ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement ground my efforts with success.

We consider it as a privilege to express our gratitude and respect to all those who guided me in completion of project work.

We will remain indebted forever to all the **Management Authorities of SJM Vidyapeetha(R), Sri Bruhanmatha, Chitradurga** and support for carrying out this project work successfully.

We extend our sincere and heart full thanks to **Dr. Bharath P B Ph.D., Principal,** and **Dr. Siddesh K B M.Tech.,Ph.D, HOD, Department of Electronics and communication Engineering** for providing me the right ambience, constant inspiration and support for carrying out this project work successfully.

We wish to express thanks to the Project Coordinator **Prof. Roopa S,** Assistant Professor, **Department of Electronics and communication Engineering**, for her guidance, invaluable help, advice and suggestions.

We profoundly indebted to my Project work guide**, Prof. Farzana Parveen B A , Asst. Professor Department of Electronics and communication Engineering**, for innumerable acts of timely advice, encouragement and I sincerely express my gratitude to her.

We express our enormous pleasure and thankfulness to all teaching and non-teaching staff of the **Department of Electronics and communication Engineering.**

NAME :	**USN NO:**
CHANDAN M L	**4SM22EC404**
CHANDANA U	**4SM22EC405**
KARTHIK N	**4SM22EC410**
PRIYANKA N	**4SM22EC419**

ABSTRACT

In the digital age, public mobile charging has become a necessity, especially in areas like transportation hubs, educational institutions, and public spaces. However, unsecured charging points pose risks such as device theft and unauthorized access. This project proposes a Secure Smart Mobile Charging System that ensures safe and user-authenticated mobile charging through biometric verification and coin-based access.

Built on the ESP32 DevKit V1 platform, the system integrates a coin acceptor, fingerprint sensor, and servo-operated locker to grant secure access. Once a coin is inserted, the system prompts the user for fingerprint enrollment. Upon successful verification, the locker opens, allowing the user to place their device for charging. The charging process is monitored and controlled using a **relay**, and the duration is time-limited. If the device remains uncollected after the charging period, a buzzer alert is triggered, and the system waits for fingerprint re-verification to release the device.

An I2C LCD provides real-time status updates, ensuring user awareness throughout the process. This system enhances public charging security, minimizes the risk of device theft, and introduces a smart, self-sustained solution for public mobile charging with minimal human intervention.

CONTENTS

ACKNOWLEDGEMENT
ABSTRACT

Chapter No	CHAPTER NAME	Page No
1	**INTRODUCTION**	1
1.1	Objective	2-3
1.2	Problem statement	3
1.3	Motivation	4
1.4	Existing System	4-5
1.5	Proposed System	5
2	**LITERATURE SURVEY**	6
3	**METHODOLOGY**	7
3.1	Block Diagram	7-9
3.2	Hardware and Software Requirments	10-17
3.3	Activity Diagram	18-19
4	**ADVANTAGE & DISADVANTAGES**	20-21
4.2	Limitations	21
4.3	Applications	22
5	**RESULT AND DISCUSSION**	23-28
6	**CONCLUSION**	29
	FUTURE ENHANCEMENT	30
	REFERENCES	31
	APPENDIXCODE	32-35

CHAPTER 1

INTRODUCTION

With the exponential rise in the use of smartphones and other portable electronic devices, the demand for public charging stations has significantly increased. In places such as railway stations, airports, colleges, and bus terminals, users often find themselves in need of quick and secure charging options. However, most public charging systems today lack essential features such as safety, authentication, and user accountability. Incidents of mobile theft, unauthorized device access, and misuse of public charging facilities are becoming increasingly common, raising serious concerns about device security and user trust.

Traditional public charging kiosks often offer open ports without any form of locking or access control, making it risky for users to leave their devices unattended. This problem calls for a smart, secure, and user-authenticated solution that not only charges the device but also ensures its safety during the entire charging process. To address this issue, this project proposes a Secure Smart Mobile Charging System that integrates biometric authentication using a fingerprint sensor along with a coin-based access mechanism.

The system is designed to offer a user-friendly interface through an LCD screen and provides audible alerts via a buzzer to notify users of successful authentication, charging status, and completion. A servo motor-controlled locker secures the mobile device during the charging session, while relay modules manage the switching of the charging circuit and the coin acceptor. Once the user inserts a coin and successfully enrolls or verifies their fingerprint, the locker opens for the user to place their mobile device, and charging begins. Only the authenticated fingerprint can unlock the locker to retrieve the device, thus ensuring security.

This project aims to deliver a cost-effective, scalable, and intelligent mobile charging solution that can be deployed in various public locations, enhancing both security and convenience for users. Through the integration of automation, biometric verification, and real-time feedback, this system represents a significant step towards improving public infrastructure in the digital age.

1.1 OBJECTIVE

The primary objective of this project is to design a Secure Smart Mobile Charging System that ensures safe and reliable charging of mobile devices in public spaces. It addresses issues like device theft, unauthorized access, and lack of user authentication in conventional public chargers. The system integrates fingerprint-based biometric authentication, allowing only the rightful user to access their device after charging. A coin-operated mechanism regulates usage, enabling a pay-per-use model suitable for commercial deployment.

The project uses servo motors to control a secure locker and relays to manage power supply. Real-time status updates and alerts are provided via an LCD display and buzzer, enhancing user interaction. This solution aims to offer a secure, user-friendly, and efficient charging option for busy public locations such as stations, airports, and malls.

Detailed Objectives

1. Secure Mobile Charging

Ensuring a safe charging environment is crucial, especially in public spaces like offices, libraries, and campuses. The security aspect can be enhanced with locked charging compartments that prevent unauthorized access. These lockers can be reinforced with strong materials and tamper-proof mechanisms to safeguard devices while they charge.

2. Automated Access Control

Fingerprint authentication provides a seamless yet highly secure way for users to retrieve their devices. The system can store authorized fingerprints and match them against users attempting access. This minimizes security risks and prevents device theft or unauthorized usage. Biometric authentication ensures that only rightful owners can access their phones once placed in the charging station.

3. Efficient Energy Management

Overcharging can reduce battery life and lead to excessive power consumption. An automated energy management system monitors each device’s charge level and disconnects power once optimal charge is reached. Smart algorithms can also distribute power effectively across multiple devices to balance energy usage and prevent unnecessary electricity waste.

4. User-Friendly Interface

An LCD screen integrated into the charging station can display useful information such as charge percentage, estimated time for full charge, and system alerts. Users can interact with the display to check the status of their devices. Visual and audible notifications can inform users when their phone is fully charged or ready for retrieval, enhancing convenience.

