IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secured Energy Transfer via Bluetooth Encryption

[1]Dr. Nitin Dhawas,[2]Piyush Sawkar, [3]Rutuja Bankar, [4]Arpita Ghojage

[1]Professor, Department of Electronics and Telecommunication, Nutan Maharashtra Institute & Engineering & Technology, Talegaon Dabhade Pune, India

[2 3 4]Students Department of Electronics and Telecommunication, Nutan Maharashtra Institute & Engineering & Technology, Talegaon Dabhade, Pune, India

Abstract

The Encrypted Power Supply Using Bluetooth system represents an innovative approach to enhancing the security of power supply communication through the utilization of Bluetooth technology. This system seamlessly integrates advanced encryption algorithms with Bluetooth Low Energy (BLE) modules to establish secure and dependable communication channels, serving a broad range of applications including Internet of Things (IoT) devices, industrial control systems, and smart grids. To address the critical security concerns inherent in power supply communication, the solution employs robust encryption mechanisms alongside Bluetooth Low Energy technology. Within the system, the transmitter, seamlessly integrated into the power supply unit, utilizes sophisticated cryptographic algorithms to safeguard power supply data from unauthorized access and tampering. Meanwhile, BLE technology facilitates wireless communication with minimal power consumption, making it a fitting choice for energy-efficient applications and battery-operated devices. A notable feature of the system lies in its adaptability and scalability. Designed to seamlessly integrate with existing infrastructure and accommodate future enhancements, it can be tailored to various use cases and environments, thereby meeting the evolving needs of diverse industries and applications. Moreover, the system incorporates efficient power management mechanisms to optimize energy consumption and extend battery life in battery-operated devices. The Encrypted Power Supply Using Bluetooth system finds versatile applications across multiple industries and domains. In IoT deployments, it offers a secure communication platform for a variety of devices including smart home devices, industrial sensors, and environmental monitoring systems. Within industrial settings, it facilitates secure data transmission across control systems, machinery, and process automation. Furthermore, in smart grid infrastructure, it enables secure communication among utility providers, substations, and smart meters, ensuring the integrity and confidentiality of power consumption data. Encrypted Power Supply Using Bluetooth system presents a robust and efficient solution for enhancing the security of power supply communication. Through the integration of encryption algorithms with Bluetooth technology, the system ensures the confidentiality, integrity, and reliability of data transmission across a wide spectrum of applications.

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 significantly enhance the security measures in electronic systems. This innovative type of circuit breaker introduces a fundamental shift by necessitating a password input to either permit or deny electrical flow, thereby adding electrical current that provides an additional line of defense against tampering or unwanted access. It’s possible uses of this technology are diverse, ranging from securing electronic devices to protecting sensitive equipment and maintaining controlled access in areas where security is paramount.

The essence of this exploration is to delve into and implement a security mechanism that leverages password protection to effectively control and manage access to electrical circuits. By incorporating this technology, the overarching goal is to enhance safety measures and thwart unauthorized individuals from tampering with or accessing specific circuits. This, in turn, ensures the establishment of controlled and secure electrical systems across various domains. At its core, the encrypted power supply functions as a guardian, requiring users to provide a correct password to control and regulate access to a system or resource. This strategic approach aims to bolster security by safeguarding the integrity and confidentiality of the protected circuit, 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, offering a sophisticated and proactive solution to the challenges posed by unauthorized access and potential tampering. By emphasizing controlled access through password protection, this Technology strengthens the security of electronic systems and adds to their general dependability and integrity. Through this 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

Encrypting a power supply using Bluetooth methodology involves securing communication between a power supply unit and a gadget that makes use of Bluetooth technology, such a computer or smartphone. This becomes especially helpful in situations when remote control or remote control or In order to guarantee the privacy and accuracy of the communication, a power supply must be monitored. Here is a complete guide on how to implement such a system:

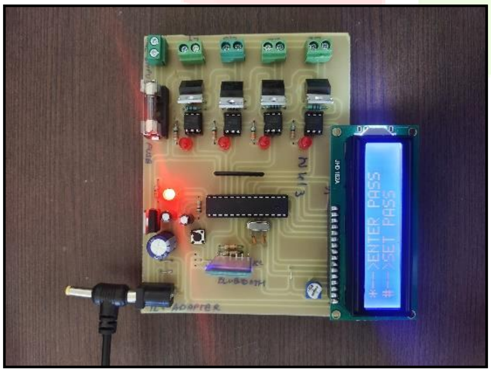

Fig.1. Model

Required Components:

1. Bluetooth Module:

- To achieve energy efficiency, choose a Bluetooth module that supports the Bluetooth Low Energy (BLE) protocol. Nordic Semiconductor's nRF52 or nRF51 series modules are suitable examples.

