices, and restricted areas mainly rely on mechanical locks, RFID tags, or simple password-based electronic keypads. Mechanical locks provide only single-level physical security and are vulnerable to key duplication, lock picking, and physical damage. Once a key is lost or duplicated, unauthorized individuals can easily gain entry, making these systems unreliable for modern security needs. Similarly, RFID-based systems suffer from issues such as card cloning, signal interference, and dependency on physical tags, which can be misplaced or stolen.

Traditional electronic keypads also offer only a single-step authentication process: the user enters a password, and if it matches the stored value, the lock opens. This single-layer structure makes the system highly susceptible to shoulder surfing, brute-force attacks, password leakage, and misuse by unauthorized persons. Moreover, these systems do not provide any remote monitoring capability. The user must be physically present to operate the lock, and there is no mechanism to notify the owner during unauthorized access attempts. If an intruder repeatedly enters the wrong password, the system simply remains locked without alerting anyone.

3.2 Block Diagram

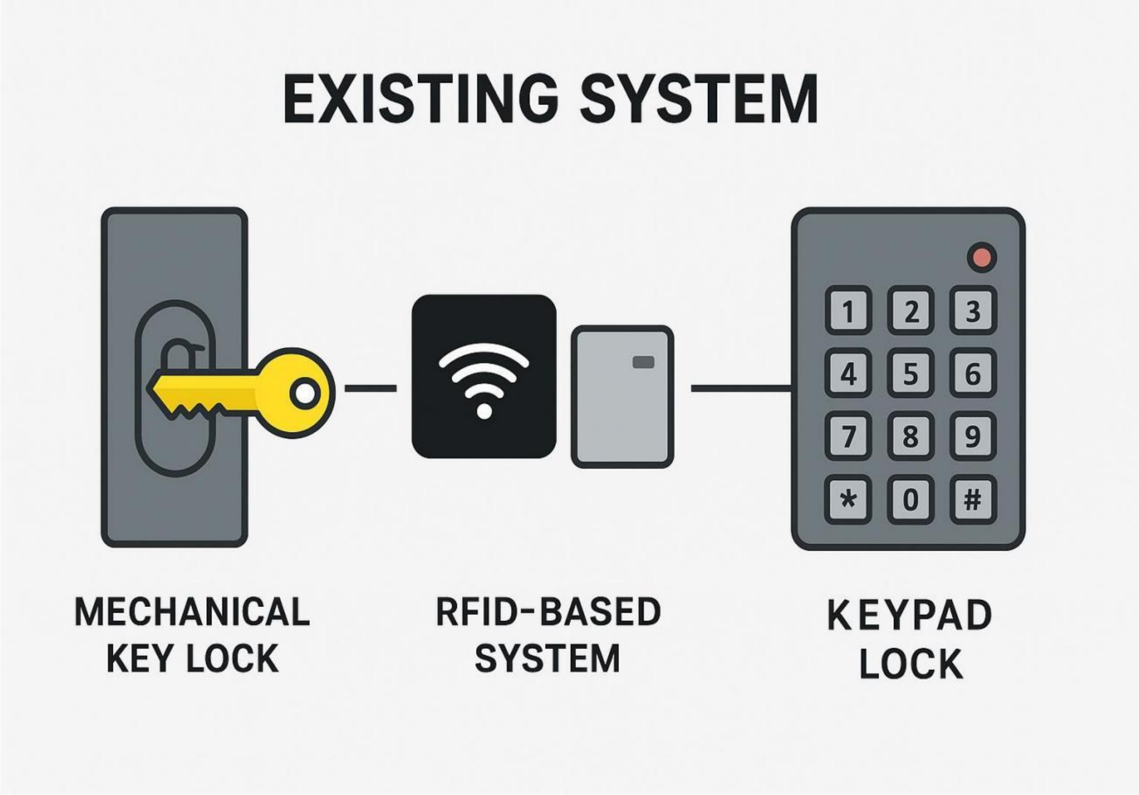


Figure 3.2 Block Diagram

3.3 Working of Existing System

a) Mechanical Lock-Based Systems

Mechanical locks are the most common and foundational security systems used in residential and commercial buildings. These systems operate based on a physical key mechanism, where a metal key with uniquely cut ridges is inserted into a lock cylinder. Inside the lock, multiple spring-loaded pins of varying lengths align at the shear line when the correct key is inserted, allowing the lock to open. If an invalid key is used, the pins do not align, and access is denied. In terms of functional behavior, authentication depends entirely on the physical presence of the key. There is no digital verification involved, and the system offers no support for remote access or monitoring.

