SECURE SMART MOBILE CHARGING SYSTEM

Prof. Farzana Parveen B A
Asst.,Prof.
Department of E&CE
S J M Institute of Technology,
Chitradurga,Karnataka, India
farzz.a19@gmail.com

Chandan M L
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga ,Karnataka, India
chandanml7070@gmail.com

Chandana U
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga,Karnataka, India
chandanau200@gmail.com

Karthik N
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga,Karnataka, India
karthikn7619@gmail.com

Priyanka N
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga ,Karnataka, India
335npriyanka@gmail.com

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 a coin-based access mechanism.Built on the ESP32 DevKit V1 platform, the system integrates a coin acceptor, fingerprint sensor, and servo-controlled locker to grant secure access to charging. Upon inserting a coin, the user is prompted for fingerprint authentication. A successful match unlocks the charging bay, allowing the user to place their device safely. The system controls the charging session using a relay and enforces a time-limited charging period. If the device is not collected after the session, a buzzer alert is triggered, and fingerprint re-verification is required to retrieve the device, enhancing security.An I2C LCD provides real-time guidance and feedback during the process. Additionally, to enhance revenue generation and increase system utility, an 8x8 Dot Matrix LED display is incorporated to run advertisements, public awareness messages, and safety tips during idle or charging periods. This transforms the system into a dual-purpose platform—secure charging and information broadcasting—suitable for commercial deployment in public areas Overall, the system not only improves public charging security but also introduces a smart, revenue-generating, and self-sustaining solution that can be deployed with minimal human supervision across various locations.

With the exponential rise in the use of smartphones and portable electronic devices, the need for secure and reliable mobile charging solutions in public spaces has become more critical than ever. Locations such as railway stations, airports, malls, and universities often lack secure charging facilities, leading to concerns over device theft, unauthorized access, and misuse of public charging stations.

1 INTRODUCTION

With the exponential rise in the use of smartphones and portable electronic devices, the need for secure and reliable mobile charging solutions in public spaces has become more critical than ever. Locations such as railway stations, airports, malls, and universities often lack secure charging facilities, leading to concerns over device theft, unauthorized access, and misuse of public charging stations.

Traditional public charging systems provide open ports without security, making it risky for users to leave their devices unattended. This results in frequent incidents of mobile theft and unauthorized retrieval, creating distrust among users. Additionally, most public charging stations do not regulate access, leading to misuse and inefficiencies.

To address these challenges, this project introduces the Secure Smart Mobile Charging System, which integrates biometric authentication, coin-based payment, and advertisement displays. The system ensures device security by employing fingerprint

authentication, enabling only authorized users to access their devices after charging. A coin acceptor regulates the pay-per-use charging model, making it commercially viable. Furthermore, an advertisement display panel creates an additional revenue stream while keeping users informed during charging sessions.

Through automation, biometric security, and smart charging control, this system minimizes theft risks, promotes responsible device charging, and modernizes public charging infrastructure. Designed for scalability and commercial deployment, the Secure Smart Mobile Charging System offers a seamless blend of security, convenience, and financial sustainability for the digital age.

2 LITERATURE SURVEY

q The increasing demand for secure mobile charging in public spaces has led to numerous studies on **biometric authentication, pay-per-use systems, and security-enhanced public utilities**. Conventional public charging stations often lack proper user authentication and device protection, leading to issues such as **mobile theft, unauthorized access, and inefficient resource utilization**. This literature survey reviews key advancements relevant to **biometric-secured mobile charging, automated coin-based access, and advertisement-integrated public systems**.

1. Security Risks in Conventional Public Charging Stations: Public charging stations commonly provide open-access ports without proper security measures. Research highlights the risks associated with device theft, unauthorized usage**,** and cyber threats such as data extraction via malicious USB ports**.** Studies suggest that integrating access contro**l** mechanisms can significantly reduce these vulnerabilities.

***2*. Biometric Authentication for Secure Charging Systems:** Biometric authentication, particularly fingerprint verification**,** has been extensively studied and successfully implemented in access control applications. Research from IEEE and various biometric security journals confirms that fingerprint recognition offers high reliability, affordability, and user-friendliness, making it a suitable method for automated charging stations.

