MINOR REPORT DRAFT (1) (1).pdf

Mar Baselios College of Engineering and Technology

Document Details

Submission ID
trn:oid:::3618:120806607

Submission Date
Nov 10, 2025, 10:14 PM GMT+5:30

Download Date
Nov 10, 2025, 10:20 PM GMT+5:30

File Name
MINOR REPORT DRAFT (1) (1).pdf

File Size
825.0 KB

35 Pages

7,853 Words

49,321 Characters

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

Smart RFID-Enabled Prepaid Charging Infrastructure for Wired Power Transfer

MINOR PROJECT REPORT

Submitted to the APJ Abdul Kalam Technological University in partial fulfillment of requirements for the award of degree

Bachelor of Technology Degree
with
Minor in Computer Science and Engineering

By

ABHINANDI C R (MBT22EE004)
JOHAN MATHEW(MBT22EE028)
SACHITH S SANTHOSH (MBT22EE043)
SREYA KRISHNAN(MBT22EC100)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEEERING

MAR BASELIOS COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous)
Mar Ivanios Vidyanagar, Nalanchira

Thiruvananthapuram 15

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MAR BASELIOS COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous)

Nalanchira, Thiruvananthapuram.

MAR BASELIOS
COLLEGE OF ENGINEERING AND TECHNOLOGY
AUTONOMOUS

CERTIFICATE

*This is to certify that this project report entitled "**Smart RFID-Enabled Prepaid Charging Infrastructure for Wired Power Transfer**" is a Bonafide record of work done by **ABHINANDI C R(MBT22EE004), JOHAN MATHEWS(MBT22EE028), SACHITH S SANTHOSH(MBT22EE043), SREYA KRISHNAN(MBT22EC100)** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of **B.Tech degree with Minor in Computer Science and Engineering**. This is a Bonafide record of the project work carried out by us under proper guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.*

Project Guide	Project Co-ordinator	Head of the Department
Dr. Tessy Mathew Professor Dept. of CSE MBCET	Dr. Jisha John Professor Dept. of CSE MBCET	Dr. Jisha John Professor Dept. of CSE MBCET

ACKOWLEDGEMENT

We express our sincere gratitude to the Principal, **Dr. S. Viswanatha Rao**, for providing us with the opportunity to undertake this mini project. We are deeply grateful to our project guide, **Dr. Tessy Mathew**, Professor, and our coordinator, **Dr. Jisha John**, Professor, whose valuable guidance, support, and encouragement were instrumental in the successful completion of this project. We extend our heartfelt thanks to **Dr. Jisha John**, Head of the Department of Computer Science and Engineering, for providing us with the resources and academic environment required for the development of this project. We would also like to thank all the faculty members and staff of the Department of Computer Science and Engineering for their continuous support. Finally, we thank our families and friends for their unwavering motivation, encouragement, and support throughout this journey.

ABSTRACT

As electric vehicles (EVs) become more common, there is a growing need for intelligent, safe, and simple charging methods. Standard EV charging is still often reliant on the user to prompt authentication and payment by tapping a card or tag to initiate the process. This can be inefficient, offers opportunities for error, and is non-automated process. For this project, we will present an RFID-based EV management process that will allow the user to authenticate and get energy consumption data in real-time while charging his/her EV without the need to worry about prompt payment. Once the EV is plugged into the charging station, the energy meter will show and record how much energy it takes to charge the vehicle. The user removes the card from his/her key chain, the RFID reader will read the UID information. The electrical energy management system will check to see if the user has balance available to charge, since we will have a credit balance from the user account. After the user approves the charge, the relay will permit charging to occur and the energy meter logs the energy used. All transactions will be again recorded and logged to the database. The user will be able to see current balance and transactions using a simple software interface. This authorized process utilizes an augmented form of RFID and energy metering coupled with automated billing in a systematic user-friendly way which adds convenience, transparency, and accountability to the EV charging process, representing a fair approach to harnessing the evolving technology and the move towards sustainable mobility.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

The world is moving toward sustainable, green energy, and the adoption of Electric Vehicles (EVs) is starting to ramp up considerably. EVs are essential to reducing greenhouse gasses and reliance on fossil fuels as well as represent a broader international shift to cleaner modes of transportation. With increased usage of EVs will come higher demands for energy-efficient, safe, smart, charging infrastructure to support it. Charging EVs typically entails manual user billing and user authentication processes which can lead to user mischarging, inaccuracies, inefficiencies, and misuse. Some avenues to eradicate these inefficiencies are through optimized real time technologies like Radio Frequency Identification (RFID) or the Internet of Things (IoT). RFID technology allows for contactless user authentication and IoT technology allows for real-time monitoring of charged energy usage. In summary, a combination of these technologies could enable a smart, prepaid charging system that also contains user verification of smart charging for possible limitations of time or energy. The goal of this project is to research, develop and test a Smart RFID-enabled Prepaid Charging Infrastructure that ultimately automates the entire EV charging process commencing as user authentication through a payment toll gate to verify charged energy usage with a safe and user-friendly interface.