Additionally, when several individuals require access, duplicate keys must be created for each user. Although simple and widely used, these systems rely solely on the security of a key, making them vulnerable in modern safety environments.

b) Password-Based Electronic Keypad Systems

Password-based electronic keypad systems introduce a basic electronic method for access control. Their working principle involves a user entering a password on a keypad, after which the microcontroller compares the entered value with a pre-stored password stored in memory. If the password matches, the microcontroller activates a relay or motor driver to unlock the door. If the password does not match, access is denied and the system remains locked. Functionally, these systems rely on single-factor authentication, where only the password determines access. Some models provide multiple attempts before temporarily disabling the keypad, but they still lack advanced security features. Since users must remember and enter a password manually, the system becomes vulnerable to observation, misuse, and attacks that exploit password weaknesses.

c) RFID Tag-Based Access Systems

RFID tag-based systems gained popularity due to their convenience and level of automation. In these systems, the user carries an RFID card containing a unique identification code stored within an embedded chip. When the card is brought near the RFID reader, radio waves power the tag (particularly in passive RFID systems) and extract the identification code. The reader then compares the received ID with its database of authorized users to determine whether access should be granted. If the ID matches the stored information, the relay activates to unlock the door; otherwise, access is denied. Functionally, authentication is based solely on the RFID tag, making the process quick, contactless, and easy for the user. However, like other traditional systems, reliance on physical tags introduces limitations regarding security, loss, and unauthorized usage.

3.4 Drawbacks

a) Mechanical Lock-Based Systems

Mechanical lock-based systems face several limitations that reduce their effectiveness in modern security applications. One of the major issues is key duplication, as keys can be easily copied at local shops or using digital key-cutting machines, and even high-security keys can be replicated using advanced 3D printing techniques. These locks are also vulnerable to lock picking and physical tampering, where methods such as lock bumping, picking, drilling, or forceful entry can silently compromise the lock. Another drawback is the complete dependence on physical keys; losing a key results in an immediate breach of security, and users must carry keys at all times, which is both inconvenient and risky. Additionally, mechanical locks provide no activity monitoring, meaning there is no record of who accessed the premises, and no alerts are generated during unauthorized attempts or forceful break-ins, making them inadequate for environments requiring real-time security awareness.

b) RFID-Based Access Systems

RFID-based systems, despite offering convenience, present multiple limitations. One major issue is card cloning and skimming, as RFID tags can be wirelessly scanned and duplicated using inexpensive tools, allowing attackers to create unauthorized copies without physical contact. The loss or theft of an RFID card also poses a significant risk because anyone in possession of the card can easily access the secured area. RFID systems are also prone to signal interference; dust, metal surfaces, and electromagnetic disturbances can reduce the system’s reliability and performance. Another drawback is the reliance on physical cards, which users must carry with them, and misplacing the card can lead to immediate denial of access.

Moreover, these systems offer no real-time alerts, meaning they operate locally and do not notify the owner during unauthorized access attempts or suspicious activity.

c) Password-Based Electronic Keypad Systems

Password-based electronic keypad systems also come with several significant limitations. A major drawback is that they rely on single-level authentication, meaning only a password is required to unlock the door; if this password is leaked, anyone can gain access. These systems are also vulnerable to shoulder surfing attacks, where an unauthorized person may observe the user entering the password. In addition, brute-force attempts, where an intruder repeatedly tries different passwords, may eventually succeed if the system does not have strict attempt limits. Password sharing or misuse is also common, as users often share passwords with others, compromising security. Furthermore, passwords are typically easy to remember but also easy to guess. These systems lack remote monitoring capabilities, preventing owners from controlling or tracking access from a distance, and even multiple incorrect attempts do not trigger any alerts. Additionally, they do not include intrusion detection features, meaning the system does not notify the user when tampering occurs at the keypad.

CHAPTER 4

PROPOSED SYSTEM

4.1 Introduction

The proposed GSM-Based Smart Security System with Password Verification and Remote Access is designed to overcome the limitations of conventional mechanical and single-layer electronic locking methods. Traditional systems rely solely on physical keys or local password entry, making them highly vulnerable to key duplication, password leakage, physical attacks, and the inability to monitor access remotely. To address these challenges, the proposed system introduces a dual-layer authentication mechanism that integrates both local password verification and remote authorization via GSM communication. When a user enters a valid password using the keypad, the microcontroller verifies it and immediately sends an SMS notification to the authorized mobile number. Only upon receiving a correct response command—such as "OPEN" or "CLOSE"—will the system activate the relay driver to control the locking mechanism. This ensures that even if the password is compromised, access cannot be granted without mobile confirmation.