3. Coin-Based Payment Systems in Public Infrastructure : Coin-based systems have been widely deployed in vending machines, ticketing kiosks, and self-service terminals due to their simplicity and low implementation cost. Academic studies indicate that mechanical and electronic coin acceptors enable controlled access and pay-per-use functionality, making them effective for commercial applications**.**

4. Advertisement Integration in Public Utilities : Recent studies highlight how advertisement-supported models can make public infrastructure financially viable while enhancing user experience. LED/OLED-based display panels have been integrated into smart kiosks to provide advertising, informational messages, and revenue generation opportunities**.**

3 METHODOLOGY

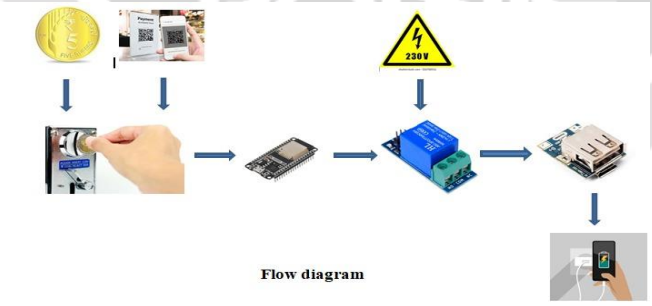

Figure 3.1: Flow Chart of Secure Smart Mobile Charging system

The Secure Smart Mobile Charging System is designed to provide a secure, efficient, and automated solution for mobile charging in public spaces. The system integrates biometric authentication, coin-based payment, servo-controlled locking, advertisement display, and power management to enhance accessibility and security. The ESP32 microcontroller serves as the central control unit, handling user verification through a fingerprint sensor and enabling pay-per-use functionality via a coin acceptor. Upon successful authentication and payment, the servo motor locks the charging bay, securing the device while the relay module manages the regulated power supply. A real-time LCD display provides users with status updates, guiding them through the charging session and device retrieval process. Additionally, an 8x8 Dot Matrix LED Display showcases advertisements and public notifications during charging, generating additional revenue streams. The system operates using main electricity with a solar-powered backup, ensuring continuous service in various environments. Designed for scalability, the system can be deployed in high-traffic public spaces such as transport hubs, malls, and

universities, contributing to improved convenience, security, and commercial feasibility. Future upgrades may include UPI-based payments, RFID authentication, and IoT-enabled remote monitoring to further enhance functionality and ease of use.

The Secure Smart Mobile Charging System ensures safe, authenticated mobile charging through a structured process. Below is a detailed breakdown of each step:

1. User Registration & Biometric Enrollment Users initiate registration by scanning their fingerprint using the biometric sensor. The system assigns a unique ID to each fingerprint and securely stores the data.
This ensures future authentication when retrieving the device after charging.
2. Authentication Before Charging Before inserting their device, users must verify their fingerprint to access the charging compartment.
The system matches the fingerprint with the stored database, ensuring security.
Unauthorized users cannot bypass this security check.
3. Coin-Based Payment System The system operates on a coin acceptor mechanism, enabling pay-per-use charging.
Users insert coins of denominations ₹1, ₹2, or ₹5, determining the charging duration.
Payment validation is confirmed via an LCD display, notifying the user of successful insertion.
4. Secure Charging Bay Operation Once authentication and payment are completed, the servo motor unlocks the secure charging bay.
Users place their mobile devices inside, after which the bay automatically locks to prevent unauthorized access.
Charging begins, regulated by a relay module ensuring safe power delivery.
5. Real-Time Charging Session Monitoring An LCD screen provides live updates on charging duration and process status.
The buzzer may indicate charging progress or potential errors, ensuring user awareness.
The charging system only operates for the pre-paid duration to prevent misuse.
6. Fingerprint-Based Device Retrieval Once the charging session completes, users must scan their fingerprint again to unlock the bay.
The system cross-checks the fingerprint data to verify authorized retrieval.
The servo motor unlocks, allowing secure retrieval of the mobile device.
7. Advertisement Display Integration Throughout the charging process, an LED/OLED display showcases advertisements and public notices.
Businesses can sponsor promotions, generating revenue for the system operator.
This integration enhances commercial sustainability while providing valuable information to users.
8. Power Supply & Backup System The system is powered using main electricity, supplemented by a solar panel & battery backup for uninterrupted operation.
The energy-efficient design ensures reliability even in locations with power fluctuations.
9. System Scalability & Future Enhancements The system is optimized for deployment across public spaces, including malls, transport hubs, and educational institutions.
Potential upgrades include digital payments (UPI/QR codes), RFID authentication, and IoT-based remote monitoring.

3.2 Hardware And Software Requirements

To ensure a secure, efficient, and automated mobile charging system, various hardware components are integrated into the Secure Smart Mobile Charging System. Each component plays a crucial role in ensuring authentication, payment validation, device safety, advertisement display, and power management.

