IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

RoboShop-Cart – An Intelligent Trolley

Dr. Nitin Dhawas[1], *Professor, Electronics and Telecommunication,*
Nutan Maharashtra Institute of Engineering and Technology, Talegaon, Pune E-mail: nitin.dhawas@nmiet.edu.in
Simarpreet Kaur Chawla[2], *Student, Electronics and Telecommunication,*
Nutan Maharashtra Institute of Engineering and Technology, Talegaon, Pune E-mail: simarchawla767@gmail.com
Samruddhi Kakade[3], *Student, Electronics and Telecommunication,*
Nutan Maharashtra Institute of Engineering and Technology, Talegaon, Pune E-mail: samruddhikakade167@gmail.com
Abhishek Lavate[4], *Student, Electronics and Telecommunication,*
Nutan Maharashtra Institute of Engineering and Technology, Talegaon, Pune E-mail: abhisheklavate1751@gmail.com

Abstract
In this paper, we present an innovative Internet of Things (IoT) system designed specifically for retail applications, with a primary focus on enhancing operational efficiency and improving customer experience. Our system leverages NodeMCU as the central controller and integrates ESP32 for advanced human-following capabilities, offering a comprehensive solution to meet the diverse needs of modern retailers. Key features of our system include automatic billing and a human-following robot, both of which contribute to creating a transformative retail environment.
The automatic billing component utilizes RFID technology and sensors to facilitate quick and precise transactions, streamlining the checkout process for both customers and retailers. NodeMCU, chosen for its enhanced connectivity and versatility, efficiently coordinates these functions, providing a robust platform for seamless billing processes.
In addition to automated billing, our system incorporates a Bluetooth-controlled human-following robot powered by the ESP32 controller. This robot adds an interactive and futuristic element to the retail landscape, engaging customers in a novel and captivating manner. By intelligently tracking and following human movements, the robot enhances customer interaction and contributes to a more immersive retail experience. The integration of NodeMCU and ESP32 controllers addresses common challenges faced in the retail sector, offering improved connectivity, scalability, and advanced human-following capabilities. Real-world testing confirms the efficacy of our system, demonstrating its potential to redefine retail experiences through a combination of automated billing and cutting-edge human-following technology. By seamlessly coordinating these functionalities, our dual-controller system showcases the versatility and transformative impact of advanced IoT applications in the dynamic realm of retail. The result is an innovative and adaptable system poised to elevate efficiency, customer engagement, and overall retail experiences to new heights.

1. INTRODUCTION

In the rapidly advancing technological landscape, the " "Secured Energy Transfer via Bluetooth Encryption"" paper stands out as a beacon of innovation, poised to revolutionize power management in electrical systems. As the demand grows for efficient, user-friendly, and secure solutions, this study introduces a pioneering approach, seamlessly integrating Bluetooth technology into power supply systems. The convergence of Bluetooth's convenience with the robustness of password-based access control represents a significant advancement in enhancing accessibility and control within electrical infrastructures.

While traditional power circuit breakers remain crucial, they are undergoing transformation as modern methods of operation and control evolve. This paper focuses on introducing an avant-garde methodology, utilizing Bluetooth connectivity as the pivotal communication bridge between users and power circuit breakers. This connection improves accessibility while also streamlining the level of control users can exert over power distribution.

At the core of this innovation is the concept of an " "Secured Energy Transfer via Bluetooth Encryption"" a security mechanism designed to control access to systems or devices. Drawing parallels to physical circuit breakers that interrupt power flow during faults, this paper adapts the concept to the digital realm. Here, a password serves as the key, enabling or disabling access, functioning like a switch for the circuit. Upon entering the correct password, the circuit remains "closed," allowing normal system operation. However, an incorrect password or the detection of a security threat triggers a circuit breaker "trip," temporarily blocking access to prevent unauthorized entry. This paradigm enhances security by safeguarding sensitive information and resources behind a robust password-protected barrier.