The proposed system offers several advanced features, including real-time monitoring, remote control, tamper resistance, and fail-safe operation. By leveraging GSM technology, the system eliminates the need for internet connectivity, making it suitable for homes, offices, banks, lockers, laboratories, and industrial access zones in both urban and rural environments. The architecture is modular, allowing easy integration of future enhancements such as biometric modules, RFID readers, IoT dashboards, and smartphone apps. Overall, the proposed system enhances security, convenience, and operational reliability, delivering a modern and robust solution for controlled access environments.

4.2 Block Diagram

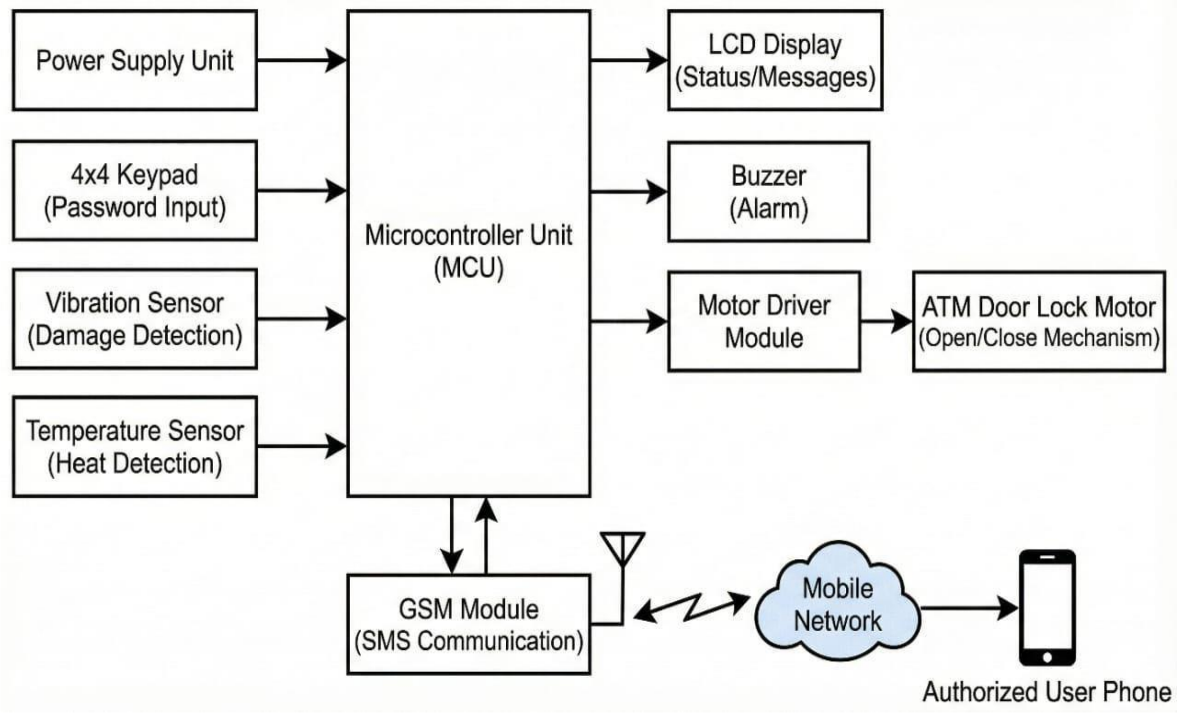

Power Supply Unit
4x4 Keypad (Password Input)
Vibration Sensor (Damage Detection)
Temperature Sensor (Heat Detection)
Microcontroller Unit (MCU)
LCD Display (Status/Messages)
Buzzer (Alarm)
Motor Driver Module
ATM Door Lock Motor (Open/Close Mechanism)
GSM Module (SMS Communication)
Mobile Network
Authorized User Phone

Figure 4.2 Block diagram of the proposed system

4.3 Working of Project Model

The GSM-Based Smart Security System operates through a dual-layer security mechanism designed to provide strong protection against unauthorized access while ensuring convenient and reliable user operation. The entire working process is divided into several stages, starting from password entry to GSM-based remote authorization and final lock operation. Each module in the system—keypad, microcontroller, LCD, GSM module, and relay-operated door lock—performs a coordinated function to ensure accurate authentication, real-time monitoring, and secure access control. The following sections describe the step-by-step working of the proposed model in detail.

a) Local Password Authentication

The working sequence begins when a user approaches the secured area and enters a numeric password using the keypad module. The keypad is connected to the microcontroller through a matrix of rows and columns, enabling efficient key scanning. Each keypress is detected, debounced, and sent to the microcontroller for processing.