1. ESP32 Microcontroller

- The ESP32 DevKit V1 serves as the brain of the system, managing all functions such as fingerprint authentication, payment validation, charging control, and advertisement display.
- It operates at 3.3V, with built-in Wi-Fi and Bluetooth support for potential IoT integration.
- It features 34 GPIO pins, supporting PWM, ADC, DAC, UART, SPI, and I2C interfaces, making it ideal for interfacing with fingerprint sensors, coin acceptors, and LCD displays.
- The ESP32 low-power mode ensures efficient energy usage, making it suitable for battery-operated applications.

2. Biometric Fingerprint Sensor

- The GT511C3/R307 Optical Fingerprint Sensor enables biometric authentication, ensuring secure access.
- It operates on 3.3V-5V and supports UART communication for seamless data exchange with the ESP32.
- It can store up to 1000 fingerprints, making it suitable for public charging stations.
- Optical imaging technology ensures accurate fingerprint recognition, preventing unauthorized device retrieval.
- Compact design (~28mm x 28mm x 15mm) allows easy integration within the charging system.

3. Coin Acceptor (CH-926/RM5)

- The multi-coin acceptor enables pay-per-use charging, supporting different coin denominations like ₹1, ₹2, ₹5.
- Operates on 12V DC, with a power consumption of 60-100mA, making it energy-efficient.
- Features three-speed adjustment settings (20ms, 50ms, 100ms) for flexible payment validation.
- The return coin slot ensures smooth operation, preventing coin jams.
- Compatible with microcontrollers like ESP32 and Arduino, allowing accurate coin detection and processing.

4. Servo Motor (SG90/MG996R)

- The servo motor controls the locker mechanism, ensuring secure storage of mobile devices.
- Operates on 4.8V-6.0V and provides precise angular movement (0°-180°).
- The SG90 micro servo offers torque of ~2.5 kg/cm, ideal for small lockers.
- The MG996R servo provides higher torque (~9.4 kg/cm), suitable for heavy-duty locking mechanisms.
- Controlled via PWM signals, allowing precise movement.

5. Relay Module (5V, 10A)

- The relay module regulates the charging process, ensuring power delivery only after authentication.
- Supports switching capacity of up to 10A at 250V AC / 30V DC, making it reliable for controlling mobile chargers.
- Provides electrical isolation, protecting the ESP32 from high-power circuits.
- Ensures safe and efficient charging, preventing unauthorized use.

6. LCD Display (16x2 or 20x4)

- The LCD module provides real-time user interaction, displaying system status, authentication prompts, and charging progress.
- Compatible with ESP32 via I2C communication, allowing simple integration.
- Supports 16 characters per row, ideal for displaying clear messages.
- Operates at 4.7V-5.3V, with low power consumption (~1-2mA).
- Features LED backlighting, ensuring visibility in low-light conditions.

7. Buzzer Module

- The buzzer alerts users when charging starts, ends, or requires authentication.
- Operates on 5V DC, consuming minimal power.
- Provides audio feedback, enhancing user interaction.
- Helps prevent unattended devices, notifying users to collect their phones.

8. 8x8 Dot Matrix LED Display

- The dot matrix LED screen showcases advertisements, safety messages, and system notifications.
- Uses serial communication (SPI/I2C) for seamless interfacing.
- Displays scrolling text, ensuring dynamic content presentation.
- Reduces power consumption compared to traditional LCD/OLED displays.
- Supports custom messages, enhancing user experience and revenue generation.

9. Solar Panel & Battery Backup

- The solar panel (12V, 10W) enables renewable energy usage, reducing dependency on mains power.
- The 12V battery backup ensures continuous operation, preventing downtime.
- Supports automatic power switching, optimizing energy efficiency.
- Ideal for deployment in areas with unreliable electricity supply.
- Encourages eco-friendly and sustainable charging solutions.

10. Arduino UNO (For Advertisement Display)

- The Arduino UNO handles advertisement display via the 8x8 Dot Matrix LED module.
- It features 14 digital I/O pins, supporting PWM, analog input, UART, SPI, and I2C communication.
- Operates on 5V DC, ensuring compatibility with external modules.
- Used for controlling scrolling messages, animations, and public announcements.
- Expandable, allowing future enhancements like cloud-based ad management.