The overarching objective of this research is to explore, implement, and validate the effectiveness of an encrypted power supply system utilizing Bluetooth technology. The paper delves into the intricacies of this novel approach, addressing its potential applications in securing electronic devices, sensitive equipment, or areas where controlled access is paramount. By leveraging the synergy of Bluetooth and encrypted access control, this research seeks to redefine the standards of secure power distribution in the contemporary technological landscape.

2. OBJECTIVE

The primary objective of investigating an encrypted power supply is to elevate the security measures within electronic systems to a new level. This innovative circuit breaker introduces a paradigm shift by requiring a password input to either permit or deny electrical flow, thereby augmenting the security of electrical circuits against tampering or unauthorized access. The potential applications of this technology are broad, ranging from securing electronic devices to protecting sensitive equipment and enforcing controlled access in high-security environments.

The essence of this exploration is to delve deeply into and implement a robust security mechanism that harnesses password protection to effectively control and manage access to electrical circuits. By integrating this technology, the overarching goal is to enhance safety measures and thwart unauthorized individuals from tampering with or accessing specific circuits. This initiative aims to establish controlled and ensure the safety of electrical systems in diverse domains.

At its core, the encrypted power supply functions as a guardian, mandating users to provide a correct password to control and regulate access to a system or resource. This strategic approach seeks to fortify security by safeguarding the integrity and confidentiality of the protected circuit, thereby effectively preventing unauthorized access. In doing so, it introduces a dynamic paradigm shift in how electronic systems are safeguarded, acknowledging the growing need for robust security measures in an increasingly interconnected and digital world.

In practical terms, the encrypted power supply serves as a crucial line of defense, providing a sophisticated and proactive solution to the challenges posed by unauthorized access and potential tampering. By prioritizing controlled access through password protection, this technology strengthens the security of electronic systems and enhances their overall dependability and integrity. Through thorough exploration and implementation, the encrypted power supply emerges as a pivotal advancement in ensuring the secure, controlled, and efficient operation of electronic systems across diverse applications and industries.

3. METHODOLOGY

Our methodology ensures a systematic approach towards investigating and implementing an encrypted power supply for enhanced security in electronic systems, specifically focusing on the RoboShop Cart—an intelligent trolley designed for retail applications. We begin by analysing the security requirements unique to the RoboShop Cart and selecting suitable encryption technologies tailored to its needs. The methodology then progresses through the following steps:

Required Components:

Bluetooth Module:
Choose a Bluetooth module supporting Bluetooth Low Energy (BLE) for efficient energy usage. Examples include Nordic Semiconductor's nRF52 or nRF51 series modules.

Microcontroller/Processor:
Utilize a microcontroller or processor capable of managing the RoboShop Cart's operations and handling encryption/decryption tasks. Suitable options include an ESP32, Raspberry Pi, or specialized ones with BLE capabilities.

Power Supply Unit:
Implement a physical power supply unit within the RoboShop Cart, requiring remote control or monitoring capabilities.

Encryption Algorithm:
Employ the Advanced Encryption Standard (AES) as the primary encryption strategy for securing communication between the RoboShop Cart and its controlling device.

3.1 Steps to Implement

Bluetooth Setup:
Interface the selected Bluetooth module with the chosen microcontroller.
Configure the microcontroller to establish a BLE connection for communication.

Security Configuration:
Implement a secure pairing process between the RoboShop Cart and its controlling device, incorporating a robust passkey or secure pairing method supported by Bluetooth.

Encryption Implementation:
Integrate AES encryption algorithm into the microcontroller's firmware to encrypt communication between the RoboShop Cart and its controlling device.

Authentication:
Implement authentication procedures to prevent unauthorized devices from controlling the RoboShop Cart.
Utilize secure authentication protocols to validate the identity of the controlling device.

Key Management:
Establish secure key management practices to safeguard encryption keys, including periodic key updates for enhanced security.

Testing:
Conduct comprehensive testing to ensure secure and reliable communication between the RoboShop Cart and its controlling device, verifying the effectiveness of encryption and authentication mechanisms.

User Interface:
Develop a user-friendly interface, such as a mobile application, enabling seamless interaction and control of the RoboShop Cart by the user.