1.1 Need for Smart Charging Infrastructure

As the demand for electric vehicles (EVs) surges, so does the need for expedient and reliable charging. However, there are a number of challenges with the current EV charging ecosystem:

- Unauthorized Access: Traditional systems can have access by non-approved users, resulting in energy theft,
- Manual Billing: Human collected billing systems introduced errors, delays and inconvenience,
- Lack of Transparency: Generally, there is no real-time view of energy consumption or balances to the user,
- Inconsistent Tariff Management: Electricity tariffs fluctuate in real time, however most systems will allow billing without a change in tariff management.

Therefore, a successful automated and safe charging system will incorporate access controls and payment systems that digitalize the billing process to give efficiencies, transparency and

better user experience. A comprehensive approach to these challenges can be achieved with RFID and IoT technologies as they provide effortless communication between equipment and cloud- based management services.

1.2 Overview of RFID and IoT Integration

RFID technology utilizes electromagnetic fields to automatically identify and track tags connected with objects. For this project, RFID technology is used to uniquely identify end-users and link them to their prepaid accounts. Each user is assigned an RFID tag with a unique ID, which an RFID reader is able to scan and will be located at the charging station.

After the user has been verified, the system will retrieve user information, such as balance / ID, from a central database. The microcontroller will determine the number of charging units permitted based on available balance and will begin charging. While the charging is taking place, the IoT-based monitoring will continue to measure energy uptake and will track the data and send it to the database in real-time.

The combined RFID and IoT system allow for:

- Contactless and secure user authentication
- Real-time energy use and charge applicability monitoring and billing
- Data transfer between hardware and cloud services.

1.3 Problem Statement

Current EV charging systems preside without a secure authenticated identity and billing process often requiring users to pay manually, which is itself a lengthy and error-prone process. This creates a mixture of discrepancies, billing disputes, and possible related issues. Therefore, an integrated smart charging system should be combined with RFID-based user recognition and balance-based payment with preloaded charging integrated with an IoT-enabled monitoring system to promote secure, transparency, and automation.

1.4 Objectives

The primary aim of this project is to create a Smart RFID-Enabled Prepaid Charging System that provides a user-friendly, security-enhanced, automated energy charging process.

The specific aims are:

1. To design a prepaid energy management system that allows users to authenticate via RFID.

2. To design a control unit based on a microcontroller which is connected to the electric vehicle for energy transfer as well as billing purposes.

3. To use IoT technology for real-time monitoring of charging periods for both the user and customer.

4. To allow for automated billing and cashless service to the user's RFID-linked account from the remaining balance as charging occurs.

5. To notify the user of their energy consumption and remaining balance via a GSM module and/or dashboard.

1.5 Scope of the Project

This project includes hardware and software integration to develop a prototype of a prepaid electric vehicle (EV) charging system. Hardware includes an RFID reader, microcontroller (ATmega328P), GSM module, energy meter, and relay. The software component includes programming the controller to govern charging sessions and use its IoT connectivity to update a user database. Although this system is aimed primarily at charging wires, the same infrastructure will be extended to wireless power transfer (WPT) systems in the future. This prototype system will serve as a reference for "secure" and automated energy dispensing and payment systems in both public and private networks to support EV charging.

CHAPTER 2
LITERATURE REVIEW

The authors of [1] review a design and implementation of a complete and intelligent charging station management system (CSMS) that aims to enhance the operational efficiency, reliability, and performance of electric vehicle (EV) charging infrastructures. They present a modular and centralized architecture for a CSMS that integrates charging units through a supervisory control and data acquisition layer to allow the CSMS to monitor charging sessions, schedule their operation, control energy transfer, and record real-time data for performance monitoring. CSMS includes remote monitoring, real-time dynamic load balancing and energy optimization strategies, to allow the responsible use of available stored energy and minimize vehicle wait time and public grid overload. Also included are data analytics and billing capabilities to serve easy user and public operator monitoring of session energy consumption with transparency and ease of operation. Although the paper does not address RFID access systems directly, the architectural framework it presents can be readily applied to projects that include user authorization systems, such as RFID. In the case of the current research project on EV charging management using RFID tags, it will be straightforward to adapt the system design in this paper to include RFID user identification and access control so that each authorized user can start or stop a charging session through tag authentication. The management structure in the backend, as described in the text, can then be used to manage session monitoring, energy accountability, and data storage associated with the applicable RFID identity. In addition, the emphasis in the paper on intelligent decision-making, energy optimizations, and communication between charging units provides a technical framework to occur RFID access control methods alongside smart charging management. Altogether, this paper is quite relevant for the current project, as it offers a scalable and efficient management architecture that is securely and practically implemented to use RFID-based interactions by users, delivering a more automated, data-driven, and streamlined EV charging experience.