2. Microcontroller/Processor:

- Utilize a microcontroller or processor to manage the power supply and handle encryption/decryption tasks. Popular choices include microcontrollers from Arduino, Raspberry Pi, or specialized ones with BLE capabilities.

3. Power Supply Unit:

- The physical power supply that requires remote control or monitoring.

4. Encryption Algorithm:

- Is AES the single encryption strategy utilized whereas exchanging keys? How much time ought to AES keys take to ended up completely secure? The Utilize of AES Encryption in Data assurance The Progressed Encryption Standard, or AES, may be a conspicuous encryption innovation for information assurance and capacity.

3.1 Steps to Implement

1. Bluetooth Setup:
- Interface the Bluetooth module to the microcontroller
- Configure the microcontroller to establish a Bluetooth Low Energy (BLE) connection.

2. Security Configuration:
- Implement a secure pairing process between the power supply unit and the controlling device. This may involve using a passkey or other secure pairing methods supported by Bluetooth.

3. Encryption Implementation:
- Integrate the chosen encryption algorithm (e.g., AES) into the microcontroller code.
- Encrypt the communication between the power supply unit and the controlling device using the selected algorithm.

4. Authentication:
- Execute verification procedures to anticipate unauthorized gadgets from controlling the control supply.
- Utilize secure authentication protocols to validate the identity of the controlling device.

5. Key Management:
- Manage encryption keys securely, preventing unauthorized access.
- Consider periodic key updates for enhanced security.

6. Testing:
- Thoroughly test the system to guarantee secure and reliable communication between the power supply unit and the controlling device.

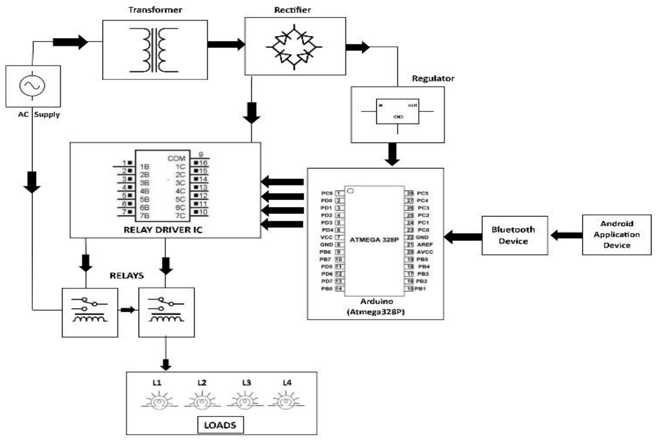

Fig.2 Block Diagram

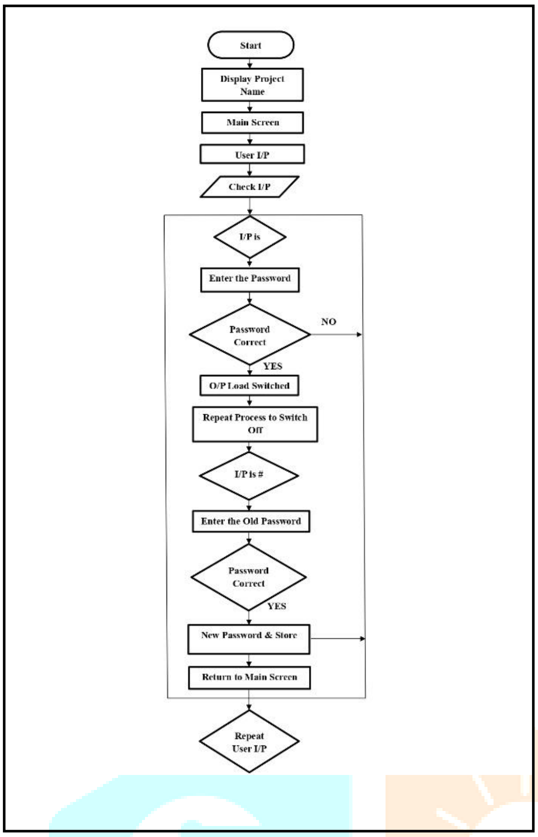

Fig.3 Flow Chart

3.2 Security Considerations:

- Ensure the Bluetooth module, microcontroller, and communication protocols are secure and resilient against common attacks.

- Redesign firmware discontinuously to expect security issues.

- Consider implementing features like secure boot to maintain firmware integrity.

- Creating a secure system requires careful consideration of the specific use case and potential threats. For critical systems, consulting with a security expert or team is advisable to ensure the highest level of security.

