IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125331

Authorized vehicle parts recognition and alerting system for Ev vehicle

Dr. R Manjunatha[1], Janya L S[2], Inchara K[3], Madhumati I K[4], Manohari K V[5]

Associate Professor, Electronics and Communication, P.E.S College of Engineering, Mandya, India[1]

Student, Electronics and Communication, P.E.S College of Engineering, Mandya, India[2-5]

Abstract: The project aims to enhance the safety and authenticity of Electric Vehicle (EV) components by implementing a system that distinguishes authorized (original) and unauthorized (duplicate) products. Using the BQ2026 for identification and the ESP32 for control, the system verifies product authenticity via unique identification numbers. Authorized components activate the corresponding port's power supply via MOSFETs, while unauthorized ones trigger power cut-offs, display warnings, activate a buzzer, and send alerts through the Blynk app. This innovative approach ensures EV reliability, reduces counterfeit risks, and provides real-time notifications to users.

Keywords: Electric Vehicle (EV), BQ2026 (Battery Management Identification IC BQ2026), ESP32 (Espressif Systems Microcontroller ESP32), MOSFETs (Metal-Oxide-Semiconductor Field-Effect Transistors), IC (Integrated Circuit), Blynk app (Mobile IoT Application for Real-Time Monitoring and Control)

I. INTRODUCTION

Counterfeit products in electric vehicle (EV) systems present serious risks, including compromised safety, reduced performance, and diminished durability, making them a growing concern for manufacturers and users alike. Unauthorized components can lead to unexpected failures, increased maintenance costs, and potential safety hazards, negatively impacting the overall efficiency of EVs. To mitigate these risks, this project introduces an advanced identification system capable of differentiating original and duplicate EV components, ensuring the use of authentic parts.

Utilizing the BQ2026 identification IC and the ESP32 microcontroller, the system enables precise authentication of EV components by verifying their unique identification numbers. This approach ensures that only authorized products are used in vehicle operations, thereby improving reliability and preventing counterfeit-related damages. Additionally, the system integrates modern mobile app technology, allowing real-time monitoring and instant alerts for unauthorized components. If counterfeit parts are detected, the system triggers power cut-offs, displays warning notifications, activates a buzzer, and sends alerts via the Blynk app, ensuring immediate user awareness and action.

By enhancing EV security and authenticity, this system strengthens industry standards, fosters trust among users, and contributes to safer and more dependable electric mobility solutions.

II. RELATED WORK

[1] Vehicle Part Authentication Using Deep Learning authored by D.Thomas, A.Delahaies (2020): The above paper proposes a novel method for verifying the authenticity of Vehicle parts using deep learning techniques. It addresses the growing issue of counterfeit auto parts, which can compromise vehicle safety and performance. Applicability: Utilizing the datasets the paper can enhance the accuracy of model, particularly for EV-specific parts and enables real-time monitoring and alerting users if unauthorized parts are detected.

[2] Counterfeit Part Detection in Automotive Supply Chain authored by Kunal Wasnik, Isha Sondawle, Rushikesh Wani (2019): In This research, it explores the integration of blockchain technology and the Internet of Things (IoT) to combat counterfeit parts in the automotive industry. From this paper, Integrating IoT devices provides alerts when unauthorized components are detected. This approach not only enhances security but also improves traceability and allows for quick identification of counterfeit parts.

[3] Image-Based Vehicle Part Recognition authored by W.Clarkson, T. Weyrich (2018): This paper examines the use of computer vision techniques for identifying vehicle parts, focusing on improving accuracy while addressing challenges. It highlights applications in automotive manufacturing, maintenance, security, and counterfeit detection.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125331

Machine learning and image processing enhance classification and verification of components. Challenges include variations in lighting, occlusions, and complex vehicle designs. The paper compares methodologies to optimize identification accuracy. Advancements in feature extraction and neural networks contribute to efficiency. Findings support intelligent EV authentication systems and reliable automotive solutions. Let me know if you need any refinements.

[4] Counterfeit detection based on the unclonable feature of paper using a mobile camera authored by W. Wong and M. Wu (2017): This paper focuses on the distinction between genuine and counterfeit items, ensuring that the detection process is both efficient and user-friendly. By leveraging advanced identification techniques, the system aims to improve accuracy while minimizing complexity, allowing for seamless authentication of products. One of its key strengths is its accessibility, as mobile cameras enable users to verify items without the need for specialized equipment. This technology empowers consumers, mechanics, and service providers by providing a reliable tool for verifying authenticity in real time. It enhances security and trust in various industries by preventing counterfeit products from entering the supply chain. The integration of mobile-based detection methods ensures widespread usability, making it a practical solution for everyday applications in product verification and quality assurance.