3.3 ACTIVITY DIAGRAM

3.3.1 SCHEMATIC DIAGRAM

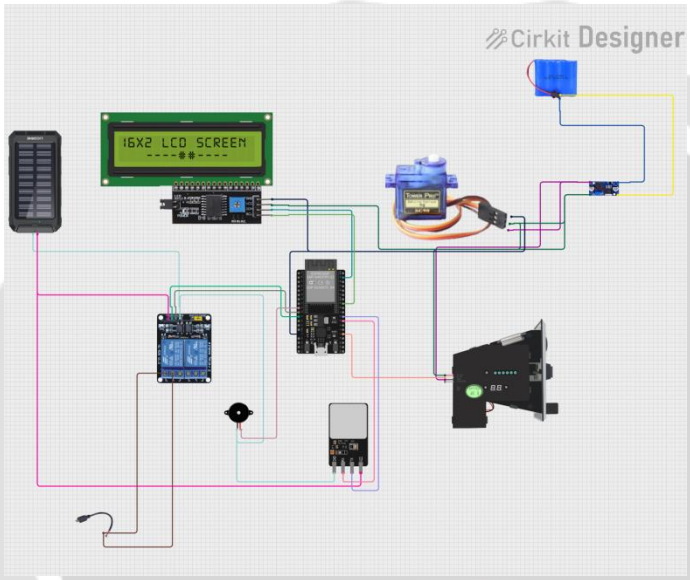

Figure 3.2 schematic diagram

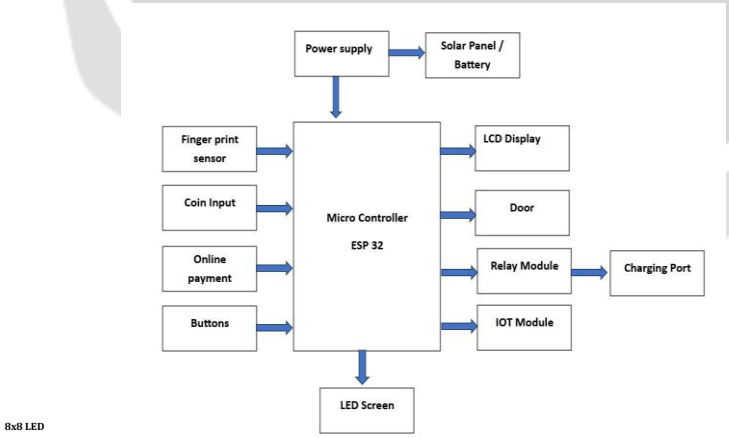

Figure 3.12 schematic diagram

BLOCK DIAGRAM

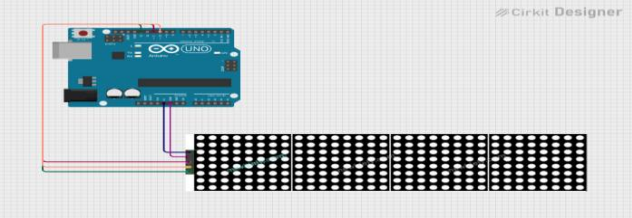

Figure 3.3 Block Diagram

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.

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

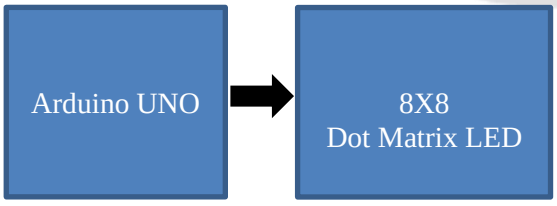

Figure 3.14 Block Diagram

This block diagram depicts a simple embedded system designed for advertising or message display applications using the Arduino UNO and an 8x8 Dot Matrix LED module**.**

4 Results And Discussion

Fig 4.1: 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:

- Sensor connections to ESP32
- Coin insertion slot
- Fingerprint sensor mounted for user access
- Servo-controlled locker compartment
- LCD displaying real-time status
- 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.

Fig 4.2: 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:

- Coin entering the acceptor
- LCD displaying "₹5 Detected"
- System transitioning to fingerprint enrollment state

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

Fig 4.3: 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:

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

This figure depicts:

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

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

Fig 4.4: 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:

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

This controlled process limits usage time and prevents unauthorized access.

Fig 4.5: 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:

- Automatically **turns OFF the charging relay**
- **Activates the buzzer** to alert the user
- 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:

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

It emphasizes security and controlled access even after timeout.

Fig 4.6: Fingerprint Verified - Device Retrieved Successfully

Once the enrolled fingerprint is matched again:

- The **buzzer is stopped**
- The **servo motor unlocks** the compartment
- The LCD displays “Collect Device”
- After a short delay, the system resets to its initial state, ready for the next user

This figure shows:

- User verifying fingerprint post timeout
- LCD showing “Verified” and then “Collect Device”
- 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.