4. RESULTS & DISCUSSION

4.1 Key Findings:

- 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.
- 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.
- Potential for enhanced security: Bluetooth authentication can be combined with password protection for added security, although implementation quality is crucial.
- Cost-effectiveness: Bluetooth modules are relatively inexpensive, making them feasible for integration into circuit breakers.

4.2 Implementation challenges:

Security weaknesses, if not adequately safe, Bluetooth communication is prone to hacking. Reliability, Unwavering quality Bluetooth associations can be influenced by impedances and extend impediments Compatibility, ensuring compatibility with different Bluetooth devices and operating systems is essential.

4.3 Discussion Points:

- Adjust between security and comfort: It is critical to discover the right adjust between security measures and client consolation for commonsense execution.
- Range and interference considerations: Understanding Bluetooth range limitations and potential interference sources is crucial for reliable operation.
- 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:

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

5. CONCLUSION

In conclusion, using a power supply that's encrypted and connected via Bluetooth offers a strong way to improve security and control in many situations, especially in devices like smart gadgets and systems for the Internet of Things (IoT). By combining encryption with Bluetooth, this system can protect against unauthorized access, hacking attempts, and tampering.
With Bluetooth, the encrypted power supply can easily and securely communicate with devices it's meant to work with. This allows for remote control and monitoring of the power supply's settings, making things more efficient and convenient for users.
Adding encryption means that any data sent between the power supply and connected devices is scrambled, making it much harder for anyone to snoop or mess with the information. To sum up, an encrypted power supply using Bluetooth doesn't just offer better security—it also provides flexibility, scalability, and easy integration with other systems. As more and more devices become part of the IoT, solutions like this one will become increasingly important for keeping everything running smoothly and securely.

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. REFERENCE

1) [1] Veena, “Electric line man safety system with OTP based circuit breaker”, SR Engineering College, Volume:2, May 2015

2) Deepak Sharma & Major Sing Goraga: “International Journal of Current Engineering And Scientific Research (IJCESR)” Volume2, issue-May 2015

3) E. Brier, C. Clavier and F. Olivier, "Correlation power analysis with a leakage model", Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst., pp. 16-29, 2004.

4) John M.Osepchuk: “IEEE Engineering in Medicine and Biology Volume15(1),Page:116- 120,Issue:June 1996

5) Mohammad Tasdighi: “Inductive FCL's impact on circuit breaker's interruption condition during short-line faults” North American Power Symposium (NAPS), Issue: 22-24 Sept2013

6) Genesh Naik & Srikanth N “Password Based Circuit Breaker”, Dr.Ambedkar Institute of Technology, August 2017.

7) PASSWORD BASED CIRCUIT BREAKER USING 8051 Under the Guidance of Mrs. B. Mounika, Assistant Professor G. Chandana. Sandhya, K. Revanth, Aaqib-Ur-Rahman, January 2021. 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.

8) 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.

9) 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

10) 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

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

12) Issues Related to Power Supply Reliability in Integrated Electronic Security Systems Operated in Buildings and Vast Areas https://doi.org/10.3390/en16083351

13) Analysis of computer network security in substation Jan 2002 Z. Gao Y. Luo G. Tu T. Wu

14) Teaching for Conceptual Change in Security. Awareness January 2009 IEEE Security and Privacy Magazine Rosanna Yuen-Yan Chan Victor K. Wei

15) Secure Internet Access to Gateway Using Secure Socket Layer July 2006 IEEE Transactions on Instrumentation and Measurement D.V. Bhatt S. Schulzeve Gerhard P. Hancke

16) Uninterruptible Power Supply Systems January 2010 Mihail hristov Antchev

17) Uninterruptible Power Supplies Adel Nasiri, Seyed Ahmad Hamidi https://doi.org/10.1016/B978-0-12-811407-0.00021-0

18) He X., Qiu R.C., Ai Q., Chu L., Xu X., Ling Z. Designing for situation awareness of future power grids: An indicator system based on linear eigenvalue statistics of large random matrices. IEEE Access. 2016;4:3557-3568.

19) 2. Suciu G., Sachian M.A., Vulpe A., Vochin M. Farao A., Koutroumpouchos N., Xenakis C. SealedGRID: Secure and Interoperable Platform for Smart GRID Applications. Sensors. 2021;21:54

20) Javaid N., Hafeez G., Iqbal S., Alrajeh N., Alabed M.S., Guizani M. Energy efficient integration of renewable energy sources in the smart grid for demand side management. IEEE Access. 2018:6:77077-77096.

21) Cybersecurity in Power Grids: Challenges and Opportunities Tim Krause,[1] Raphael Ernst,[1] Benedikt Klaer, 2,3 Immanuel Hacker,2,3 and Martin Henze[1],2021