Paper [2] presents a state-of-the-art review of EV charging infrastructure and accompanying energy management schemes to fill a perceived gap within the literature concerning comparative reviews of the same field. The paper commences by addressing how the increasing

adoption of electric vehicles puts rising demands on charging infrastructure and, therefore, emphasizes the need for efficient charging station design, integration of renewable energy resources, and supporting energy management systems. In this paper, the authors systematically classify different charging schemes according to their connection to either the conventional utility grid or renewable/solar-PV grid sources, contrast the concepts of centralized versus decentralized control architectures for charging stations, and review a very large number of EMS algorithms along with their advantages and disadvantages. For example, the survey shows that centralized control offers global optimization of charging schedules through a single aggregator, whereas decentralized control gives higher autonomy to individual EV users and better scalability and privacy. The paper further goes on to compare the standard grid versus grid-connected PV charging systems and shows that under certain conditions, PV-grid systems can have higher profitability and renewable utilization. It does so by providing a very valuable classification of EMS approaches, such as rule-based, optimization-based, hierarchical, etc., and discussing their computational complexity, scalability, and practical deployment challenges. In terms of your project, which is focused on an EV charging management system with RFID-tag access control, this survey provides very relevant input: it gives a wider context of how charging station management interacts with the grid/renewable infrastructure, what control architectures may be adopted, and what EMS algorithmic approaches you may consider. Its examination of several EMS algorithms is particularly useful since once an RFID-tagged user gets access to the site, the system still has to decide how to schedule that user's charging session, how to integrate renewable power or grid-based power, and how to optimize the session with respect to load on the station or grid constraints.

The paper [3] introduces a new wireless charging system for electric vehicles wherein the initiation and management of charging are done through radio-frequency identification tags, rather than by physical plug or connector. The authors have proposed attaching an RFID tag to a vehicle and an RFID reader to a charging pad. When the vehicle is detected via an RFID reader, the WPT mechanism will turn on, and the EV will start to charge. Compared to wired charging, the system boasts several benefits: no physical connectors (no wear and tear); great convenience in use for the user; higher safety by avoiding exposed contacts; lower susceptibility to weather and road-debris interference; and, possibly, fewer losses in energy transfer. While the paper is still conceptual, it outlines the hardware arrangement, the RFID-activated trigger for power transfer, and the advantageous implications for both in-station and

on-the-go outdoor environments. In the perspective of a project for developing an EV charging management system with RFID-tag-based access control, this work is of relevance. While your project focuses on site access via RFID tags and monitoring/user management, the paper extends that idea into the charging process itself-linking RFID authentication not only to user access but also to the charging activation mechanism. Thus, its reasoning is sound: the RFID tag used for the system can serve as an access/authorization tool and as a means of charging, either via a wireless pad or typical access after granted access. This document has some of the practical considerations including convenience, and being connector-less possibly impacting design considerations for RFID authentication with charging management. This may suggest the RFID reader-pad interface could ultimately be a point of promptness taking a user from access control to charging initiation to help enhance the user experience. All in all, though the paper does not deal with full management of charging sessions, billing, and load balancing or grid integration, it does provide valuable insight into how RFID tagging and wireless charging can be combined into one system-aspect your project could leverage or adapt, for instance, if you opt for wireless pads or want to experiment with plug-less charging.

In [4], a new EV-charging solution is proposed, based on RFID and IoT technologies, to improve user experience and operational efficiency in the charging of electric vehicles. The system, according to the authors, implements RFID tags for the identification of the vehicle or user, an RFID reader connected to a microcontroller and a relay module for managing the start and stop of the charging session, while an IoT-platform is used with MQTT or Wi-Fi for real-time monitoring, remote control, and secure payments. When the user taps their RFID tag, access is authorized and the relay is turned on to initiate charging; sensors measure current/voltage, while the IoT-platform updates a server or mobile app with charging session data, billing information, and notifications upon completion. The authors indicate that the user identification accuracy via RFID was very high, while also providing a convenient interface on the mobile dashboard for status updates and cost tracking. Although it emphasizes hardware and application layer components, which are RFID + IoT + microcontroller devices as opposed to examining advanced grid-integration or load-balancing algorithms, it demonstrates how RFID access control paired with IoT-enabled real-time monitoring facilitates a remarkable improvement in the convenience, security, and usability of charging infrastructure for EVs. This paper supports the relevance of our project, developing an EV

management system featuring RFID-tag based access control. It directly targets the authentication/authorization aspect of your system, by showing how RFID tags can automate verification of user identities and initiate charging. It coordinates RFID identification with IoT-enabled monitoring of user identities and mobile/cloud connectivity; it provides a very practical way to connect physical access to backend monitoring of sessions, usage, and user-generated feedback. By integrating RFID access here with higher-level energy management from other references, it will make your system secure and smart in the process: a user taps on an RFID tag, the system verifies his identity, and backend management monitors the session, records energy usage, bills appropriately, and optionally schedules future sessions. Thus, this paper will play an important role in grounding your design of the access/control front-end and will bridge the gap between user authentication and charging session management.