The entered digits are displayed on the LCD screen (either masked as "****" or displayed as numbers), allowing the user to verify input accuracy.
The microcontroller compares the entered password with the pre-stored password located in EEPROM or internal memory.

- If the password is incorrect, the system immediately denies access, updates the LCD with a message such as "INVALID PASSWORD," and may optionally activate a buzzer for alerting nearby security.
- If the password is correct, the system proceeds to the second authentication.

b) Triggering GSM Notification to the Authorized User

Upon successful password verification, the microcontroller automatically sends a notification SMS to the registered mobile number of the system owner. This SMS typically contains information such as:

- Password matched
- Access attempt detected
- Request for confirmation

The GSM module operates using standard AT commands sent by the microcontroller through a serial communication interface (UART). Command AT+CMGS is used to set the message format, send SMS, and check signal strength.

The purpose of this notification is to ensure that the owner is immediately informed whenever someone attempts to access the system. This notification step also prevents unauthorized entry even if the password has been leaked, as the second confirmation is mandatory for access.

c) Remote Authorization Through SMS Commands

After receiving the alert, the authorized owner replies with a specific SMS command. The system supports simple, clear commands such as:

- "OPEN" – to unlock the door
- "CLOSE" – to keep the door locked

When the GSM module receives the SMS reply, it forwards the message to the microcontroller. The controller reads the incoming message stored in the GSM buffer using AT command AT+CMGR and extracts the user's command.

This SMS-based control ensures remote monitoring and decision-making, making the system operational even when the owner is away.

d) Decision Processing and Safety Validation

Once the SMS command is received and decoded, the microcontroller processes the instruction and determines whether to grant or deny access. The system includes internal safety checks to prevent malicious operations such as repeated incorrect commands or spoofed messages. These safety mechanisms may include:

- Checking sender’s mobile number
- Verifying the command format
- Avoiding duplicate commands
- Maintaining system logs

Only after passing these validations does the system proceed to the physical lock control stage. This ensures that the system remains robust against SIM spoofing, unauthorized messages, or system misuse.

e) Relay Activation and Door Lock Operation

The final decision is executed through a relay driver circuit that controls the solenoid lock.

- If the command is “OPEN”, the microcontroller energizes the relay coil, allowing current to flow to the solenoid lock, causing it to open.
- If the command is “CLOSE”, the relay remains inactive, keeping the lock engaged and preventing any access.

The relay driver acts as an interface between the low-power microcontroller pin and the high-power solenoid lock. It ensures electrical isolation and protects the microcontroller from voltage spikes. During lock operation, the LCD simultaneously shows status messages such as “DOOR OPENED” or “ACCESS REJECTED” helping users understand the system’s current state.

f) Status Update and System Reset

After performing the lock action, the system sends a confirmation SMS back to the owner, indicating the final outcome of the operation. Examples include:

- “Door successfully opened.”
- “Access request denied.”
- “Unauthorized attempt detected.”

This closing message ensures that the owner remains informed about all security activities.The system then resets automatically and returns to its initial idle mode, ready to accept a new password input. The reset mechanism clears temporary variables, buffers, and counters to ensure smooth operation without residual errors.

g) Security Advantages of the Working Model

The dual-layer working principle of the system—combining local password verification with remote GSM authorization—offers multiple advantages:

- Unauthorized users cannot access the system even if they guess or obtain the password.
- Real-time alerts prevent unnoticed access attempts.
- Remote SMS control ensures convenience and enhanced decision-making.
- The system provides a complete audit trail through message logs.
- Relay-controlled locking ensures strong physical security.

This combination of hardware reliability and GSM communication makes the system highly suitable for homes, offices, laboratories, ATMs, and industrial units requiring secure and monitored access.