3.2 Security Considerations:

Ensure that the Bluetooth module, microcontroller, and communication protocols employed are resilient against common security threats.
Implement firmware updates periodically to address any discovered security vulnerabilities.
Take into account functionalities such as secure boot to uphold firmware integrity and safeguard against unauthorized alterations.
Tailor security measures to the specific use case of the RoboShop Cart, consulting with security experts as needed to ensure robust protection against potential threats.

1.3 Flowchart and algorithm:

1. Start
2. Check if there is data from Bluetooth:
   - If yes, read data from Bluetooth.
   - If not, move to the next step.

3. Check the real ultrasonic sensor distance:

- If the distance is greater than 15 cm and less than or equal to 70 cm, move the CMD motor forward.

- If not, proceed to the next step.

4. Check the direction indicated by the data read from Bluetooth:

- If the direction is left, move the CMD motor to the left.

- If the direction is right, move the CMD motor to the right.

5. Scan the RFID for the item:

- If a known card is detected, add the item.

- If not, mark the product as invalid.

6. If the item is added:

- Send the data to the fire bus and print on LCD.

- Update the total by adding the item price.

7. End

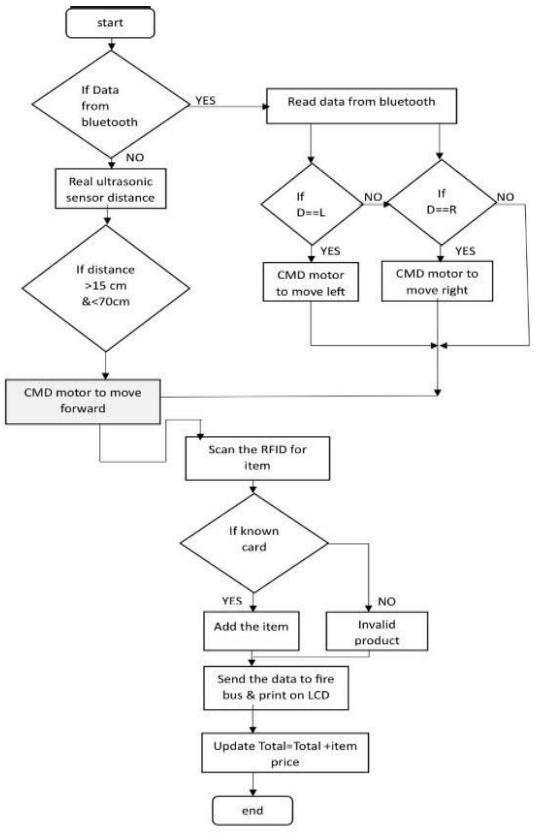


Fig. 1. Flowchart

3.3 Component Description:

1. ESP32 Controller:
A robust microcontroller featuring built-in Wi-Fi and Bluetooth functionalities, ideal for IoT applications and projects necessitating wireless connectivity.

2. NODEMCU Controller:
An open-source IoT platform utilizing the ESP8266 Wi-Fi module, equipped with incorporated USB-to-serial converter for simplified programming.

3.DC Motor:
An electric motor converting electrical energy into mechanical rotation.
Commonly used for propulsion in robotics and automation.

4.Bluetooth Module:
Enables wireless communication over short distances.
Used for connecting devices like smartphones to the robotic system.

5.RFID Scanner:
Reads radio frequency identification (RFID) tags.
Commonly employed for automatic identification and tracking in various applications.

6.RFID Tag:
Holds a distinctive identifier readable by an RFID scanner.
Used for item identification, access control, and tracking.

7.L298N Motor Driver:
Motor driver IC that controls and powers DC motors.
Facilitates motor control and direction in robotics projects.

8.Ultrasonic Sensor:
Uses sound waves to measure distance.
Ideal for detecting obstacles and enabling obstacle avoidance in robotics.

9.16X2 LCD Display with I2C Module:
A liquid crystal displays with 16 characters in 2 rows.
The I2C module simplifies communication and reduces wiring complexity.