The paper [5] titled Implementation of RFID Based Smart Electric Vehicle Charging System explores the integration of RFID technology, microcontroller control and GSM communications into an EV-charging infrastructure to enhance security, monitoring and billing functionalities. The authors propose a system built around an ATmega328P microcontroller that uses an RFID reader to authenticate users, displays real-time charging parameters on an LCD, uses current and voltage sensors to measure energy consumption and employs a GSM module to send charging information, status updates and payment notifications. The work argues that as global EV adoption accelerates and charging networks become an increasingly essential part in their use, a RFID-user authentication system both limits unauthorized access, and allows for billing of energy consumed, which adds operational transparency, by automating the billing process. From the methodological perspective, an RFID tag authenticates a user and the RFID tag initiates a charging session monitoring the session using sensor data (voltage, current), registering the amount of energy consumed to invoice and billing, at the same time, a GSM module communicates the necessary information to the user in real-time. In terms of your project, which tracks with the EV charging management system and site access through RFID tags, the paper speaks to your case as it addresses the access/authentication part utilizing the RFID as user identification to initiate the charging session and invoice the energy consumed via charging. The hardware-level implementation (microcontroller, sensors, GSM communication) offers an example of what you may emulate, or improve upon for your system. While your project also encompasses aspects of charging session management, scheduling, and perhaps site access control (user enters site, taps RFID,

system grants access and begins charging), this paper gives you detailed insight into the lower-level user authentication and billing linking process. You can build on that by incorporating your additional layers: e.g., integrating site-entry RFID authentication gate, linking that authentication to the charging management backend, scheduling/pool control of multiple chargers, energy-optimization, and user-specific session tracking

CHAPTER 3
SYSTEM DESIGN

The Smart RFID-Enabled Prepaid Charging Infrastructure serves as the proposed model to automate and secure EV charging. The model includes both hardware and software and will perform prepaid energy dispensing, user authentication, and monitoring in real-time. The operation of the Smart RFID-Enabled Prepaid Charging Infrastructure consists of linking a user RFID identity to a cloud-based prepaid account. Once a user authenticates with their RFID, the infrastructure checks the account balance, determines how much energy can be dispensed, and then begins the transfer. While charging takes place, energy usage, as well as the balance, is monitored in real time, and the balance is deducted automatically once charging is finished. This chapter presents the architecture of the Smart RFID-Enabled Prepaid Charging Infrastructure as well as a design flow and functional components.

3.1 System Overview

The system offers energy management system automation for Electric Vehicle (EV) charging stations. There are several important modules, which include the following:

1. RFID-Base Authentication Module – Recognizes authorized users and retrieves previously loaded user accounts which fund is loaded to.
2. Microcontroller Module – The main module of control that processes user input and processes energy flow.

Not only do these modules interchange for a secure experience for charging, but they also ease the use and the process of automation.

3.2 Block Diagram Explanation

Figure 3.1 provides a block diagram of the interconnections between all hardware elements. Each block has a critical function that contributes to a charging control system that is safe, efficient, and accurate.

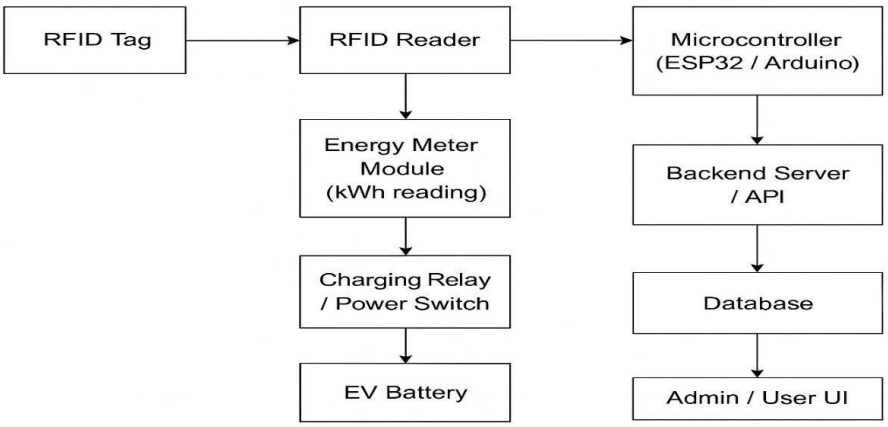

Fig 3.1 – Block Diagram

• An RFID Reader: It identifies and reads the user's RFID tag and forwards the unique ID on the tag to the microcontroller for verification and authentication.

• Microcontroller: This is the component or block identified as the main processor, responsible for running the control algorithms, verifying and authenticating user data and managing energy transfer.

The modular design lends itself to easy expansion and gives the user the possibility to interface and potentially create new systems such as the wireless power transfer system or IoT (internet of things) dashboard, over time.

3.3 Hardware Design

The hardware implementation comprises many sensing, control, and communication components integrated into one board. The main modules are explained in this section.

3.3.1 RFID Reader

The RFID reader will detect passive RFID tags, which will operate at 13.56 MHz The RFID reader will connect to the microcontroller through UART or SPI interface. Once the tag is within range, the reader will pass along the unique tag identification to the microcontroller for identification and conformation of access.

3.3.2 Microcontroller (ATmega328P)

The ATmega328P is the 8-bit microcontroller often used in Arduino Uno boards. The microcontroller processes serial communications data, and microcontroller peripheral implementations. The microcontroller is programmed to:

- Authenticate users based on RFID tag ID
- Calculate energy units based on the balance available to the user
- Control relay switching
- Update the user account

3.4 Software Components

Software design determines how to process data, authentication, and communication. The firmware is implemented in Embedded C (Arduino IDE) and incorporated into an IoT dashboard for monitoring purposes.