CHAPTER 5

HARDWARE IMPLEMENTATION

5.1 Hardware Implementation

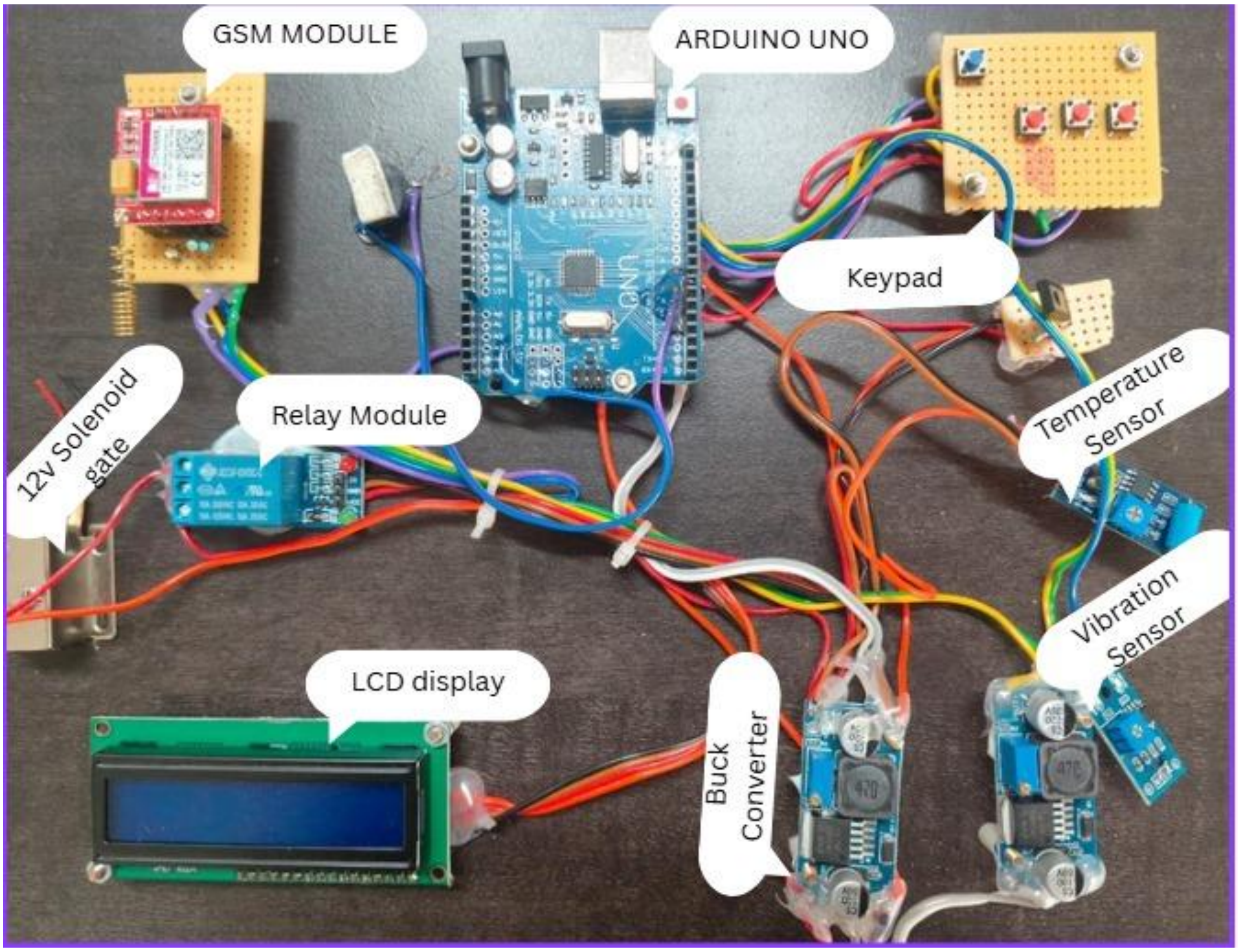


Figure 5.1 Hardware Implementation

5.2 Components Description

a) Microcontroller (Arduino)

The microcontroller acts as the central processing unit of the entire security system. It receives inputs from the keypad, processes the password, communicates with the GSM module, controls the relay, and updates the LCD display. The microcontroller also stores the predefined password in its memory and executes decision-making algorithms. Its GPIO pins are used for interfacing with external peripherals such as relays, LCD, and keypad.

b) 4x4 Keypad

The keypad serves as the primary input device through which the user enters the password. It is arranged in a matrix form with rows and columns. When a user presses a key, the microcontroller scans the matrix to identify the pressed button. The keypad provides a simple and effective method for local authentication.

c) GSM Module (SIM800L)

The GSM module is responsible for communication between the security attempted and receives SMS commands (such as OPEN or CLOSE) for card with network coverage. It ensures remote monitoring and control from any location.

d) 16x2 LCD Display

The LCD screen provides real-time feedback to the user. It displays messages such as:

"ENTER PASSWORD"
"CORRECT PASSWORD"
"PASSWORD INCORRECT"
"VIBRATION ALERT"
"FIRE ALERT"

The display helps users understand the system status during operation. It is driven by the microcontroller using either 8-bit mode.

e) Solenoid Lock

The solenoid lock acts as the physical locking mechanism. It receives power through the relay and opens or closes based on user authorization. When energized, the electromagnetic field inside the lock pulls the plunger, unlocking the door. When power is removed, the lock returns to its secure closed state.

f) Power Supply Module

The power supply unit converts AC supply or external DC supply into a regulated voltage suitable for the microcontroller and GSM module.