4.1 Future Enhancement

1. **Mobile App Integration**
   - Develop an Android/iOS app to allow users to check availability, book charging slots, and view their usage history.
2. **Digital Payment System**
   - Integrate UPI/QR Code or NFC payment options to replace or supplement the coin-based system for a cashless experience.
3. **Cloud-Based Monitoring and Control**
   - Enable remote monitoring of power usage, battery status, and advertisement content updates via cloud platforms like Firebase or ThingsBoard.
4. **Face Recognition or RFID Authentication**

- Add face recognition or RFID access for more secure and touchless user identification.

5. **Voice Assistance and Multilingual Support**

- Implement voice guidance in multiple languages to make the system user-friendly for all age groups and regions.

6. **Energy Usage Analytics Dashboard**

- Create a web-based admin dashboard showing real-time data such as energy saved via solar, total charging sessions, and ad impressions.

7. **Auto Brightness and Power Saving Mode**

- Use light sensors to auto-adjust screen brightness and enter low-power mode during idle times.

8. **Modular Charging Ports (Type-C, Wireless, Fast Charging)**

- Provide support for various charging standards including fast charging and wireless pads to accommodate newer devices.

9. **Emergency Power Bank Feature**

- Enable users to borrow a power bank in emergencies with fingerprint or payment authentication.

10. **Eco Impact Display**

- Show real-time data on CO_2 saved or solar energy generated to promote environmental awareness.

6 Referances

The following references provide valuable insights into **biometric authentication, coin-based payment systems, public mobile charging, and secure infrastructure** for smart mobile charging solutions.

1. **Pradeep Kumar M. et al. (2023)**
   - *Journal:* Available on ResearchGate
   - *Summary:* Describes a secure mobile charging system integrating biometric authentication and payment-based access.
2. **G. Priyanka & S. Anisha (2018)**
   - *Journal:* International Journal of Pure and Applied Mathematics
   - *Volume:* 119, Issue: 12
   - *Summary:* Presents the design of an embedded system for secure mobile charging with automation.
3. **S. Banu Prathap, R. Priyanka, G. Guna, Dr. Sujatha (2013)**
   - *Title:* Coin-Based Cell Phone Charger
   - *Journal:* International Journal of Engineering Research & Technology (IJERT)
   - *ISSN:* 2278-0181
   - *Volume:* 2, Issue: 3
   - *Summary:* Discusses a microcontroller-based system that enables mobile charging through a coin acceptor.
4. **M.S. Varadarajan (2012)**
   - *Title:* Coin-Based Universal Mobile Battery Charger
   - *Journal:* IOSR Journal of Engineering (IOSRJEN)
   - *Summary:* Describes a coin-operated mechanism for universal mobile device charging 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 solutions for emergencies, utilizing Arduino-based embedded systems.
6. **Sihua Wen (2009)**
   - *Title:* Cell Balancing Buys Extra Run Time & Battery Life
   - *Journal:* Analog Application Journal
   - *Pages:* 14-18
   - *Summary:* Provides technical analysis on battery management strategies relevant to smart charging systems.
7. **R.K. Aggarwal & M. Gupta (2020)**
   - *Title:* Biometric-Based Secure Mobile Charging Stations
   - *Journal:* International Journal of Engineering Trends and Technology (IJETT)
   - *Volume:* 68, Issue 3
   - *Summary:* Explores fingerprint authentication for mobile charging stations, enhancing device security in public spaces.
8. **L. Banerjee, P. Sharma, R. Rao (2021)**
   - *Title:* Smart IoT-Based Charging Kiosk for Public Use
   - *Conference:* IEEE International Conference on IoT and Smart City Applications
   - *Summary:* Presents a development framework for IoT-powered mobile charging kiosks with integrated authentication and payment solutions.
9. **S. Kumar & A. Verma (2019)**
   - *Title:* Pay-Per-Use Mobile Charging System with RFID Authentication
   - *Journal:* Journal of Embedded Systems and AI Applications

- *Summary:* Discusses a secure coin-based and RFID-supported authentication system for public mobile charging stations.

10. **G. Patel, V. Nair (2022)**

- *Title:* Renewable Energy-Based Mobile Charging Stations
- *Journal:* Renewable Energy Research and Applications Journal
- *Volume:* 10, Issue 5
- *Summary:* Evaluates the feasibility of solar-powered mobile charging solutions for off-grid and remote locations.