The software specifications include the following main features:

- Checking RFID tags and mapping to database entries.
- The calculation logic for balance and tariffs.
- Control of the relays depending on whether to charge.

The software also allows for potentially creating scalability for cloud dashboards (continued cloud work will be on platforms).

3.5 Procedure and Flowchart

The sequence starts with initialization, followed by RFID detection, validation, and session management. The logical flow ensures that charging only occurs after authentication and the balance has been checked.

1. Begin system initialization
2. Scan for RFID
3. If tag is valid, retrieve user information
4. Calculate allowed units based on balance
5. Begin the charging session and monitor energy consumption
6. End charging when units have been consumed, or SOC limits have been reached
7. Go idle.

3.6 Communication and Data Flow

There is a bidirectional exchange between the charging hardware and the cloud server. Data including RFID ID, energy usage, and user balance are transmitted securely over either GSM or IoT communication protocols. In summary, the upstream flow is RFID → Microcontroller

→ Cloud Database and downstream flow is Cloud → Microcontroller → User Interface. This provides a means for accurate, up-to-date communication between hardware and user data to ensure accurate billing.

3.7 Advantages of the Design

- Energy access that is verified and securitized
- Transparency and real-time billing
- An automated operation that requires little human interaction
- Ability to scale to multiple users
- Easily integrated with IoT cloud

CHAPTER 4
METHODOLOGY

The Smart RFID-Enabled Prepaid Charging System methodology provides the logical process that the above information followed in relation to the design, development, and realization of the prototype. The methodology involves considerable hardware, software, and communication infrastructures working together to support seamless system automation, and is usually broken down into several operational phases, starting from RFID-based authentication stage, through to session end, and billing. Each of these different phases are logically linked to requisite communication and system processes, to provide assurance that the system can perform all its tasks with correctness and efficiency. In general, the overarching methodology involves automation, with particular attention to security and user convenience, gained using RFID, IoT, and GSM based communication technologies. The next sections explain the details of each of the phases.

4.1 Overview of the Proposed System

The suggested system is an autonomous energy management system, with the user's RFID card being the user's digital identity access to energy. The process begins with the user scanning their RFID tag in proximity to the reader. The system calls the user ID and checks the data from the database. Once the user is validated, then the microcontroller retrieves the prepaid value account of the user and calculates the billable energy units for that charge. If a positive dollar amount is found in the prepaid value account, the charger relay will become engaged, and the flow of energy will begin to charge. While charging, the energy meter will measure the user energy usage and the microcontroller will measure that consumption in real-time from the energy meter. When the user is approaching the prepaid value limit, the relay will de-energize automatically, and update the prepaid value account.

4.2 Phase 1: Login and Session Preparation

4.2.1 System Initialization

The microcontroller initializes all peripheral devices like RFID reader, GSM module, and energy meter. The system then enters an idle mode, continuously scanning for nearby

RFID tags.

4.2.2 RFID Tag Detection and UID Reading

As soon as a user comes into range of the RFID reader with the RFID card, the reader reads the tag's Unique Identification Number (UID). Immediately afterwards, the UID is sent to the microcontroller through serial communications (UART/SPI). Once the UID received is valid, the UID is reviewed against the user database that is locally or remotely stored on the server.

4.2.3 Database Communication

The UID is sent by the controller to either a remote web server or a local database. The server will respond back with user-specific information, such as:

- Username
- Account number
- Prepaid balance

4.2.4 Balance and Unit Calculation

The controller determines the maximum number of units that can be allowed based on the current cost of electricity per unit and the user's balance.

For example, if the user's balance is ₹70 cost of electricity per unit is ₹7 , the controller would allow the user to charge 10 units.

4.2.5 User Input and Validation

The system prompts the user to do one of the following:

- Insert the number of units to be charged, or
- Insert an amount to be charged (which the system will change to a few units).

4.3 Phase 2: Charging and real-time monitoring

4.3.1 Session Start

Upon successful authentication and verification, the microcontroller:

- Logs the start time.
- Turn the relay module on to create a power connection.

- Initiates charging through the energy meter.

4.3.2 Energy Measurement

The energy meter continuously measures current (I) and voltage (V). The microcontroller computes instantaneous power P=V×I and accumulates energy consumption over time in kilowatt-hours (kWh).

4.3.3 Real-Time Monitoring

The system includes continuous monitoring during a charging session for the following activities:

- Energy Units Delivered – Ensures that the energy units charged do not exceed the paid-for limit.
- State of Charge (SOC) – Optionally can monitor the SOC of the vehicle if connected to the BMS.
- Manual Interrupt – Detects the user has unplugged/disconnected the EVSE or power failure.

4.3.4 Data Logging

The microcontroller keeps a record that contains the:

- User ID
- Start and end time
- Energy usage
- Remaining balance

These records are stored locally and updated to the remote server on a regular basis.

4.4 Phase 3: Disconnection and Billing

4.4.1 Charging Termination

The charging process will cease once one of these conditions has been satisfied when:

- The requested number of units has been supplied.
- The prepaid balance has reached zero.
- The user disconnects manually.
- The battery of the EV has charged to a 100% SOC.

After the charging has ceased, the microcontroller will then:

- Deactivate the relay to disconnect the power supply.