[5] Electric Vehicle Market Trends authored by C. Jin, J. Tang, P. Ghosh (2020): This paper examines the growing electric vehicle (EV) market, focusing on consumer adoption, battery technology advancements, and environmental awareness. Increased EV adoption is driven by affordability, government incentives, and sustainability concerns. Innovations in battery technology enhance energy efficiency, charging speed, and lifespan, supporting widespread use. Environmental awareness and regulations promote cleaner energy and lower emissions. To maintain brand integrity and customer trust, preventing unauthorized parts is crucial. Ensuring only genuine components are used improves reliability, safety, and consumer confidence, reinforcing the credibility of EV manufacturers.

III. PROPOSED MODEL

Methodology*:*

The proposed system utilizes the ESP32 microcontroller as the central processing unit, managing identification, authentication, power control, and alert mechanisms to ensure the security and authenticity of EV components. The methodology follows a structured approach to efficiently verify authorized and unauthorized parts, preventing counterfeit products from compromising vehicle safety and performance. The identification process is executed using the BQ2026 identification IC, which contains a unique 64-bit ROM ID for each component. The ESP32 communicates with the BQ2026 via the 1-Wire protocol, a simplified interface requiring only a single GPIO pin for data transfer. Once retrieved, the ROM ID is compared against a predefined list of authorized IDs stored in the ESP32's memory. If a match is found, the system allows normal operation; otherwise, it initiates countermeasures to prevent unauthorized use.

To regulate power supply, the ESP32 controls MOSFETs, enabling or disabling individual ports based on the authentication result. Authorized components are granted access to power, while counterfeit or unauthorized products trigger automatic power cut-offs, preventing potentially unsafe or unreliable components from functioning within the system. Additionally, immediate alerts are generated through multiple feedback mechanisms. A buzzer is activated to provide an audible warning, LEDs illuminate to indicate component status, and warning messages are displayed on a 16x2 LCD screen connected via the I2C protocol. The LCD serves as an intuitive interface, displaying messages such as "Duplicate Item on PORT1" or "All items are genuine," ensuring users receive clear and immediate feedback regarding their system's status.

To enhance remote monitoring capabilities, the system integrates cloud connectivity using the ESP32's built-in Wi-Fi module. The microcontroller connects to the Blynk cloud platform, allowing real-time alerts to be sent directly to users' mobile devices through the Blynk app. When an unauthorized product is detected, the ESP32 transmits a notification to the cloud, instantly pushing alerts to the user's smartphone, ensuring timely intervention even when they are away from the system. This feature not only improves convenience but also strengthens security by enabling proactive monitoring. Through rigorous testing and optimization, the methodology ensures seamless integration of hardware and software components for reliable, real-time authentication. By combining efficient identification techniques, automated alerts, local feedback systems, and cloud-based monitoring, the system provides a robust solution for preventing counterfeit EV parts. Its structured approach minimizes risks associated with unauthorized components, enhancing security, reliability, and compliance with industry standards. Ultimately, this comprehensive system contributes to a safer and more trustworthy EV ecosystem by ensuring the use of genuine components and preventing unauthorized modifications

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125331

Working Principle:

The ESP32 microcontroller serves as the **central processing unit** of the system, managing all operations related to component identification, authentication, and control. It plays a crucial role in ensuring the proper functioning and security of the system by orchestrating interactions between different hardware modules. One of its primary functions is to read **unique identification numbers** from the **BQ2026 chips** via the **1-Wire communication protocol**, which uses a single **GPIO pin** to transfer data efficiently. This protocol simplifies wiring while ensuring reliable data exchange between the ESP32 and identification chips. The retrieved **64-bit ROM ID** is then compared against a **predefined list of authorized product IDs** stored in the ESP32's memory.

Based on the authentication results, the ESP32 decides the appropriate course of action. If the ID matches an authorized product, the microcontroller **enables power supply** to the respective port by controlling **MOSFETs**, ensuring seamless operation of genuine components. However, if an unauthorized product is detected, the system **cuts off power** to prevent counterfeit parts from functioning, thereby maintaining component integrity and safety. Additionally, the ESP32 initiates multiple warning mechanisms, including activating a **buzzer** to produce an audible alert, updating the **LCD display** with status messages, and **illuminating LEDs** to indicate the component's authorization status. The LCD, a **16x2 display module**, is connected via the **I2C protocol**, which requires only two communication lines—**SDA (data line)** and **SCL (clock line)**—for efficient data transmission. The display provides users with real-time status updates such as "**Duplicate Item on PORT1**" or "**All items are genuine**", ensuring immediate awareness of system conditions.