3.4 System Architecture:

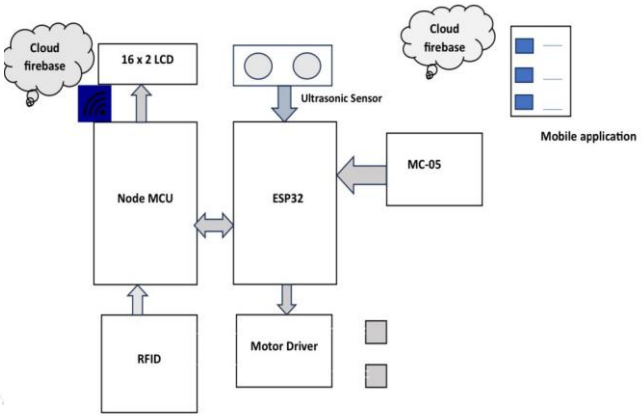


Fig.2. Architecture

The system architecture of the project consists of an ESP32 microcontroller and ultrasonic sensors for user tracking and navigation. It integrates with a Bluetooth app for manual control and offers two billing options: a specialized app for real-time tracking and an RFID reader with an LCD screen for immediate checkout.

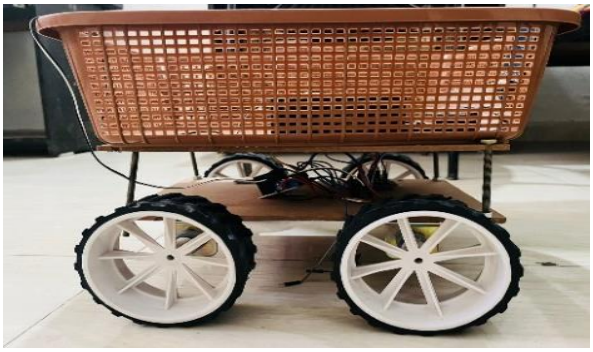
Working:

The smart shopping trolley utilizes an ESP32 microcontroller and ultrasonic sensors to autonomously follow users, maintaining a safe distance. Additionally, a Bluetooth app enables manual control for directional movement. For billing, users have two options: a specialized app for real-time tracking or an RFID reader with an LCD screen for immediate checkout. This integration of smart technology aims to streamline the shopping experience, offering convenience and flexibility to users.

4. RESULTS & DISCUSSION

In this project, we utilized ultrasonic sensors and ESP32 microcontrollers to create a smart shopping cart capable of autonomously following users while maintaining a safe distance. The integration of Bluetooth technology allowed for manual control via a smartphone application, providing users with

flexibility in navigation. Additionally, the inclusion of a dual billing system, consisting of a specialized app for real-time tracking and an RFID reader with an LCD screen for immediate checkout, enhanced the overall shopping experience. Through this integration of advanced technologies, we successfully developed a versatile and user-friendly solution for modern retail environments, aiming to streamline the shopping process and elevate customer satisfaction.



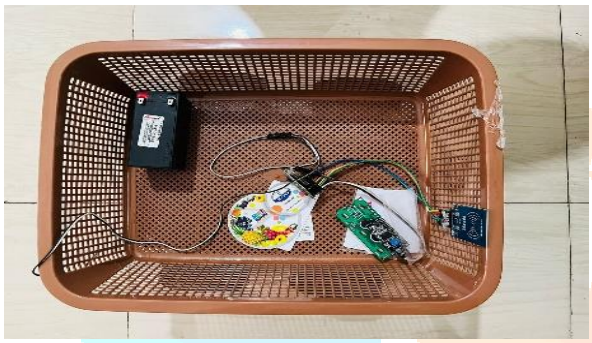


Fig.3.Result

4.1 Key Findings:

1. Enhanced convenience and remote control: Bluetooth allows remote operation of circuit breakers from smartphones or other devices, eliminating the need for physical proximity and keypad interaction.
2. Improved safety for linemen: In electrical substations, Bluetooth control reduces the risk of electric shocks by enabling linemen to function circuit breakers from a secure remove.
3. Potential for enhanced security: Bluetooth authentication can be combined with password protection for added security, although implementation quality is crucial.
4. Cost-effectiveness: Bluetooth modules are relatively inexpensive, making them feasible for integration into circuit breakers.