- Record the end time.
- Log the session information to calculate billing.

4.4.2 Billing and Account Update

The final deduction will be obtained by multiplying the total units consumed by the tariff rate. The microcontroller will then debit the account balance of the user to account for the amount billed.

For example: 5 units consumed × ₹7/unit then the total deduction will be ₹35.

The remaining balance will be displayed in the database.

4.4.3 System Reset

After successful billing, the system resets to its idle state, ready to serve the next user. The relay remains open until another authenticated user tag is detected.

4.5 Advantages

- Automation: Enhanced user interaction with minimal human involvement.
- Secure Access: Authorized users just start charging.
- Real-Time Monitoring: Monitoring, plus checks for fraud during charging.
- Transparent Billing: Real-time payment capabilities will shorten the distance between estimated billing and billing based on manual activation.
- Scalability: Can accommodate a large number of charging locations.
- Streamlined: Fast, touchless, cash-less, EV charging experience.

CHAPTER 5
PROJECT DESIGN

The enhanced prepaid charging infrastructure uses Smart RFID technology in order to provide users with an efficient way to manage their EV charging in uncomplicated, automated, and safe manner. The infrastructure is designed so the only suitable users can have charging access, by authenticating their RFID tags with a smart RFID reader connected to an Arduino Uno microcontroller.

The design of the project consists of two sections:

1. Hardware Design, which consists of the physical components and circuitry used for the prototype
2. Software Design, which defines the logical flow and programming that describes the physical system's operation.

Both hardware and software work in conjunction with one another to provide an effective operation with a contactless authentication approach to control the charging outlet.

5.1 Overview of Project Design

The system that has been developed operates on a basic principle. When someone brings their RFID tag into the RFID reader's range, the Arduino will read the tag ID. If the ID equals one of the authorized tags stored in memory, it sends a signal to close a relay and power up the charger, allowing current to flow to the electric vehicle. If the tag is taken away or is a non-authorized counterpart, the relay will open back and shut off the supply.

5.2 Hardware Design

5.2.1 Components Used

1. **Arduino Uno (ATmega328P Microcontroller):**
   In this system, an Arduino Uno serves as the controller. The Arduino Uno receives signals from the RFID reader, processes the tag data, and outputs a control signal to the relay when needed.
   - Operating Voltage: 5V DC
   - Clock Rate: 16 MHz
   - Digital I/O Pins: 14

- Analog Pins: 6
- Communication Protocols: UART, SPI, I²C

Fig 5.1 – Arduino Uno

2. RFID Reader Module (RC522)

The RFID reader is designed to identify users without needing to contact them. It operates at 13.56 MHz and communicates with Arduino via the SPI protocol. Whenever a tag is brought near the RFID reader, it will read the UID of the tag.

- Operating Voltage: 3.3V
- Communication: SPI
- Range: 2-5 cm
- Frequency: 13.56 MHz

Fig 5.2 – RFID Reader Module

3. RFID Tags

RFID tags are tiny cards or key fobs equipped with a unique code for each authorized user.

They are self-powered and do not run off of a power source but are powered by the electromagnetic field of the RFID reader.

- Name: Passive RFID Tag
- Frequency: 13.56 MHz
- Range: Up to 5 cm
- Memory Type: EEPROM

Fig 5.3 – RFID Tag

5.2.2 Circuit Connections

All components work together as shown below:

Component	Arduino Pin	Function
RFID Reader SDA	D10	Slave Select (SPI)
RFID Reader SCK	D13	Clock Signal
RFID Reader MOSI	D11	Data Output from Arduino
RFID Reader MISO	D12	Data Input to Arduino
RFID Reader RST	D9	Reset Pin

Table 5.1 – Circuit Connections

The RFID reader sends tag data to the Arduino for processing, then sends control signals to the relay to check if the tag is authorized or not.

5.2.3 Working Principle of Hardware

- Power is supplied to the system, and the Arduino initializes all attached components.
- The RFID reader scans constantly for RFID tags that are nearby.

- If a tag is in range, it will read the UID and transmit it back to the Arduino.
- The Arduino will check the UID against previously stored IDs that have been authorized.
- If the ID is authorized, the relay will be turned ON, and the socket will activate for charging and if the ID is unauthorized, the relay will remain OFF.
- The system will return to idle status, waiting to read the next tag.

5.3 Software Design

The firmware section displays the software that drives the hardware. The entire application is implemented in Embedded C, in the Arduino IDE.

5.3.1 Software Requirements

Software Tool	Purpose
Arduino IDE	Development of programs and upload to board
Embedded C	Programming language and control logic
SPI (Serial Peripheral Interface) and MFRC522 Libraries	Communication and transfer data between the Arduino and RFID module
Serial Monitor	Testing and debugging purposes with your output

Table 5.2 – Software Requirements

5.3.2 Software Implementation Process

- Initialization: The IoT SPI communication process initiates with the Arduino establishing the relay pin for digital output. The RFID scanner will begin power settings and configuration to start scanning tags.
- Tag Detection: The Arduino will begin a continuous scan for any of the newly designed RFID tags that move into the range of the reader.
- Reading UID: Once the tag is detected, the UID will be read, and it will be shown in a human-readable format.
- Validating UID: The UID from the previous read tag will be matched to valid UIDs residing on the Arduino in EEPROM.
- Activating the battery charging:
  - If the previous actions detected a valid UID, the battery starts charging.

