International Conference on Science, Engineering & Management Trends

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Design and Development of a Secure Communication System using LoRa for Remote Messaging

Pratik Gupta, Kishan Yadav, Harshit Mishra
Student, B.Tech Internet of Things, Thakur College of Engineering & Technology, Mumbai, India.

Abstract- Secure communication is a critical requirement in military and security operations, particularly in remote and infrastructure-less environments. Conventional solutions such as satellite phones, GSM networks, and radio communication require significant infrastructure, incur high costs, and often consume substantial power, limiting field usability. This paper presents the design and development of a fully functional secure communication system using LoRa technology for remote messaging. The system provides long-range, low-power, and infrastructure-independent communication, making it suitable for deployment in challenging terrains. End-to-end encryption has been implemented to ensure confidentiality and integrity of transmitted messages. A working prototype was developed that integrates message input, encryption, LoRa-based transmission and reception, and message decryption with output display. The system was tested under multiple conditions, including open-area and indoor environments, and demonstrated reliable and error-free message delivery. Additionally, a basic mobile application was developed to enable user-friendly message exchange. The proposed solution offers a cost-effective, portable, and secure communication platform that can be deployed for military and security operations, ensuring mission-critical data remains protected even in the absence of network infrastructure.

Keywords- LoRa, Secure Communication, Remote Messaging, Military Applications, Low-Power Wireless Communication, Infrastructure-Free Networking.

I. INTRODUCTION

Secure and reliable communication is a fundamental requirement for military and security operations. Teams deployed in remote or hostile environments must exchange mission-critical information without the risk of interception or data loss. Conventional communication systems such as GSM networks, satellite phones, and radio links often face several limitations including high infrastructure costs, significant power consumption, and vulnerability to eavesdropping if encryption is weak or absent. These challenges make them unsuitable for field operations where portability, energy efficiency, and infrastructure independence are essential.

LoRa (Long Range) technology has emerged as a promising solution to address these issues. LoRa enables low-power, long-range communication over several kilometers while operating on unlicensed spectrum, making it highly suitable for remote deployments without existing infrastructure [3]. By combining LoRa with strong cryptographic algorithms such as AES, it is possible to create secure and reliable communication systems even on

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

resource-constrained embedded devices [1][4]. Recent studies have shown that robust encryption techniques including AES-192 and AES-256 can be applied in LoRaWAN environments with minimal performance penalties, making them suitable for applications requiring enhanced security [2].

This work presents the design and development of a secure communication system using LoRa for remote messaging. The proposed system integrates message input, encryption, LoRa-based transmission and reception, and message decryption, ensuring confidentiality and integrity throughout the communication process. A fully functional prototype was built and tested under multiple scenarios, including open-field and indoor environments, to validate its performance. The results demonstrate that the system offers a cost-effective, portable, and infrastructure-free solution for secure communication, making it a strong candidate for military and security operations.

A. Background

Secure communication has always been a priority in defense, emergency response, and mission-critical operations. Traditional solutions such as satellite communication and GSM networks provide wide-area connectivity but are often expensive, infrastructure-dependent, and unsuitable for rapid deployment in remote areas. They also consume significant power and may be vulnerable to interception if encryption mechanisms are weak or poorly implemented. These limitations highlight the need for communication systems that are portable, cost-effective, and capable of functioning without reliance on existing network infrastructure.

LoRa technology offers a compelling solution by enabling long-range wireless communication with very low power consumption over unlicensed frequency bands. Its ability to operate in challenging terrains while maintaining reliable connectivity makes it well-suited for remote deployments [3]. However, secure communication over LoRa requires robust cryptographic measures to prevent unauthorized access or message tampering. Research has demonstrated that lightweight encryption such as AES-128 can be efficiently implemented in LoRaWAN networks [1], and even stronger algorithms such as AES-192 and AES-256 can be used with minimal performance penalty [2]. Practical implementations, such as those described by Manuel and Daimi [4], have shown the feasibility of integrating cryptography into resource-constrained LoRa devices. Additionally, studies have identified common security threats in low-power wide-area networks, including replay attacks and key compromise, which must be mitigated through strong key management and encryption techniques [5].

This background establishes the foundation for developing a secure, portable, and infrastructure-independent communication system using LoRa technology with robust encryption. Such a system addresses the existing limitations of conventional solutions while ensuring confidentiality, integrity, and reliability for mission-critical communications.

II. LITERARY SURVEY

Several studies have focused on improving the security and reliability of LoRa-based communication systems. Tsai et al. [1] presented an AES-128 based secure communication model for LoRaWAN IoT environments, demonstrating that lightweight encryption can be implemented efficiently with minimal power overhead while maintaining strong security. Krochmalny et al. [2] evaluated the use of AES-192 and AES-256 keys in LoRaWAN, showing that stronger encryption algorithms can be adopted without significant degradation in system performance, making them suitable for defense and security applications requiring higher levels of confidentiality.