4.2 Implementation challenges:

1. Security vulnerabilities: Insufficiently secured Bluetooth communication channels may be susceptible to interception and unauthorized access, posing risks of eavesdropping and hacking.
2. Reliability: Unwavering quality Bluetooth associations can be influenced by impedances and extend impediments
3. Compatibility: Ensuring compatibility with different Bluetooth devices and operating systems is essential.

4.3 Discussion Points:

1. Adjust between security and comfort: It is critical to discover the right adjust between security measures and client consolation for commonsense execution.
2. Range and interference considerations: Understanding Bluetooth range limitations and potential interference sources is crucial for reliable operation.
3. Integration with smart home systems: Bluetooth circuit breakers could potentially be integrated into smart home systems for more comprehensive control and automation.

4.4 Additional Considerations:

1. Alternative wireless technologies: Other wireless technologies, such as Wi-Fi or Zigbee, could also be explored for circuit breaker control, each with its own benefits and challenges
2. Multi-factor authentication: Combining password-based authentication with other factors, such as biometrics or physical tokens, could further strengthen security.
3. Regular security audits and updates: Regularly assessing and updating security measures is crucial to address evolving threats.
4. User Training: It is important for effective protection to ensure that the user understands her security risks and best practices.

5. LIMITATION

Here are the limitations of password-based circuit breakers using Bluetooth:
1. Security Concerns:
-Password Strength: Weak passwords can be easily guessed or cracked, compromising the system's security.
-Bluetooth Vulnerability: Bluetooth communication can be susceptible to interception and attacks, potentially allowing unauthorized access.
-Encryption: Lack of encryption can expose sensitive data, such as passwords, transmitted over Bluetooth.

2. Range Limitations:
-Bluetooth Range: Bluetooth typically has a limited range of around 10-20 meters, restricting remote control capabilities.
-Signal Interference: Physical obstructions and interference from other devices can further reduce the effective range

3. Connectivity Issues:
-Pairing Challenges: Initial pairing of devices can sometimes be problematic, causing delays or frustration.
-Connection Loss: Bluetooth connections can drop unexpectedly, requiring manual reconnection.
-Device Compatibility: interoperability issues arise because not all devices are compatible with a particular Bluetooth standard.

4. Power Consumption:
-Battery Drain: Bluetooth communication can drain battery power on mobile devices, affecting their overall usage time.

5. Limited Data Access:
-Real Time Data: Bluetooth-based systems often lack real-time data transmission capabilities, restricting access to circuit breaker status and usage information.

6. FUTURE IMPLEMENTATION

The future implementations of the Encrypted Power Supply utilizing Bluetooth technology offer exciting possibilities for advancing energy management and security. Incorporating

Artificial Intelligence (AI) algorithms could introduce predictive maintenance capabilities, optimizing power distribution and minimizing downtime. Integration with smart grids holds promise for real-time monitoring and adaptive power allocation. The system's scalability opens avenues for expansion into smart homes, enabling users to remotely monitor and control power usage securely through encrypted Bluetooth connections. Collaborative ventures with renewable energy sources may lead to sustainable solutions, facilitating the secure integration of alternative power generation methods. Considering advancements in biometric authentication could improve security and ensure that only authorized people have access to authentication. These prospective developments are poised to transform power distribution networks, making them more resilient, intelligent, and user-centric in response to the dynamic landscape of emerging smart technologies.

7. CONCLUSION

In conclusion, this smart shopping trolley project makes shopping a lot easier and more fun. By using Bluetooth and a special shopping app, shoppers can now guide the trolley themselves or let it follow them around automatically. This means less hassle carrying things and more control over your shopping trip. The project mixes technology like self-moving trolleys and an app that helps you keep track of what you are buying and how much you're spending. Overall, this project is a big step towards making shopping smoother and more enjoyable. It shows how using smart technology can make our everyday tasks, like going to the store, a lot better and more convenient.