- If it was not a valid UID, the relay will remain OFF, access denied.

- Status output: The Arduino will write to the Serial Monitor (or optional LCD etc.) for its detected access and logs to the status, either allowing access or denying access.
- Idle Mode: Once it has printed the status of the message, it will switch back into scan mode for the next detected tag.

5.4 Advantages of the Design

- Delivers protected and contactless authentication for purposes of charging.
- Utilizes inexpensive, off-the-shelf components.
- Automates access to charging without supervision by an individual.
- Can incorporate IoT or payment modules easily.

CHAPTER 6
RESULT

The process of development and testing of the Smart RFID-Enabled Prepaid Charging Infrastructure system has demonstrated that the system is functional and dependable. The system was tested in terms of operational performance, whereby the system successfully authenticated users through RFID tags and controlled the charging circuit through a relay module. Users were either authenticated to permit or prevented access when unauthorized as evidence of a reliable automated system.

6.1 Experimental Setup

The arrangement of the equipment involves the following components:

- Arduino Uno board - For control.
- RFID Reader: reads the RFID tags.
- RFID Tags: Two samples of authorized and unauthorized tags for the testing procedure.

The Arduino and components were arranged on a breadboard and powered via the Arduino USB port.

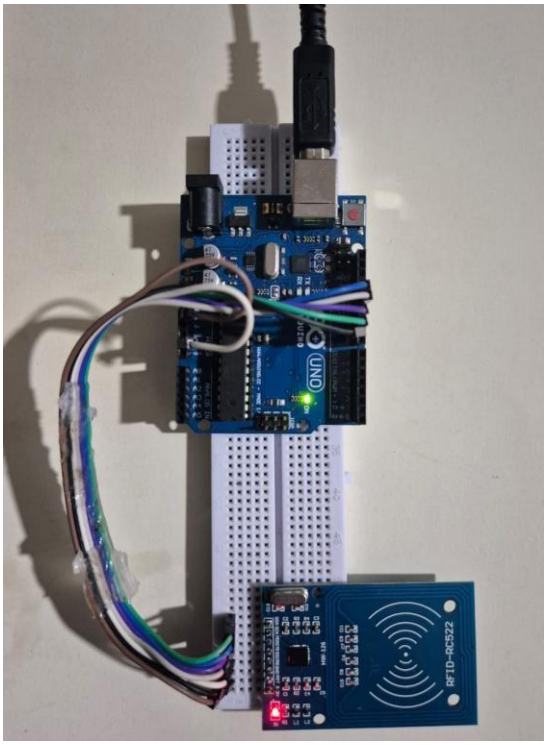

Fig 6.1 - Experimental Setup of the Smart RFID-Based Charging System

6.2 Testing Procedure

The testing procedure occurred using the steps below:

- Power ON the Arduino and entire configuration.
- The RFID reader was enabled in scan mode, and scan initiated for tags nearby.
- Bi-focal tags were placed close to the RFID reader to test for activation at a short distance.
- The tags were valid and invalid alternately.

The test was run multiple times to ensure reliability and consistency.

6.3 Observed Results

The system's performance was measured across multiple test cases. The results can be seen in the table below.

Test Case	Tag Type	System Response	Relay/LED Response	Serial Monitor Output
1	Authorized Tag 1	Access Granted	ON	"Access Granted – Charging Started"
2	Authorized Tag 2	Access Granted	ON	"Access Granted – Charging Started"
3	Unauthorized Tag	Access Denied	OFF	"Access Denied – Invalid Tag"
4	No Tag Present	Idle Mode	OFF	"Waiting for RFID Tag…"

Table 5.3 – Results Observed

6.4 System Response

- Upon scanning a valid RFID tag, the system instantly recognized the UID of the tag as being registered. The indicated system was in the charging state.
- Upon scanning an invalid tag, the UID did not match any of the stored IDs. The relay remained OFF, which prevented entry, and the Serial Monitor output an "Access Denied" message.
- When there was no tag detected, the system remained idle while continually scanning new tags.

6.5 Stability and Error Handling

The prototype was subject to multiple continuous runs to test stability. The following were observed:

- Consistent stable tag detection, and reliable relay operation after many scans.
- All unauthorized tags were denied correctly during every test.
- The prototype re-established connection without issue (auto-recovery) from short power interruptions.
- No spurious triggering no misreads during testing.

All hardware and software components remained stable and consistent with no irregularities throughout all tests or continuous runs.

6.6 Advantages

- Quick and Contactless Verification: The tag detection and relay operation happen almost instantaneously, without physical contact.
- Simple to Use: Users only need to scan their tag to start or stop the flow of energy.
- Low Power Requirements: Functionality is available with low, DC power.
- Lightweight: The prototype can be easily relocated given minimal design restraints.
- Secured User Access: Limits user access to prevent accidental operation, from unauthorized users.

6.7 Limitations

The prototype operated, however, there were issues:

- The RFID detection range is less than optimal, just a few centimeters.
- The current system handles only one user at a time.
- The management of the prepaid balance is not automated in this version.