A typical setup includes:

12V adapter for the relay and lock.

5V regulated supply (using 7805 IC) for the microcontroller and LCD Separate filtering capacitors and protection diodes.

A stable power supply is essential for reliable GSM communication.

g) SIM Card

A functional SIM card is required inside the GSM module to enable SMS sending and receiving. The SIM card must be activated and have sufficient network coverage. Prepaid or postpaid connections can be used.

h) Buzzer

The buzzer can be used to alert the user in case of:

Wrong password attempts.

Unauthorized access System errors.

It adds an additional layer of security and user awareness.

CHAPTER 6

RESULT AND DISCUSSION

6.1 Hardware Output

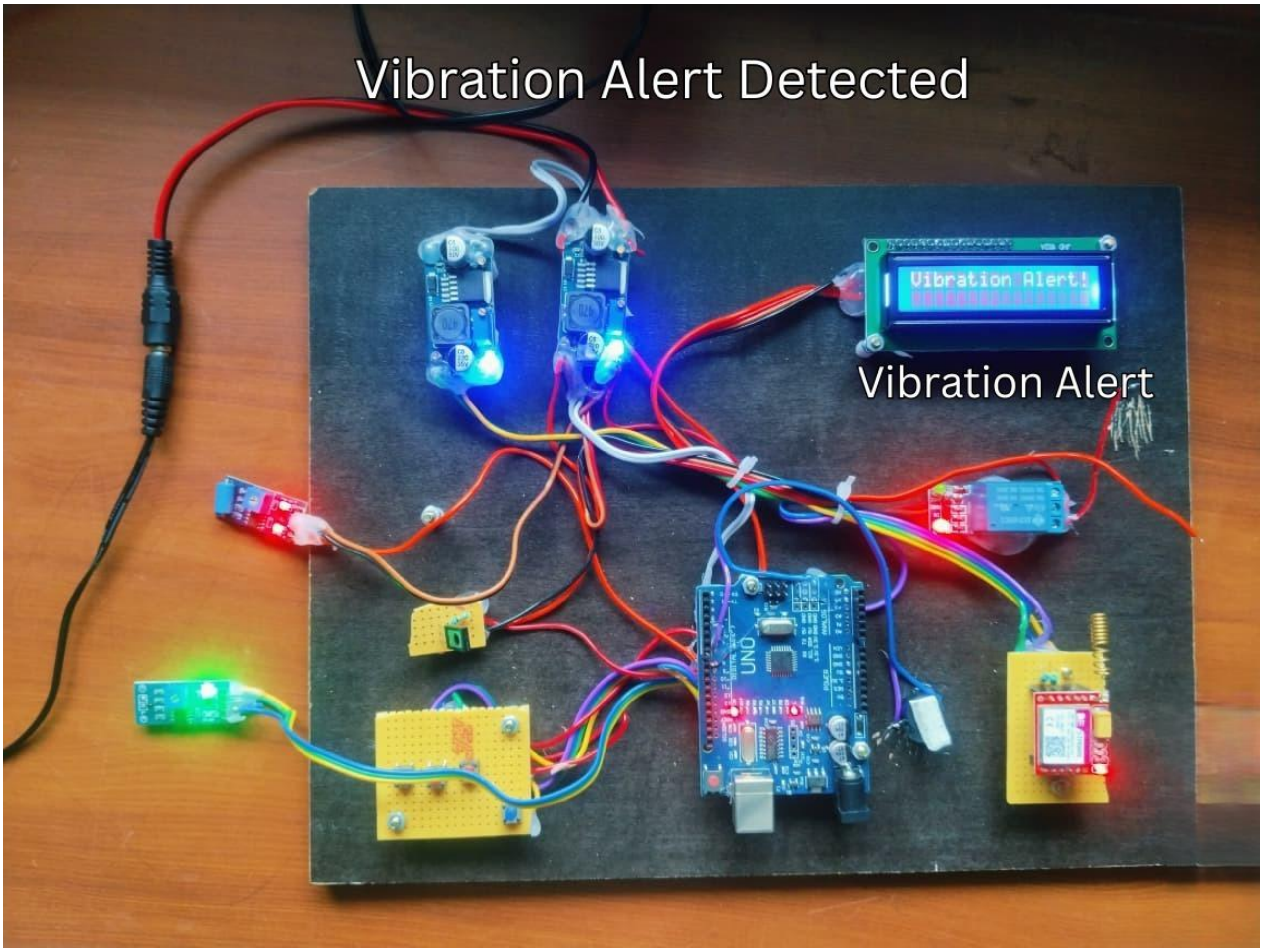


Figure 6.1 Hardware Output

6.2 Discussion

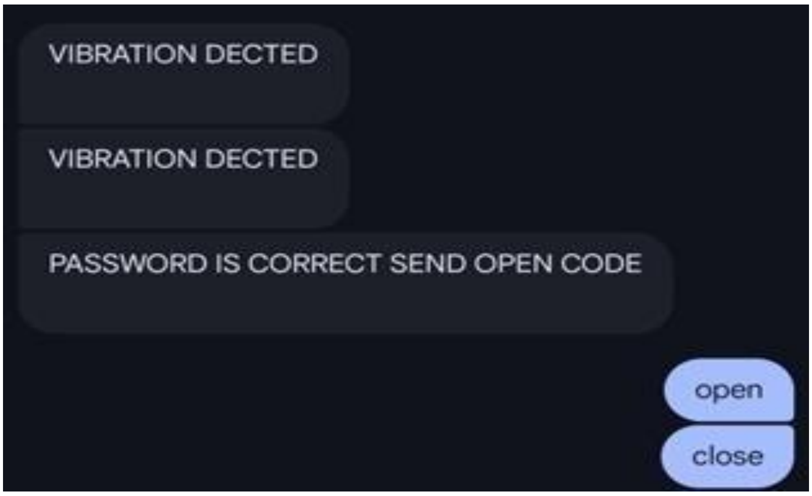
The proposed GSM-based smart security system was implemented using an Arduino Uno, 4-button keypad, SIM800L GSM module, LCD display, vibration and temperature sensors, and a 12-V solenoid lock. The developed prototype was tested under different conditions to evaluate password accuracy, sensor performance, and remote-control reliability.

During regular operation, the LCD displayed “Enter Password”, indicating readiness for user input. When the correct password was entered, the GSM module instantly sent an SMS: “Password Is Correct Send Open Code”. Upon receiving the command “open” from the authorized user, the relay activated the solenoid lock and granted access. Sending “close” successfully re-locked the cabinet. These tests confirm that GSM-based remote control is fast, responsive, and reliable for real-time access management. The vibration sensor was tested by applying mechanical taps on the cabinet surface. The system correctly detected vibration and displayed “Vibration Alert” on the LCD while simultaneously sending an SMS: “Vibration Detected”. This