5. Enhanced Device Safety

To prevent theft and misuse, the charging station locks devices until the authentication process confirms the rightful owner. In addition, anti-tamper alarms can notify authorities if an unauthorized access attempt is detected. Implementing unique authentication mechanisms, such as passwords or facial recognition alongside fingerprints, further strengthens security.

1.2 PROBLEM STATEMENT

With the growing dependence on mobile devices, public charging stations have become essential in places like airports, malls, and transit hubs. However, conventional charging points lack adequate security measures, making devices vulnerable to theft or unauthorized use. Users often leave their devices unattended while charging, exposing them to potential loss or tampering. Moreover, there is no effective method to authenticate users or restrict access to the charging unit once connected, leading to misuse and safety concerns. Additionally, most public charging systems operate without any usage regulation or payment mechanism, which limits their scalability and sustainability in commercial environments. These challenges highlight the need for a secure, user-friendly mobile charging system that not only safeguards devices but also controls access and enables a pay-per-use model. This project addresses these problems by integrating fingerprint biometric authentication, secure locking mechanisms, and controlled power supply, ensuring that only authorized users can access their devices after charging, thereby enhancing security and trust in public charging infrastructure.

1.3 MOTIVATION

1. **Public Convenience:** Provides a secure and reliable mobile charging solution in public places where users can easily access charging services by inserting coins.
2. **Simple Payment Method:** Uses a straightforward coin-based payment system, making it accessible to all users regardless of digital payment literacy or smartphone access.
3. **Revenue Generation:** Offers businesses, public facilities, and transport hubs a practical revenue stream through pay-per-use mobile charging services.
4. **Security Through Biometrics:** Implements fingerprint-based authentication to ensure that only authorized users can unlock and retrieve their devices, reducing theft and unauthorized access.
5. **Energy Efficiency:** Encourages responsible energy use by controlling charging sessions and incorporating energy-saving mechanisms.
6. **Smart Automation:** Automates the entire process—from coin validation, fingerprint enrollment and verification, to locker control and charging session management
7. **Scalability & Integration:** Designed for easy scaling across multiple locations, with potential for future integration with cloud-based monitoring and management systems.
8. **User-Friendly Interface:** Provides real-time feedback via LCD displays and buzzer alerts to guide users through payment, charging, and device retrieval processes smoothly.
9. **Enhanced User Trust:** Increases user confidence in public charging stations by securing devices and ensuring fair usage through automated control and biometric verification.

1.4 EXISTING SYSTEM

Most public mobile charging stations currently provide either free or paid charging services without any form of user authentication or device security. As a result, devices are often left unattended during charging, increasing the risk of theft or misuse. These systems lack user tracking or identification, making it difficult to hold anyone accountable in case of loss or damage.

Payment options are generally limited to cash, with no support for modern digital payment methods such as UPI. Additionally, many stations require manual operation or monitoring, which reduces operational efficiency and scalability. There are also no measures to handle user data privacy or implement security protocols, as these systems do not integrate user identity verification.

1.5 PROPOSED SYSTEM

The proposed system addresses these issues by incorporating biometric fingerprint authentication to ensure secure user identification before and after each charging session, preventing unauthorized access. The charging bays are designed to automatically lock during charging and only unlock upon successful re-authentication, securing users' devices effectively. Payment flexibility is enhanced by supporting both coin-based payments and UPI digital transactions, including a convenient "Pay Later" option for registered users. Time-based charging is accurately managed according to the amount paid, improving transparency and fairness. The system is fully automated, handling validation, door control, and session management with minimal human intervention. To ensure continuous operation, a solar panel and battery backup are integrated. Real-time notifications are displayed on an LCD to inform users about session status and remaining time. Additionally, the system includes an LED/OLED display to broadcast advertisements, safety alerts, and public awareness messages. Designed for scalability, the system can be deployed across multiple locations with network integration, allowing users to access accounts and transaction history securely.

CHAPTER 2

LITERATURE SURVEY

The development of secure and smart public charging systems has garnered significant attention due to the increasing use of mobile devices and the rising demand for accessible power sources in public areas. Conventional public charging kiosks typically allow open access without any user authentication or monitoring, which raises security concerns like device theft or unauthorized retrieval. Existing literature reveals that most traditional systems lack user identification, time-based charging control, and versatile payment options, thereby limiting their safety and scalability in busy environments.

Biometric authentication, particularly fingerprint recognition, has been extensively studied and successfully applied in access control systems. Research papers from IEEE and other reputed sources emphasize that fingerprint sensors provide an effective balance of affordability, security, and reliability. Their integration into public service points, such as charging stations, enhances accountability and prevents unauthorized use.

Coin-operated embedded systems have been widely used in vending machines and other public utilities due to their simplicity and cost-effectiveness. However, these systems often do not support smart features or accommodate users preferring digital payment options, limiting their applicability in modern contexts.

The rise of digital payment platforms, especially Unified Payments Interface (UPI), has opened new avenues for cashless transactions in public services. Studies demonstrate that integrating UPI via QR codes or account linking into IoT devices offers a seamless and flexible payment experience, contributing to financial inclusion.

Moreover, IoT-based smart charging systems equipped with sensors, cloud connectivity, and automation capabilities offer enhanced monitoring and user management. Combining biometric security with hybrid payment options further improves user trust, operational efficiency, and accountability. Current research also highlights the importance of local biometric data storage and compliance with data protection laws like GDPR to safeguard user privacy.

CHAPTER 3

METHODOLOGY

The methodology of this project involves a systematic approach to design, develop, and implement the secure smart mobile charging system. Initially, the hardware components such as the fingerprint sensor, coin acceptor, servo motor, and relays are interfaced with the microcontroller to ensure seamless communication. The biometric authentication process is integrated to provide secure access, while the payment mechanism is programmed to accept coins and validate sessions accordingly. Real-time status updates and alerts are managed through an LCD and buzzer for enhanced user interaction. Finally, the entire system is tested rigorously to ensure reliability, security, and user-friendliness in practical scenarios.