Throughout this timeframe, we have encountered a user-friendly environment and engaged in real-time industrial application development. As a result, we acquired skills such as teamwork, time management, and interacting professionally with industry experts.

8. REFERENCES

[1] S Mobeen Shahroz, Muhammad Faheem Mushtaq, Maqsood Ahmad1, Saleem Ullah, Arif Mehmood, And Gyu Sang Choi "IoT-Based Smart Shopping Cart Using Radio Frequency Identification", 2020

[2] T.R. Lekhaa, S. Rajeshwari, J. Aiswarya Sequeira, S. Akshayaa "Intelligent Shopping Cart Using Bolt Esp8266 Based on Internet of Things", 2019.

[3] Mohit Kumar, Jaspreet Singh, Anju, Varun Sanduja. Smart Trolley with Instant Billing to Ease Queues at shopping malls using ARM7 LPC2148. 2018

[4] Vaishali Rane, Krutik Shah, Kaushal Vyas, Sahil Shah, Nishant Upadhyay Smart Trolley Using RFID Jan 2019

[5] Priyanka S. Sahare, Anup Gade, Jayant Rohankar A Review on Automated Billing for Smart Shopping System Using IOT International Information and engineering technology association 20 December 2018

[6] P.T. Sivagurunathan, P. Seema, M. Shalini, R. Sindhu Smart Shopping Trolley Using RFID International Journal of Pure and Applied Mathematics (2018).

[7] Yathisha, L., Abhishek, A., Harshith, R., Darshan Koundinya, S.R., Srinidhi, K.: Automation of shopping cart to ease queue in malls by using RFID (2015).

[8] Tharindu Athauda, Juan Carlos Lugo Marin, Jonathan Lee, Nemai Karmakar Department of Electrical and Computer Systems Engineering Robust Low-Cost Passive UHF RFID Based Smart Shopping Trolley IEEE Journal of Radio Frequency Identification (2018)

[9] Mr. P. Chandrasekar and Ms. T. Sangeetha" Smart Shopping Cart with Automatic Billing System through RFID and ZigBee", IEEE,2014

[10] Gangwal, U., Roy, S., Bapat, J.: Smart shopping cart for automated billing purpose using wireless sensor networks. IEEE (2013).

[11] S.V. Joshi and R. D. Kanphade, "Deep Learning Based Person Authentication Using Hand Radiographs: A Forensic Approach," in IEEE Access, vol. 8, pp. 95424-95434, 2020, doi: 10.1109/ACCESS.2020.2995788.

[12] Joshi, S.V., Kanphade, R.D. (2020). Forensic Approach of Human Identification Using Dual Cross Pattern of Hand Radiographs. In: Abraham, A., Cherukuri, A., Melin, P., Gandhi, N. (eds) Intelligent Systems Design and Applications. ISDA 2018 2018. Advances in Intelligent Systems and Computing, vol 941. Springer, Cham. https://doi.org/10.1007/978-3-030-16660-1_105.

[13] Anuradha D. Thakare, Rohini S Hanchate . Introducing Hybrid model for Data Clustering using K-Harmonic Means and Gravitational Search Algorithms. International Journal of Computer Applications. 88, 17 (February 2014), 17-23. DOI=10.5120/15445-4002

[14] Hanchate, R., & Anandan, R. (2023). Medical Image Encryption Using Hybrid Adaptive Elliptic Curve Cryptography and Logistic Map-based DNA Sequence in IoT Environment. IETE Journal of Research, 1–16. https://doi.org/10.1080/03772063.2023.2268578

[15] Prof. Pritam Ahire,Akanksha Kale,Kajal Pasalkar,Sneha Gujar,Nikita Gadhave, "ECG MONITORING SYSTEM", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.9, Issue 3, pp.407-412, March 2021, Available at :http://www.ijcrt.org/papers/IJCRT2103052.pdf

[16] LSTM based stock price prediction, P Ahire, H Lad, S Parekh, S Kabrawala - International Journal of Creative Research Thoughts, 2021.