Beyond local alerts, the ESP32 extends its capabilities through **cloud connectivity**, utilizing its built-in **Wi-Fi module** to integrate with the **Blynk app** for remote monitoring and notifications. Once an unauthorized component is detected, the ESP32 sends a **real-time alert** to the **Blynk cloud platform**, which then pushes notifications directly to users' mobile devices. This remote functionality allows users to monitor and respond to security threats efficiently, even when they are not near the system. By combining **hardware authentication, power control, real-time feedback, and cloud integration**, the ESP32 ensures **comprehensive security and reliability** in EV component management. This advanced approach not only prevents counterfeit product usage but also enhances user convenience, system performance, and industry compliance. Let me know if you need any refinements.

System Design Approach:

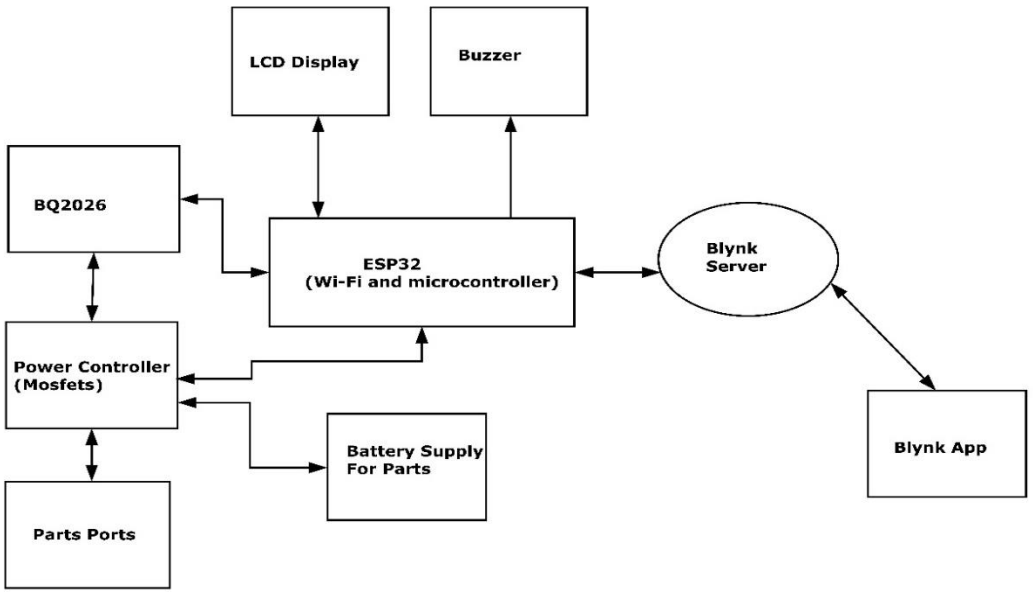

Fig. 1 Block diagram

The fig illustrates the system block diagram where it combines efficient hardware and software integration. The ESP32 acts as a central hub, interfacing with the BQ2026 for identification, controlling peripherals like the LCD, LEDs, and buzzer, and connecting to the cloud for remote notifications. This comprehensive setup ensures real-time detection and effective alerts for authorized and unauthorized products in EVs.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125331

Proposed Workflow:

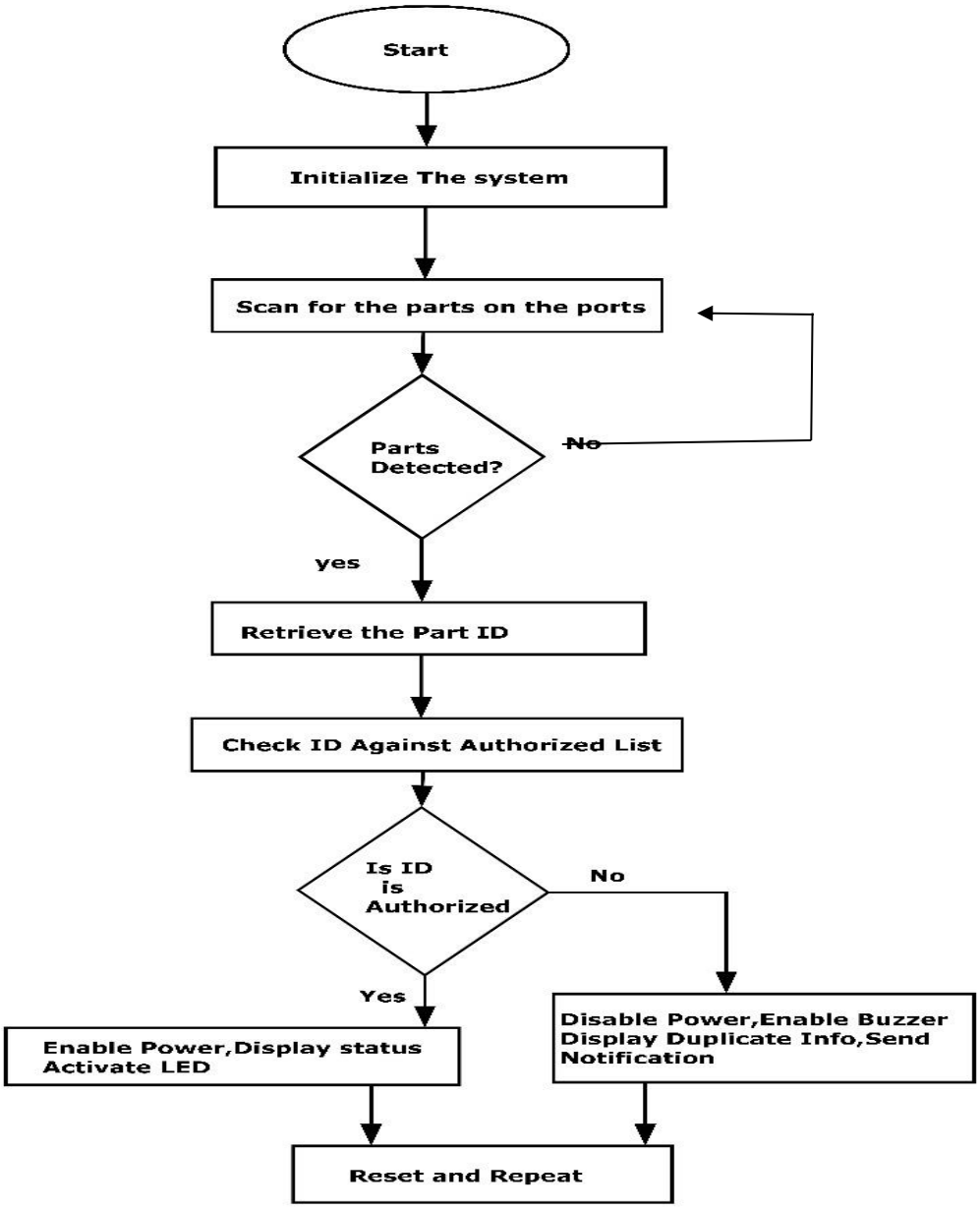

Fig. 2 Flow chart

The process begins with the initialization of the system, where the sink node is powered on and its internal components are prepared for operation. It then scans the available ports to check for any connected devices or parts. If parts are detected, the system proceeds to retrieve their unique identification (ID) using the BQ2026 chip via the 1-Wire communication protocol. Once the ID is obtained, it is compared against a pre-configured list of authorized component IDs stored within the ESP32 microcontroller. If the ID matches an authorized part, the system enables power to the respective port, displays the connection status on the LCD, and activates an LED to indicate successful authentication. However, if the component is unauthorized, the system disables power to the part, activates a buzzer to alert the user, and displays an error message indicating the presence of a duplicate or unauthorized product. Additionally, a notification is sent to the designated monitoring system via the Blynk app to ensure remote awareness and timely intervention. After executing these actions, the system resets and loops back to the scanning step, continuously checking for new or modified connections. This iterative approach maintains real-time verification, ensuring the authenticity and security of vehicle components in an efficient and automated manner. Let me know if you need further refinements.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125331

IV. RESULT

The system successfully identified authorized and unauthorized EV components using the BQ2026 chip and the ESP32 microcontroller. The ESP32 read the unique 64-bit ROM ID from each BQ2026 chip and compared it with a list of authorized IDs stored in memory. If the ID matched, the product was authorized; if not, it was classified as unauthorized..