3.1 Block Diagram of Secure Smart Mobile Charging System

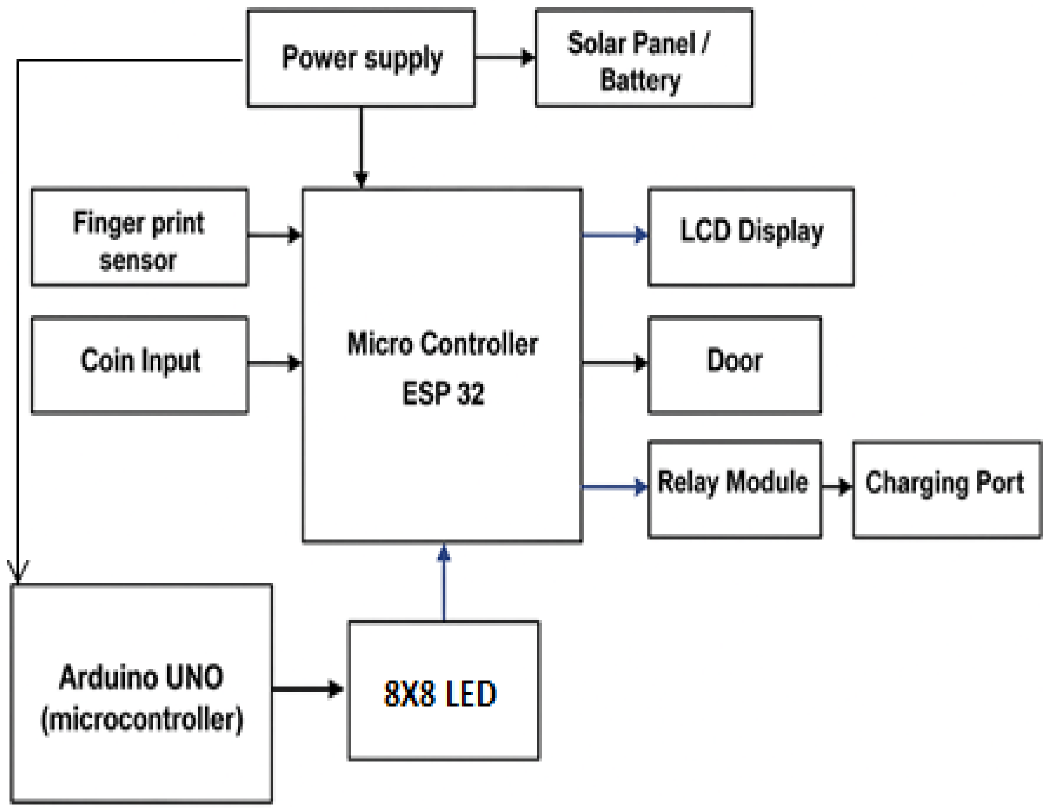

Figure 3.1: Block diagram of Secure Smart Mobile Charging System

The block diagram represents a smart access and payment-based system using an

ESP32 microcontroller. It receives power from a solar panel or battery and connects to various input components like a fingerprint sensor, coin input, online payment module, and buttons for authentication and payment.

The microcontroller controls output devices such as an LCD display, LED screen, door, relay module, and IoT module**,** enabling access control and device operation. The relay module manages the charging port, allowing users to charge devices after successful authentication. The IoT module enables remote monitoring and control, making the system suitable for smart access, vending, and charging applications.

1. **Microcontroller (ESP32):** The central processing unit of the system, responsible for managing inputs and outputs. It controls all the components based on received signals and executes programmed logic for authentication, payment processing, and device control.
2. **Power Supply (Solar Panel / Battery):** Provides the necessary electrical power to the ESP32 and connected peripherals. A solar panel or battery ensures uninterrupted operation, making the system energy-efficient and suitable for remote locations.
3. **Fingerprint Sensor:** Used for biometric authentication, allowing access to authorized users based on their stored fingerprint data.
4. **Coin Input:** A coin acceptor module that enables users to make payments by inserting coins, commonly used in vending machines, public charging stations, and similar applications.
5. **LCD Display**: A screen that shows real-time information, instructions, or status updates regarding the system, such as successful authentication or payment confirmation.
6. **Door:** Represents a controlled access mechanism that unlocks or opens when authentication is successful, commonly used in smart lockers or access control systems.
7. **Relay Module:** An electrical switch controlled by the ESP32, used to activate or deactivate external devices, such as the charging port or door lock.
8. **Charging Port:** An output device powered through the relay module, allowing users to charge electronic devices such as mobile phones or electric vehicles after successful authentication or payment.

9. **ArduinoUNO**

   The Arduino UNO is the microcontroller that acts as the brain of the system. It is responsible for:

   1. Storing predefined advertisement messages or text patterns
   2. Sending data signals to the LED matrix to display characters, animations, or scrolling messages
   3. Controlling the timing and brightness of the LED display

10. **8X8 Dot matrix LED Display**

    This is a grid of 64 LEDs arranged in 8 rows and 8 columns. It is used to display characters or symbols by selectively turning on specific LEDs. In this advertising application, it can:

    1. Scroll promotional messages (e.g., “SALE”, “50% OFF”, “WELCOME”)
    2. Display symbols or animations
    3. Cycle through multiple text ads

This system is ideal for automated access control, vending, and smart charging applications, integrating multiple authentication and payment methods for a seamless user experience.