dual-alert mechanism enhances security by immediately informing the user of any physical tampering attempt. The temperature sensor also performed accurately, displaying real-time temperature readings. Although not used for alerts in this prototype, it can be extended for fire or overheating warnings in future versions.

Overall system performance was stable, with a small delay of about 3–5 seconds between sensor activation and GSM message delivery, mainly due to network conditions. The solenoid lock operated smoothly, and the relay provided safe electrical isolation between control and actuation. All components functioned simultaneously without electromagnetic interference.

Compared to conventional keypad-based locks, the proposed system offers higher security through multi-level authentication, sensor-based intrusion detection, and GSM-enabled remote monitoring. The LCD interface ensures clear feedback, making the prototype suitable for home cabinets, office lockers, laboratory storage, and small industrial units.

6.3 Software Output



VIBRATION DECTED

VIBRATION DECTED

PASSWORD IS CORRECT SEND OPEN CODE

Figure 6.3 Software Output

6.4 Discussion

The software output of the GSM-Based Smart Security System demonstrates the correct functioning of both the security alert mechanism and the remote access control feature. As shown in the output screen, the system first detects abnormal physical activity near the door, such as shaking or forced entry attempts. When the vibration sensor is triggered, the microcontroller immediately sends an alert message to the registered mobile number. This behavior is visible in the repeated message “VIBRATION DETECTED”, confirming that the intrusion detection module is active and responding in real time. This ensures that the user is instantly notified of any suspicious movement, even before the intruder attempts to enter the password panel.