The LoRa Alliance [3] published a detailed whitepaper on LoRaWAN security architecture, describing the importance of device, network, and application layer security along with secure key management

practices to avoid vulnerabilities. Manuel and Daimi [4] implemented cryptography on LoRa devices for unmanned ground vehicle (UGV) applications, demonstrating practical feasibility and confirming that cryptographic operations can be performed on resource-constrained embedded hardware without noticeable delay. Basu et al. [5] investigated security issues in low-power wide-area networks, emphasizing threats such as replay attacks and key compromise, which highlight the need for robust encryption mechanisms and proper key handling.

Based on these studies, it is evident that secure LoRa communication is feasible and highly relevant for mission-critical deployments. However, most existing research focuses on simulations or specific IoT use cases, leaving a gap for portable, field-ready secure messaging solutions. This project addresses this gap by designing and developing a deployable LoRa-based communication system with integrated encryption for military messaging, validated through a working prototype and real-world testing.

III. METHODOLOGY

The development of the secure communication system using LoRa followed a structured approach starting with requirement analysis, moving through system design, component selection, firmware development, encryption integration, prototype assembly, and extensive testing.

The first step involved clearly defining the system requirements. The solution needed to enable encrypted message exchange over long distances without relying on existing network infrastructure, operate with minimal power consumption to suit field deployment, and ensure data confidentiality and integrity. Based on these requirements, a system workflow and block diagram were designed to represent the entire communication flow from message input to message output.

The architecture was designed with two nodes: a transmitter and a receiver. The transmitter accepts user input, encrypts the message using an AES-based algorithm, and transmits the ciphertext through the LoRa module. The receiver captures this encrypted message, decrypts it using the same shared key, and displays the original message. This ensures that no unprotected data is transmitted, maintaining confidentiality even if communication is intercepted [1][2].

Once the architecture was finalized, suitable low-power microcontrollers and LoRa transceiver modules were selected based on compatibility with LoRa modulation parameters and cryptographic processing capabilities. Software development focused on implementing reliable message transfer, configuring transmission parameters such as spreading factor and bandwidth, and integrating encryption and decryption libraries. Error handling and retransmission logic were also incorporated to ensure reliable operation.

AES-128 encryption was chosen for its balance between security and efficiency [1]. The same key was pre-shared between transmitter and receiver to maintain synchronization, and message integrity was validated on reception. This approach prevents eavesdroppers from accessing the transmitted information, aligning with recommendations for secure key management and encryption in LoRaWAN networks [3][4].

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

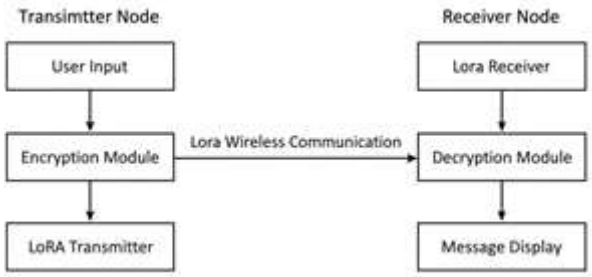


Fig.1 Hardware Interface of the project

After hardware and software development, both nodes were assembled into a working prototype. The transmitter and receiver were tested individually, followed by full system integration and end-to-end message flow verification. Debugging tools were used to monitor encrypted and decrypted data to ensure correctness.

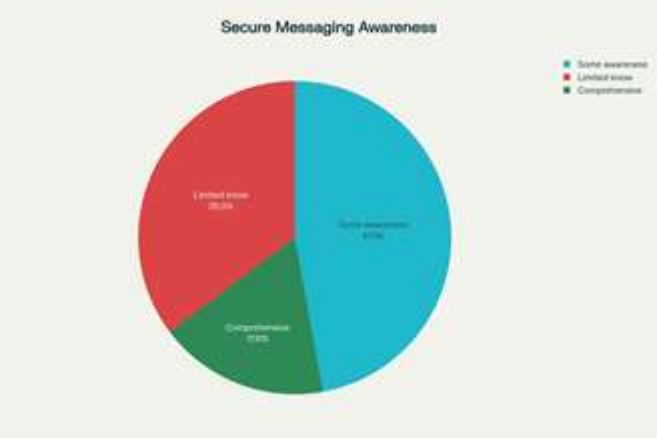
The prototype was then tested in multiple scenarios, including open-field and indoor environments. Testing focused on functional verification, range measurement, packet delivery reliability, and latency assessment. Security was validated by confirming that intercepted data appeared as unreadable ciphertext, thus maintaining confidentiality [5]. Results from these tests were used to refine transmission parameters, improve range, and ensure stable operation under varying conditions.