3.2 HARDWARE AND SOFTWARE REQUIREMENT

SOFTWARE REQUIREMENTS

1. Embedded C
2. Arduino ide

HARDWARE COMPONENTS

3.2.1 ESP 32

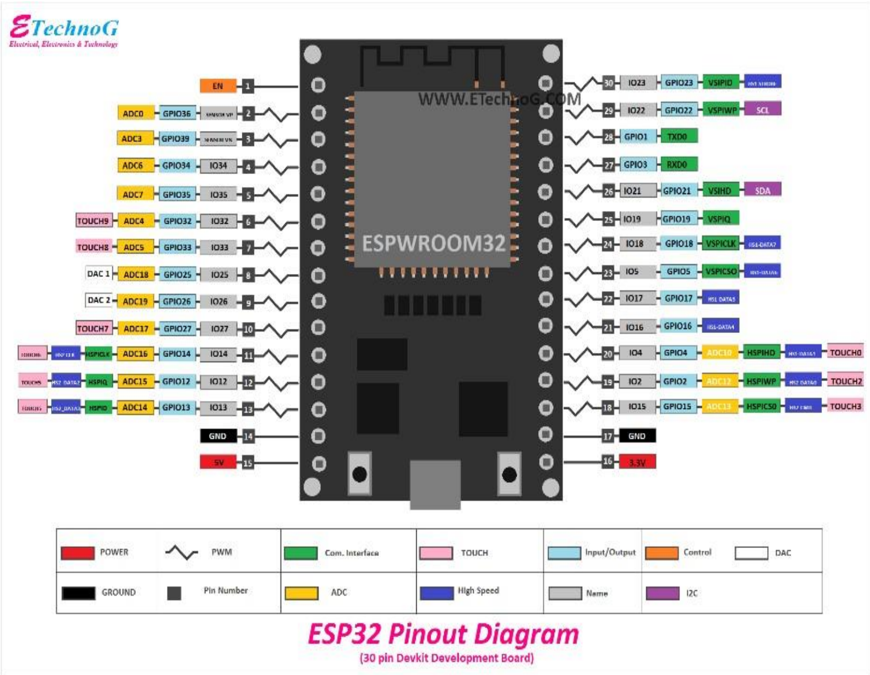

Figure 3.2: ESP32

The ESP32 is a powerful and versatile microcontroller developed by Espressif Systems, widely used in IoT applications due to its Wi-Fi and Bluetooth capabilities. It is based on a dual-core Tensilica LX6 processor with a clock speed of up to 240 MHz, making it suitable for real-time processing. The ESP32 features multiple GPIO pins, ADCs, DACs, PWM, UART, SPI, and I2C interfaces, allowing integration with various sensors and modules. It supports lowpower modes, making it ideal for battery-powered applications. Due to its built-in Wi-Fi and Bluetooth, the ESP32 is commonly used in home automation, smart devices, industrial IoT, and wireless communication projects.

The ESP32 also includes built-in secure boot and flash encryption, making it suitable for secure IoT applications. It supports Over-the-Air (OTA) updates, allowing remote firmware upgrades without physical access. With its high processing power, multiple connectivity options, and energy efficiency, the ESP32 is widely used in automation, robotics

Technical Specifications

- Microcontroller: ESP32-D0WDQ6 (dual-core Tensilica LX6)
- Operating Voltage: 3.3V
- Input Voltage (recommended): 5V via USB or 7-12V via VIN pin
- Input Voltage (limits): 3.0V to 3.6V on 3.3V pin (do not exceed)
- Digital I/O Pins: 34 GPIO pins (many support PWM, ADC, DAC, etc.)
- Analog Input Pins: 18 channels (ADC 12-bit resolution)
- Digital-to-Analog Converter (DAC): 2 channels (8-bit resolution)
- Flash Memory: 4 MB (varies by module)
- SRAM: 520 KB internal SRAM
- EEPROM: Emulated in flash (not true EEPROM)
- Wi-Fi: 802.11 b/g/n
- Bluetooth: v4.2 BR/EDR and BLE
- UART: 3 serial ports
- SPI: 4 SPI interfaces
- I2C: 2 I2C interfaces
- PWM Channels: Up to 16 channels available
- Max current per GPIO pin: 12mA (recommended max)
- Operating Temperature: -40°C to 85°C

3.2.2 COIN ACCEPTOR

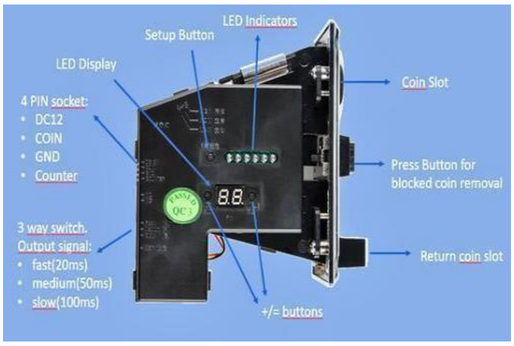

Figure 3.3: Coin acceptor

It detects and validates coins to initiate the charging process. It enhances user interaction by offering a simple and familiar payment method, ensuring ease of use. The Multi- Coin Acceptor, such as models CH-926 or RM5, is designed to support multiple coin types and denominations, providing convenience for users. Operating on a standard 12V DC supply, it ensures smooth and efficient functionality with low power consumption of approximately 60– 100mA, making it energy-efficient for continuous use.

3.2.3 BIOMETRIC SENSOR

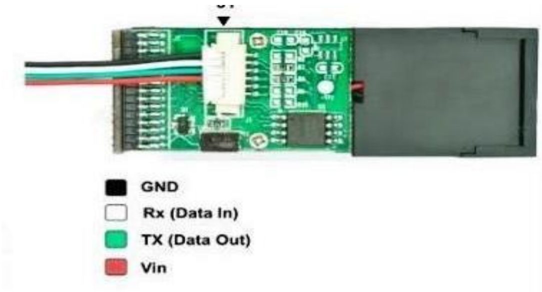

Figure 3.4: Biometric sensor

The fingerprint scanner ensures secure user authentication by scanning and verifying fingerprints for access to the charging bay, preventing unauthorized entry. It integrates seamlessly with Arduino for synchronized payment validation and bay automation while providing a fast, user-friendly authentication experience.The optical fingerprint scanner, such as the R307 or GT511C3, uses advanced optical imaging for reliable identification and operates on 3.3V–5V, ensuring compatibility with Arduino systems. With a UART interface, it supports seamless data exchange and can store 120–1000 fingerprints, making it ideal for public systems its compact design (~28mm x 28mm x 15mm) easily fits into system enclosures.

3.2.4 LCD DISPLAY

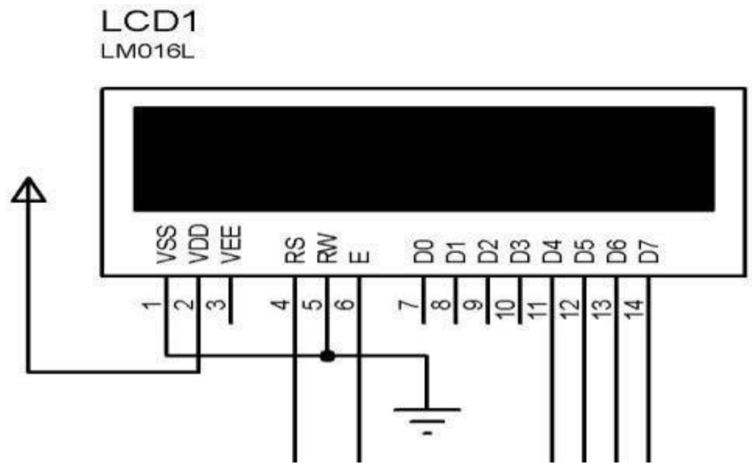

Figure 3.5: LCD display

The LCD display in the Coin & UPI-Based Mobile Charger provides real-time guidance with instructions like “Insert Coin” or “Payment Received,” displays charging status and remaining time, and issues error notifications for invalid payments or system issues. The 16x2 alphanumeric LCD, compatible with HD44780, supports up to 16 characters per line on two rows, offering clear text-based feedback with a 5x8 dot character font. Operating at 4.7V–5.3V with low power consumption (~1–2mA), it interfaces efficiently with Arduino via a parallel communication mode and features an LED backlight for visibility in diverse lighting.