CHAPTER 7
CONCLUSION

The initiative "Smart RFID-Enabled Prepaid Charging Infrastructure" was successfully designed and accomplished to create a secure, automatic, and contactless energy control system for electric vehicles. The initiative was inspired by the need for smart, user-specific, and efficient charging options in conjunction with the increasing demands for electric mobility. The initiative utilized RFID technology that is integrated into an Arduino-based automated system, which appropriately explored a prototype that was able to authenticate the user and manage prepaid access to the charging facility.

Essentially, the system relies on RFID authentication to control access to the charging process by registered users only. When the RFID tag that is registered is detected, the Arduino controller sends a signal to the relay circuit to complete the circuit and to supply power to the vehicle or load. When the RFID is read, registered or unregistered, to control the charging process, which keeps access to the charging process secure and definitive of misuse. This simple mechanism of operation ensures little to no human intervention and means that energy access is controlled with precision.

After the completion of the design process, significant attention was given to ensuring that the design was modular, reliable, and efficient to operate. The hardware (Arduino Uno, a RC522 RFID reader, RFID tags, and a relay module) was selected because of its compatibility, cost-effectiveness, and multiplicity of available examples to design from. The software was created in the Arduino IDE to read tag data, validate unique identifiers, and quickly control the relay in real-time through logical flows and conditional statements. The designed system continuously operated with low response time, low power consumption, and accurate detection of tags under each replication condition during testing.

The tested prototype was put through rigorous testing in numerous situations using valid and invalid tags. The results confirmed the accuracy, stability, and reliability of the system. Receiving tags initiated the relay as required and showed the reliability of the design. Response time for the detection of the tags and the activation of the relay was less than 1 second, demonstrating that the system can adequately perform in real applications. Overall, the results validated that RFID technology combined with microcontroller control can effectively be

applied to an access system to streamline the pre-payment options in a charging environment.

A significant result of this project is the showcasing of how inexpensive embedded systems can be used to build secure and scalable infrastructure for modern energy applications. The project achieved its primary goals:

- To provide secure authentication via RFID,
- To control automatic switching of the charging circuit, and
- To create a prepaid access model with minimal hardware.

This supports the plausibility of microcontroller-based automation for practical smart grid and energy management applications.

On a more significant scale, this project adds to the market of smart charging systems by offering a small, dependable, and easily deployable system. In addition to providing security and user functionality, it provides a foundation for future developments, such as real-time billing, IoT-monitoring, and a multi-point charging network. The prototyping of this is an example of how embedded electronics and RFID technologies combined can offer viable, sustainable, and smart charging infrastructures for the next generation of electric vehicles.

In conclusion, the Smart RFID-Enabled Prepaid Charging Infrastructure represents a reasonable and well-tested demonstration of secure prepaid charging using inexpensive hardware and relatively simple programming logic. The fact that the system can credibly authenticate users and can automatically control energy delivery presents the possibility of applying with such systems in larger public or private EV charging stations. Thus, this project offers a plausible step towards creating intelligent, expandable, and environmentally-friendly charging ecosystems that will add significant value to initiatives and development of sustainable energy technologies and intelligent transportation systems.

REFERENCES

[1] K. Papapostolou et al., "Development of a Smart Electric Vehicle Charging Station Management System," in Proc. 28th Pan-Hellenic Conf. on Informatics (PCI '24), Egaleo, Greece, 2024.

[2] R. Bhatti et al., "Electric Vehicle Charging Stations and the Employed Energy Management Schemes: A Classification Based Comparative Survey," Discover Applied Sciences, 2024, doi: 10.1007/s42452-024-06190-9.

[3] J. J. Jacob et al., "Electric Vehicle Wireless Charging Using RFID," in E3S Web of Conferences, vol. 399, Article 01010, 2023, doi: 10.1051/e3sconf/202339901010.

[4] M. M. Hassain et al., "Electric Vehicle Charging System Using RFID and IoT for Enhanced User Experience," in Proc. MENACOMM 2025, 2025, doi: 10.1109/MENACOMM62946.2025.10911013.

[5] V. Shivank et al., "Implementation of RFID Based Smart Electric Vehicle Charging System," Int. J. Emerging Technologies and Innovative Research (JETIR), vol. 11, no. 4, pp. n722–n727, Apr. 2024, ISSN 2349-5162.

[6] S. K. Goud and R. Kumar, "Smart Electric Vehicle Charging Station Using IoT," J. Emerging Technologies and Innovative Research (JETIR), vol. 12, no. 5, pp. 483–490, 2025, ISSN 2349-5162.

[7] Ajithkumar et al., "Smart E-Vehicle Charging System Using RFID," Int. J. Research and Analytical Reviews (IJRAR), vol. 7, no. 3, pp. 248–252, 2020, E-ISSN 2348-1269, P-ISSN 2349-5138.

[8] R. Teymourzadeh et al., "RFID-Based Prepaid Power Meter," in Proc. IEEE Student Conf. on Research and Development, Putrajaya, Malaysia, 2018, pp. 301–304, doi: 10.1109/SCOReD.2013.7002594.