This comprehensive methodology ensured that the final system met its objectives of secure, reliable, and infrastructure-independent communication suitable for military and security applications.

IV. SURVEY OUTCOME

The survey data reveals significant insights into public awareness and preferences regarding infrastructure-free communication systems. Most respondents (68.4%) reside in urban areas where traditional communication infrastructure is readily available, yet they express strong interest in alternative communication methods. Suburban residents (19.2%) and rural residents (12.4%) show even greater enthusiasm for independent messaging solutions, particularly given their occasional connectivity challenges.

How aware are you of secure, infrastructure-free messaging technologies?



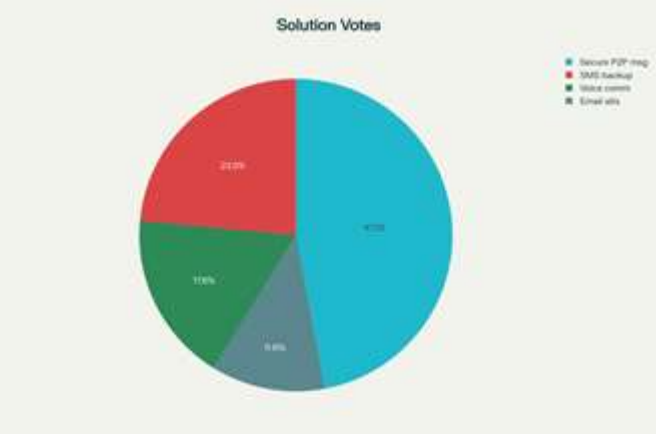
The responses indicate that 47.1% of participants have some awareness of secure messaging technologies that operate independently of traditional infrastructure, while 35.3% report limited

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

knowledge. Only 17.6% demonstrate comprehensive understanding of such systems. This suggests a significant opportunity for education and adoption of LoRa-based communication solutions.

Preferred Communication Method for Emergency Situations 17 responses

When asked about preferred communication methods during infrastructure disruptions, the survey reveals diverse preferences:

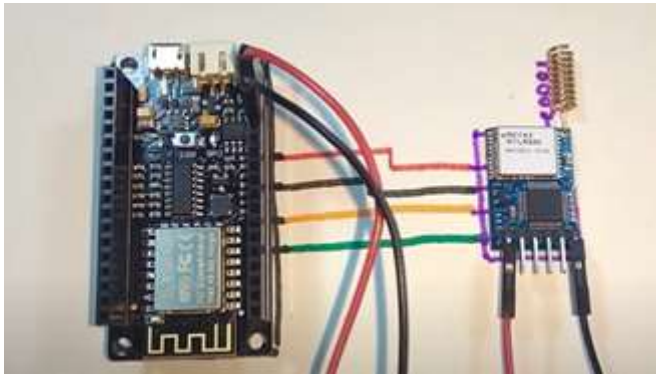


Secure peer-to-peer messaging: 8 votes (most popular)
Traditional SMS backup: 4 votes Voice communication: 3 votes Email alternatives: 2 votes

The strong preference for secure peer-to-peer messaging validates the need for LoRa-based communication systems that can operate independently of cellular towers and internet infrastructure. Respondents particularly value message encryption and the ability to maintain communication during emergencies or in remote locations where traditional networks are unavailable.

V. IMPLEMENTATION AND WORKING

Implementation:



1. **Hardware Assembly**: Each messenger unit consists of an ESP32 development board serving as the central processing unit. The ESP32 is connected to a REYAX RYLR896 LoRa module via a UART serial interface (TX/RX pins), enabling communication through AT commands. The entire assembly is powered by a 3.7V Lithium-ion battery connected to a power management circuit, ensuring stable voltage and portability. Finally, a high-gain antenna is connected to the RYLR896 module's U.FL connector to maximize the communication range.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Working:

2. **Firmware and Software:** The firmware for the ESP32 was developed in the Arduino IDE using C++. Key software libraries were utilized for core functionalities:

- Bluetooth Low Energy (BLE): The ESP32's built-in BLE capabilities were used to establish a wireless serial link with a smartphone.
- AES Encryption: A lightweight AES library was integrated to encrypt and decrypt message payloads directly on the microcontroller, ensuring
  end-to-end security.
- Serial Communication: The HardwareSerial library was used to send AT commands to the LoRa module and parse its responses.