3.2.5 SERVO MOTOR

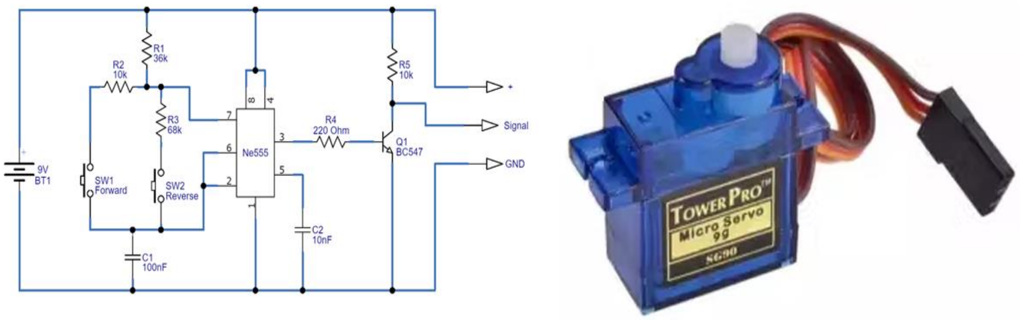

Figure 3.6: Servo motor

The charging bay automation system opens the door upon successful payment or biometric authentication and securely closes it after the device is placed, ensuring both device security and user convenience. Integrated with Arduino, it enables synchronized operation with other system components, offering smooth, precise functionality while preventing theft or tampering during charging the system uses a standard RC servo motor, such as the SG90 or MG996R, providing precise angular movement and adequate torque (~2.5 kg/cm for SG90 and ~9.4 kg/cm for MG996R) to securely handle the charging bay door. Operating at 4.8V–6.0V and controlled via PWM, it offers a 0°–180° angular range and quick operation (~0.1–0.2 seconds per 60° rotation).

3.2.6 RELAY MODULE

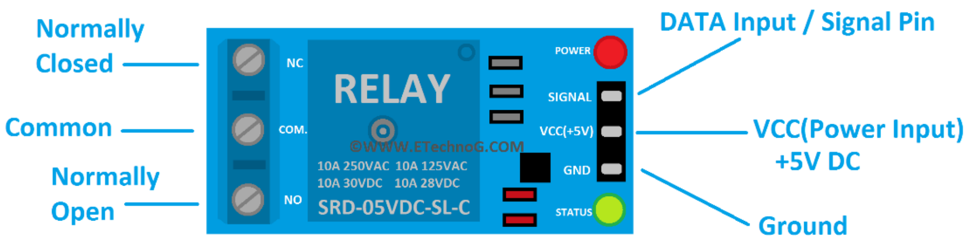

Figure 3.7: Relay Module

The relay module controls the charging circuit by connecting and disconnecting based on user payment and session duration, ensuring safety with electrical isolation to protect the Arduino from high-power components. The single-channel electromechanical relay, operating at 5V DC, controls the charging circuit with a switching capacity of up to 10A at 250V AC or 30V DC, ensuring reliable operation.

3.2.7 8X8 DOT MATRIX LED DISPLAY

Figure 3.8: 8x8 Dot Matrix LED Display

An OLED (Organic Light Emitting Diode) display is a self-emissive screen technology that does not require a backlight, making it more power-efficient than traditional LCDs. It uses organic compounds that emit light when an electric current passes through them, resulting in high contrast, deep blacks, and vibrant colors.

OLED displays are available in various resolutions and sizes, commonly used in wearable devices, smart gadgets, and IoT applications. They offer advantages such as wider viewing angles, faster response times, and low power consumption, especially in battery-powered projects.

3.2.8 SOLAR PANNEL & BATTERY

Figure 3.9: Solar pannel / Battery

SOLAR PANNEL

A solar panel is a device that converts sunlight into electricity.It is also known as a photovoltaic (PV) panel, solar electric panel, or PV module. Solar panels are made up of multiple solar cells, which are the basic units that convert light into electricity.

BATTERY

A battery is a device that stores electrical energy in chemical form and releases it when needed. It's a fundamental component in many electrical systems, providing power to a wide range of devices, from small electronics to large-scale industrial equipment.

3.2.9 ARDUINO UNO

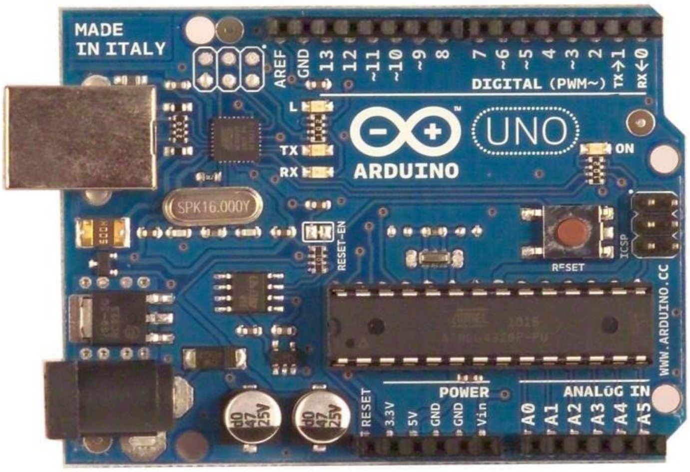

Figure 3.10: Arduino UNO

The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega8U2 programmed as a USB-to serial converter. "Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform.

Technical Specifications

- Microcontroller ATmega328
- Operating Voltage 5V
- Input Voltage (recommended) 7-12V
- Input Voltage (limits) 6-20V
- Digital I/O Pins 14 (of which 6 provide PWM output)
- Analog Input Pins 6
- DC Current per I/O Pin 40 mA

- DC Current for 3.3V Pin 50 mA
- Flash Memory 32 KB of which 0.5 KB used by boot loader
- SRAM 2 KB
- EEPROM 1 KB

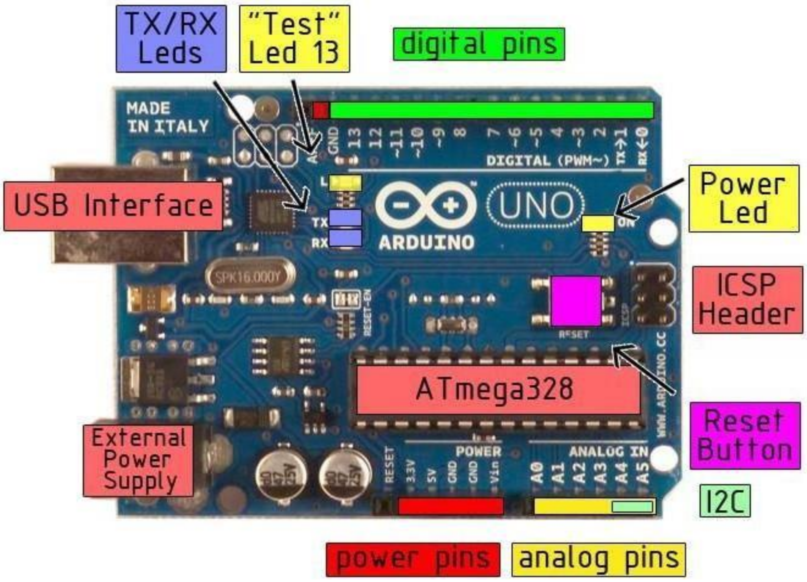

Figure 3.11: Arduino Specifications

Arduino interface boards provide the engineers, artists, designers, hobbyists and anyone who tinker with technology with a low-cost, easy-to-use technology to create their creative, interactive objects, useful projects etc., A whole new breed of projects can now be built that can be controlled from a computer.