After a legitimate user enters the correct password on the keypad, the system validates it and sends a confirmation message: “PASSWORD IS CORRECT SEND OPEN CODE”. This output proves that the software correctly executes the first level of authentication. Instead of unlocking the door immediately, the system waits for remote authorization, enabling a safer two-step verification process.In the same output screen, the options “open” and “close” indicate the commands available to the authorized user. When the user replies with “open,” the microcontroller activates the relay driver to unlock the door. If the user replies “close,” the system keeps the door locked. These responses confirm that the GSM module successfully receives and interprets incoming SMS commands, demonstrating effective bidirectional communication.

CHAPTER 7
CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

The GSM-based smart security system developed in this project successfully demonstrates an efficient, reliable, and modern approach to secure access control. By integrating two-level authentication—local password verification and remote mobile confirmation—the system significantly enhances safety compared to traditional single-level locking mechanisms. The microcontroller effectively coordinates all hardware components, including the keypad, GSM module, relay driver, and solenoid lock, enabling seamless interaction and accurate decision-making. The GSM communication feature allows real-time monitoring and remote authorization, ensuring that only the registered user can grant access even when they are not physically present.

The system provides a cost-effective solution using readily available components while maintaining high reliability and operational accuracy. Its modular design makes it easy to expand with additional features such as fire detection, intrusion alerts, or internet-based monitoring in the future. The hardware prototype performed consistently during testing, showing minimal delay in message transmission and precise lock operation. Overall, the project demonstrates the effectiveness of GSM communication technology in enhancing security and provides a robust platform for implementing intelligent access control systems in homes, offices, and industries.

7.2 Future Scope

The GSM-based smart security system developed in this project has significant potential for future improvement and expansion. With advancements in communication technologies, the system can be upgraded from SMS-based control to internet-based monitoring using Wi-Fi or IoT platforms such as Blynk, MQTT, or Firebase. This would allow real-time notifications, remote dashboard access, and enhanced monitoring capabilities. Additionally, the system can be integrated with biometric authentication methods such as fingerprint, RFID, or facial recognition to further strengthen the security levels and eliminate dependency on passwords alone. Future versions of the system can incorporate advanced sensors including PIR motion detectors, fire sensors, gas leak sensors, and camera modules to transform the setup into a complete smart home security network. The use of artificial intelligence for intrusion detection and pattern recognition can also be explored to provide predictive security alerts. Solar-powered operation and battery backup systems can make the device more reliable during power failures. Furthermore, cloud storage can be implemented to maintain logs of access attempts, user activities, and event histories.

Overall, there is immense scope for enhancing the project by adopting modern communication protocols, improving automation, and expanding the system into a fully scalable, intelligent security solution suitable for residential, commercial, and industrial applications.

REFERENCES

[1] A. Kumar and S. Thomas, “Design and Implementation of GSM Based Home Security System,” International Journal of Engineering Research and Technology (IJERT), vol. 4, no. 6, pp. 112–116, 2017.

[2] P. Verma and J. Singhai, “GSM Based Security System,” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, no. 7, pp. 2910–2914, 2016.

[3] S. R. Bharathi and K. Prakash, “Microcontroller Based Door Lock Security System Using GSM Technology,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, no. 9, pp. 178– 183, 2018.

[4] M. A. Mazidi, R. McKinlay and D. Causey, PIC Microcontroller and Embedded Systems, Pearson Education, 2008.

[5] SIMCom Wireless Solutions, “SIM900 AT Command Manual,” SIMCom, 2015. [Online]. Available: https://simcom documentation (use original source in real report).

[6] A. Tiwari, “Solenoid Lock Control Using Microcontroller,” International Journal of Electronics and Communication Engineering, vol. 7, no. 3, pp. 101–105, 2019.

[7] N. Sridhar and P. Arun, “Implementation of Two-Level Authentication for Secure Door Access,” Proceedings of the IEEE International Conference on Communication and Signal Processing (ICCSP), 2020, pp.

[8] Texas Instruments, “Voltage Regulator Datasheet (7805/7812 Series),” TI Documentation, 2019.

[9] A. Jain and A. Sharma, “IoT and GSM Based Integrated Security System,” International Journal of Computer Applications, vol. 175, no. 22, pp. 25–29, 2020.

10] A. K. Singh, “GSM–Based Remote Monitoring and Control Systems: A Review,” International Journal of Scientific Research in Electronics and Communication Engineering, vol. 8, no. 4, pp. 45–52, 2021.