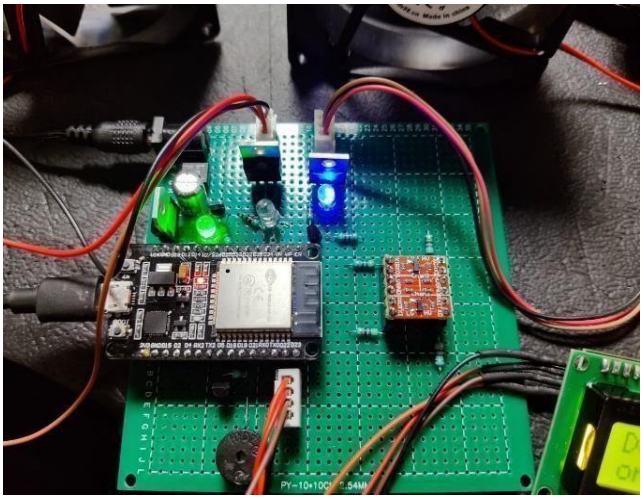

Fig. 3 Circuit connection

Fig. 4 Authorized product

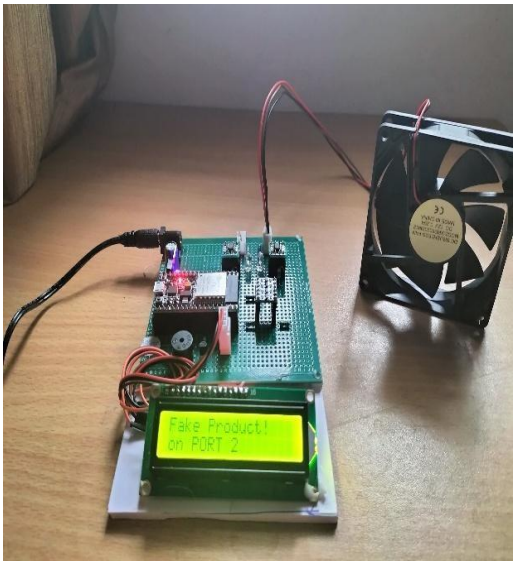

Fig. 5 Unauthorized product

The figure illustrates the detection of authorized and unauthorized components, with the ESP32 processing identification data from the BQ2026 chips. The LCD screen displays real-time status updates, indicating whether the detected components are genuine or duplicates.

V. CONCLUSION

The proposed system effectively ensures the authenticity and security of electric vehicle components by integrating advanced identification, power control, and alert mechanisms. Utilizing the ESP32 microcontroller, the system orchestrates operations by retrieving unique IDs from BQ2026 chips via the 1-Wire protocol, verifying them against a predefined database of authorized products. If an unauthorized component is detected, it triggers immediate

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125331

countermeasures, including power cut-offs, buzzer alerts, LED indicators, and real-time notifications displayed on an LCD screen. Furthermore, the system seamlessly connects to the cloud via Wi-Fi, enabling remote monitoring through the Blynk app for enhanced user awareness and timely intervention. By implementing these real-time verification and alerting features, the system significantly reduces counterfeit risks, enhances EV reliability, and ensures compliance with industry standards. The integration of hardware authentication with cloud-based monitoring establishes a robust solution that improves safety, transparency, and trust in the EV ecosystem. Ultimately, this approach strengthens the security of electric vehicles while promoting sustainable and reliable maintenance practices.

ACKNOWLEDGMENT

We express our heartfelt gratitude to the Department of Electronics and Communication Engineering, PES College of Engineering, Mandya, for providing the necessary resources and a conducive environment to carry out this work. We extend our sincere thanks to our guide, **Dr. R Manjunatha**, Associate Professor, for his constant support, technical guidance, and valuable feedback throughout the project. We also acknowledge the encouragement and moral support from our families and peers during the course of this research.

REFERENCES

[1]. “Vehicle Part Authentication Using Deep Learning” D.Thomas,A.Delahaies (2020)
[2]. “Counterfeit Part Detection in Automotive Supply Chain" Kunal Wasnik, Isha Sondawle, Rushikesh Wani (2019).
[3]. “Image-Based Vehicle Part Recognition" Kunal Wasnik, Isha Sondawle,Rushikesh Wani (2018).
[4]. "SmartVehicle Part Authentication System" Kunal Wasnik,Isha Sondawle,Rushikesh Wani (2020).
[5]. "Electric Vehicle Market Trends"C.Jin, J.Tang, P.Ghosh(2020).
[6]. “Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment” Mohammad wazid (2017).
[7]. “An IoT-Based Anti-Counterfeiting System Using Visual Features on QR Code” Yulong Yan (2020)
[8]. “Counterfeit detection based on the unclonable feature of paper using a mobile camera,” W.Wong and M. Wu (2017).
[9]. “A watermarking technique to secure printed QR codes using a statistical test,” H. P. Nguyen, A. Delahaies, F. Retraint, D. H. Nguyen, M. Pic (2017)