3.3 ACTIVITY DIAGRAM

3.3.1 SCHEMATIC DIAGRAM OF SECURE SMART MOBILE CHARGING SYSTEM

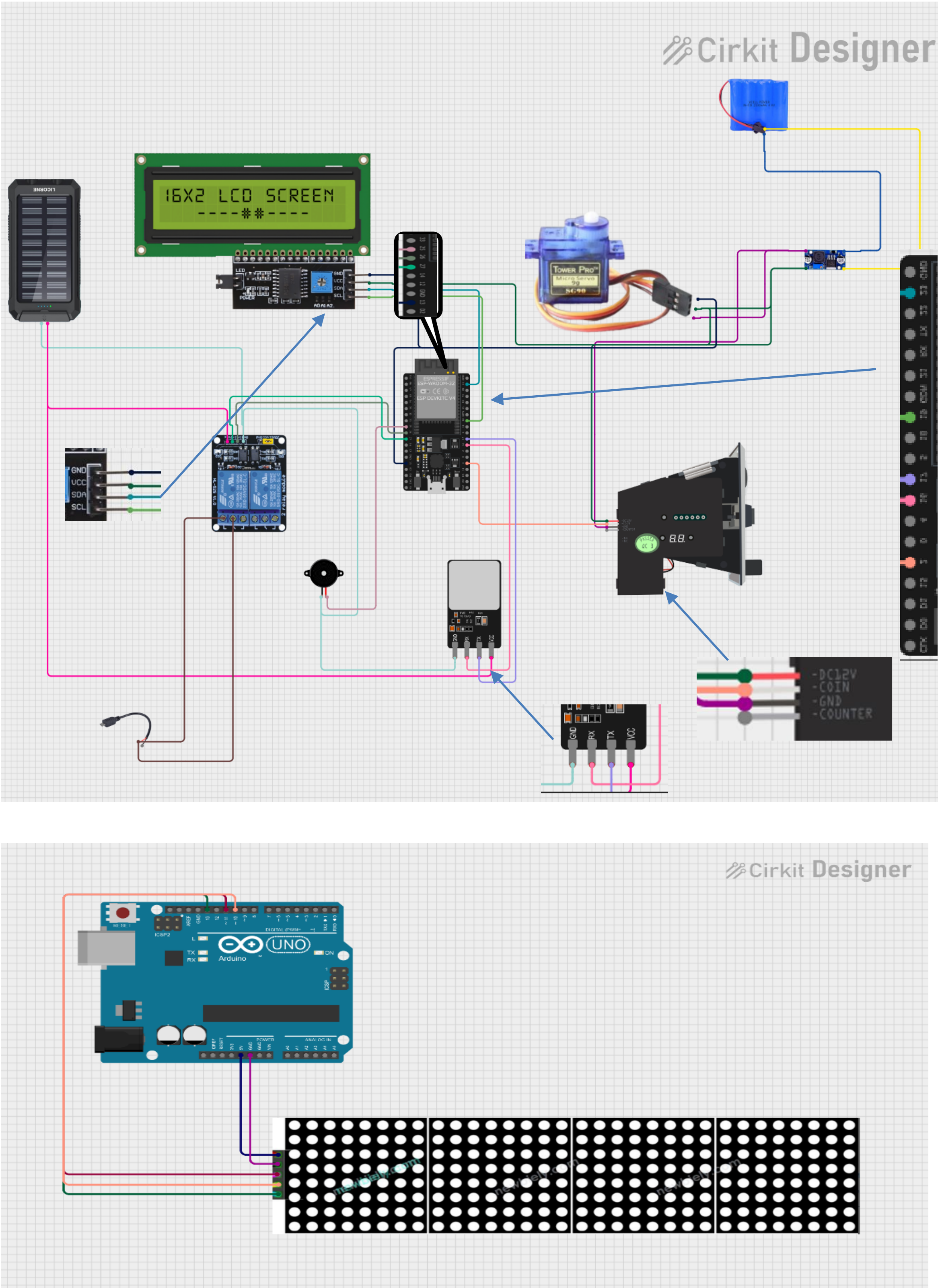

Figure 3.12: Schematic diagram of secure smart mobile charging system

The schematic diagram of the secure smart mobile charging system visually represents the interconnection of various components, ensuring automated and secure mobile charging in public spaces. At the core of the system, the ESP32 microcontroller acts as the central processor, managing user authentication, payment validation, and charging control. Users initiate the charging process by inserting a coin into the coin acceptor, which verifies payment before allowing access. Once validated, the system prompts the user to register or verify their fingerprint using the biometric sensor, ensuring that only authorized users can retrieve their devices. Upon successful authentication, the servo motor unlocks the secure charging compartment, allowing the user to place their phone inside. The relay module regulates the power supply, activating the charger for a predetermined time based on the payment received.

Throughout the charging session, the LCD display provides real-time status updates, while the buzzer alerts users when charging is complete or if additional authentication is required. To enhance operational reliability, the system is equipped with a solar panel and battery backup, ensuring uninterrupted service even in locations with inconsistent power availability. Additionally, an IoT module can be integrated for remote monitoring and data collection, making the system scalable for deployment in multiple locations.

An Arduino UNO is used to drive an 8x8 LED dot matrix display, enabling the system to broadcast advertisements, usage instructions, or public messages, further enhancing functionality and user engagement. The system’s modular design allows for future expansion, such as UPI-based digital payments or facial recognition for contactless authentication. This schematic effectively demonstrates how hardware components interact to provide a secure, automated, and user-friendly mobile charging solution for public spaces, combining practicality, safety, and smart technology in one robust design.

CHAPTER 4

ADVANTAGES & DISADVANTAGES

ADVANTAGES:

1. **Enhanced Security**
   The use of a fingerprint sensor ensures that only authenticated users can access and retrieve their devices, reducing the risk of theft or unauthorized use.
2. **Secure Payment Integration**
   The system includes a **coin acceptor**, providing a simple, offline payment method that is ideal for public installations without internet access.
3. **User-Friendly Operation**
   A clear LCD interface and automated mechanisms (servo motor for locking/unlocking) offer an intuitive experience, even for users unfamiliar with advanced technology.
4. **Standalone Operation**
   The use of **ESP32** enables the system to operate independently, and optionally support Wi-Fi-based features in the future if needed.
5. **Real-Time Feedback**
   Buzzer and LCD provide immediate status updates (e.g., "Insert Coin", "Charging", "Time's Up"), enhancing usability and interaction.
6. **Device Protection During Charging**
   Once the locker is engaged, the system prevents access until fingerprint authentication, ensuring the mobile device is secure while charging.
7. **Modular and Expandable Design**
   The use of modular components like relays and servos makes it easier to upgrade the system or integrate with future technologies (e.g., UPI, solar charging).

DISADVANTAGES:

1. **Initial Setup Cost**
   Though affordable on a small scale, integrating fingerprint modules, servo locks, and coin acceptors can raise costs in mass deployment.
2. **Limited Payment Flexibility**
   The system currently supports only coin-based payments, which may not be convenient for all users in a digital economy.

3. **Biometric Privacy Risks**
   If user fingerprint data is stored, the system must ensure encrypted storage and compliance with data privacy laws to avoid misuse.
4. **Dependence on Hardware Components**
   Failure of any one module (e.g., servo, relay, sensor) can compromise the system's operation, requiring robust maintenance protocols.
5. **No Remote Access or Monitoring**
   In its current form, the system lacks IoT integration, limiting features like remote diagnostics or user notifications.
6. **Mechanical Wear and Tear**
   Moving parts like servos and coin mechanisms are prone to mechanical wear, which may necessitate regular inspection or replacement.

4.2 LIMITATIONS:

1. **Offline Operation Only**
   The system does not currently support network connectivity, which limits its ability to offer remote monitoring or software updates.
2. **Physical Payment Constraints**
   Reliance on coins restricts its usage in cashless environments and poses challenges in ensuring coin availability or change handling.
3. **Limited User Capacity**
   As each fingerprint ID must be enrolled individually, the system is not ideal for environments with frequent user changes.
4. **Environmental Sensitivity**
   Exposure to outdoor conditions (dust, moisture) may affect the performance of components like the fingerprint sensor and LCD.
5. **Security Risks in Unattended Areas**
   Without external casing or CCTV integration, the system may be vulnerable to vandalism or tampering in public settings.
6. **Single Charging Slot Design**
   The current model handles only one user/device at a time. For high-demand areas, multiple units or a multi-slot system would be needed.

4.3 APPLICATIONS :

1. **Colleges and Universities**

   Ideal for use in student lounges, libraries, and common areas to offer secure charging for mobile phones while ensuring personal device safety.

2. **Offices and Co-Working Spaces**

   Useful in professional environments to prevent phone theft during charging, while offering a simple pay-per-use charging solution.

3. **Shopping Centers and Public Waiting Areas**

   Can be deployed in malls or bus/train stations to generate small-scale revenue through coin-operated charging, ensuring secure service.

4. **Cafes and Restaurants**

   Enhances customer experience by providing lockable charging slots for secure device charging during dining.

5. **Rural Areas and Hostels**

   Offers a secure and standalone charging solution in areas with minimal security or supervision, where theft concerns are higher.

6. **Examination and Training Centers**

   Helps students or candidates leave their phones securely while taking tests or attending training sessions.

7. **Temporary Events and Exhibitions**

   The portable and self-contained nature makes it suitable for short-term deployment at expos, fairs, or trade shows.

CHAPTER 5

RESULT AND DISCUSSION

Figure 5.1: Project Model - Secure Smart Mobile Charging System

This figure represents the complete setup of the secure smart mobile charging system. The model includes all the key components: ESP32 microcontroller, fingerprint sensor, coin acceptor, relay modules, servo motor for locking/unlocking, I2C LCD display, and buzzer. The entire system is housed in a compact enclosure with a charging bay for the user's mobile device.

The diagram visually highlights:

1. Sensor connections to ESP32
2. Coin insertion slot
3. Fingerprint sensor mounted for user access
4. Servo-controlled locker compartment
5. LCD displaying real-time status
6. Power connections and relays to control the charger

This integrated design ensures secure, authenticated, and time-limited mobile charging, especially useful in public spaces like stations, malls, and cafes.

Figure 5.2: Coin Inserted - Charging Access Granted

When the user inserts a ₹5 coin into the coin slot, the coin acceptor sends a signal to the ESP32 via the COIN_PIN. The LCD instantly updates, displaying a message like “₹5 Detected,” acknowledging successful payment.

This event initiates the fingerprint enrollment process, where the system waits for the user to place their finger on the scanner. This coin-based activation restricts unauthorized use and ensures a pay-per-use charging model.

Key highlights shown in this figure:

1. Coin entering the acceptor
2. LCD displaying "₹5 Detected"
3. System transitioning to fingerprint enrollment state

This step validates payment before allowing further interaction with the system.

Figure 5.3: Fingerprint Enrolled - Device Placement Allowed

After the coin is validated, the fingerprint sensor prompts the user to place their finger. The Adafruit fingerprint module processes and stores the fingerprint data (if not already enrolled). Once the fingerprint is successfully enrolled:

1. The servo motor rotates to unlock the compartment (locker).
2. The charging relay is activated, allowing power to the mobile charger.
3. The LCD updates to show “Charging...”, indicating the process has started.

This figure depicts:

1. User placing a finger on the sensor
2. LCD showing enrollment status (“Place Finger”, “Enroll Success”)
3. Servo motor in unlocked position
4. User placing phone inside the compartment

This mechanism ensures only the user who enrolled the fingerprint can retrieve the device after charging.

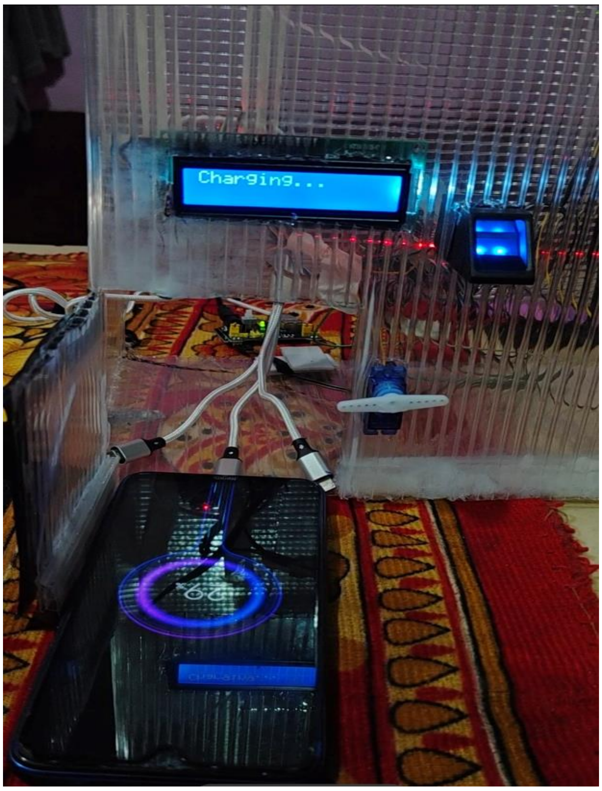

Figure 5.4: Charging in Progress - Real-Time Monitoring

During charging, the system continuously monitors two things:

1. Time elapsed since charging started.
2. User fingerprint match for early device collection.

The LCD continuously displays "Charging..." to indicate active status. If the enrolled user places their finger during charging, the fingerprint is verified, and the system allows retrieval before timeout.

This figure shows:

1. LCD with “Charging...” message
2. Charger turned ON (via relay)
3. Fingerprint verification active in the background

This controlled process limits usage time and prevents unauthorized access.

Figure 5.5: Charging Timeout - Fingerprint Verification Required for Retrieval

If the user does not collect the device within the preset charging time (e.g., 60 seconds)**,** the system performs the following:

1. Automatically turns OFF the charging relay
2. Activates the buzzer to alert the user
3. Prompts the user via LCD to verify their fingerprint again

Charging is halted until the correct fingerprint is scanned. This step prevents continuous usage beyond the paid period and ensures device security until the user returns.

This figure captures:

1. LCD displaying “Time’s Up!” or “Verify Finger...”
2. Buzzer turned ON
3. Fingerprint module waiting for input

It emphasizes security and controlled access even after timeout.

Figure 5.6: Fingerprint Verified - Device Retrieved Successfully

Once the enrolled fingerprint is matched again:

1.The buzzer is stopped
2.The servo motor unlocks the compartment
3.The LCD displays "Collect Device"
4.After a short delay, the system resets to its initial state, ready for the next user

This figure shows:

1.User verifying fingerprint post timeout
2.LCD showing "Verified" and then "Collect Device"
3.Locker opening again for device retrieval

This final step ensures that only the original user who paid and enrolled can collect the device, maintaining both security and user trust.

CHAPTER 6

CONCLUSION

The Secure Smart Mobile Charging System offers a safe and convenient solution for charging mobile devices in public spaces. By combining biometric authentication, coin-based payment, and automated security features, it effectively reduces the risk of theft and unauthorized access. Powered by an ESP32 microcontroller, the system coordinates components like a fingerprint sensor, servo motor, LCD display, and relay module to ensure smooth and secure operation.Its automated and modular design allows for easy use, minimal supervision, and future upgrades such as digital payments, IoT connectivity, and solar charging. While initial setup and maintenance may pose challenges, the system remains scalable and suitable for locations like transport hubs, schools, malls, and offices.In summary, this system provides a practical, secure, and adaptable approach to public mobile charging, with potential for further enhancements to meet evolving needs.

FUTURE ENHANCEMENT

Future enhancements for the Secure Smart Mobile Charging System aim to improve accessibility, security, and operational efficiency while integrating modern technologies. One of the key upgrades is mobile app integration, allowing users to book charging slots, check availability, and track usage history remotely. Additionally, digital payment options such as UPI, QR codes, and NFC will be incorporated to provide a cashless experience, making transactions seamless and eliminating dependence on physical currency. To improve monitoring and scalability, cloud-based analytics will enable remote tracking of power consumption, system health, and advertisement updates, ensuring efficient management. The authentication process can be further strengthened by face recognition or RFID technology, providing a contactless user verification method. Furthermore, to enhance user experience, voice assistance and multilingual support will be introduced, ensuring accessibility across different demographics and age groups.

Key Enhancements:

1. **Mobile App & Digital Payments** – Users can book slots, check availability, and make payments via UPI or NFC.
2. **Cloud Monitoring & IoT Integration** – Enables remote diagnostics, usage tracking, and system control.
3. **Advanced Authentication** – Face recognition and RFID for secure and contactless access.
4. **Energy Analytics & Eco-Impact Display** – Real-time tracking of solar energy usage and environmental benefits.
5. **Power-Saving Features** – Adaptive brightness and standby modes for energy efficiency.
6. **Modular Charging Ports** – Support for Type-C, wireless charging, and fast-charging standards.
7. **Emergency Power Bank Access** – Users can borrow a power bank in urgent situations.

REFERENCES

1. **Pradeep Pradeep Kumar M. et al.** (2023)
   Journal: Available on ResearchGate (specific journal details not provided).
   Summary: Describes a secure mobile charging system using biometric and payment-based access.
2. **G. Priyanka & S. Anisha** (2018)
   Journal: International Journal of Pure and Applied Mathematics
   Volume: 119, *Issue:* 12
   Summary: Presents design of an embedded system for secure mobile charging with automation.

3. **S. Banu Prathap, R. Priyanka, G. Guna, Dr. Sujatha**
   Title: Coin Based Cell Phone Charger
   Journal: International Journal of Engineering Research & Technology (IJERT)
   ISSN: 2278-0181, *Volume:* 2, *Issue:* 3 (March 2013)
   Summary: A microcontroller-based system that uses a coin acceptor to enable charging.
4. **M.S. Varadarajan** (2012)
   Title: Coin Based Universal Mobile Battery Charger
   Journal: IOSR Journal of Engineering (IOSRJEN)
   Summary: This system allows users to charge a variety of mobile devices via a coin-operated mechanism, powered by solar energy.
5. **T. Gunawan, Mirakartivi, Rashidah Abubakar**
   Title: Development of Portable Charger for Mobile Phone using Arduino Microcontroller during Disaster Recovery
   Conference Paper: (Year not specified)
   Summary: Focuses on mobile charging during emergencies using Arduino-based designs.
6. **Sihua Wen** (2009)
   Title: Cell Balancing Buys Extra Run Time & Battery Life
   Journal: Analog Application Journal
   Pages: 14–18
   Summary: Technical paper on battery management and efficiency, applicable for smart charging systems.