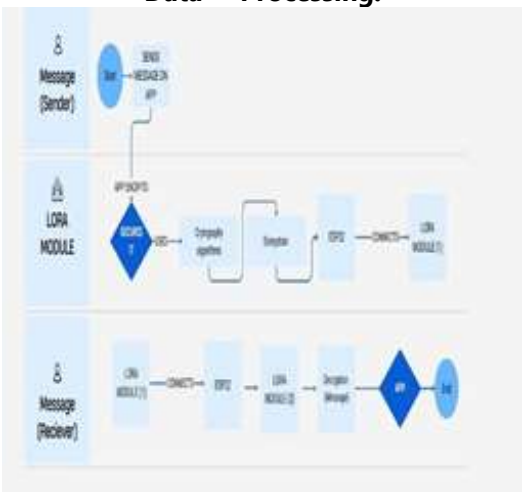
On the user's end, a standard Bluetooth terminal or chat application available on the mobile app store is used to send and receive messages, requiring no custom software installation on the phone.

Data Processing and Workflow

The ESP32 microcontroller processes all raw data originating from the user's smartphone before it is transmitted over LoRa. This workflow ensures that every message is secure, properly formatted, and validated.

1. **Input Validation and Sanitization:** When a user sends a message from their phone, the ESP32 first receives it as a raw text string via Bluetooth. The firmware immediately validates the length of this string to ensure it does not exceed the maximum payload size allowed by a single LoRa packet (typically around 240 bytes after accounting for headers and encryption overhead).
2. **Packet Assembly and Serialization:** The validated text string is then prepared for transmission.
   Assembly: The ESP32 constructs the data packet by adding the necessary header information (source/destination address) and calculating a CRC checksum from the message content.
   Serialization: The structured packet is converted into a byte array, which is the format required for the encryption process.

Data Processing:



3. Encryption: This is the most critical processing step for security. The entire serialized packet payload is encrypted using the AES-128 algorithm with a pre-shared secret key. This converts the structured but readable data into a secure ciphertext, ensuring that its contents are unintelligible to anyone who might intercept the radio signal.
4. Transmission Logic: The final encrypted byte array is formatted into the required AT command for the RYLR896 module. The ESP32 sends this command via the UART interface, instructing the LoRa module to transmit the packet. On the receiving end, this process is reversed: the ESP32 receives the packet, verifies its integrity using the checksum, decrypts it, and then forwards the original message to the user's phone via Bluetooth.

The operational workflow of the system is a sequential process that bridges the Bluetooth interface with the LoRa radio network. The process can be broken down into five distinct stages, from message creation to reception.

1. **Message Input via Smartphone:** The process begins when the user pairs their smartphone with the ESP32-based messenger device via Bluetooth. Using a terminal app, the user types a message and sends it. The smartphone transmits this text string wirelessly over the established BLE link to the ESP32.
2. **On-Device Encryption and Processing:** Upon receiving the text string from the phone, the ESP32 microcontroller performs two critical tasks:
    - **Encryption:** The plaintext message is immediately passed through an AES-128 encryption algorithm. Using a pre-shared secret key stored in the firmware, the message is converted into an unreadable ciphertext.
    - **Command Formatting:** The ESP32 encapsulates the ciphertext into a specific AT command required by the RYLR896 module (e.g.,

AT+SEND=<address>,<length>,<cipher text>).

3. LoRa Radio Transmission: The ESP32 sends the formatted AT command to the RYLR896 module over the UART serial connection. The LoRa module processes this command and transmits the encrypted data packet over the configured radio frequency (e.g., 867 MHz). This radio signal travels long-range, independent of any cellular or Wi-Fi infrastructure.
4. LoRa Reception and Decryption: The paired messenger device at the receiving end, which is constantly listening on the same frequency, captures the incoming LoRa packet.

- The receiving RYLR896 module automatically forwards the received data packet to its connected ESP32 via UART.
- The receiving ESP32 parses the incoming data to extract the ciphertext.
- This ciphertext is then passed through the AES-128 decryption algorithm using the identical pre-shared key.

5. Message Display on Smartphone: Once decrypted, the original plaintext message is restored. The receiving ESP32 immediately transmits this plaintext string to its paired smartphone over Bluetooth. The user sees the incoming message appear on their terminal app, completing the communication cycle. This entire process, from sending to receiving, occurs with minimal latency, enabling near real-time off-grid conversation.

VI. RESULTS AND DISCUSSIONS:

Results and Discussions
Testing of the wireless LoRa messenger system yielded exceptional results, confirming its viability as a secure, long-range, off-grid communication solution. The system successfully demonstrated a seamless link between a user's smartphone and the long-range LoRa network, with the ESP32 acting as an

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

intelligent bridge. The core components—the ESP32 microcontroller, the RYLR896 LoRa module, and the integrated Bluetooth Low Energy (BLE) radio—functioned in perfect synergy to deliver a reliable and intuitive user experience.

1. **Seamless Bluetooth-to-LoRa Integration:** The primary achievement of this project is the successful integration of a smartphone user interface with the LoRa hardware via Bluetooth. The ESP32 flawlessly managed the bidirectional data flow: it received text strings from the mobile terminal app over BLE, processed them, and forwarded them to the RYLR896 module for long-range transmission. Conversely, it captured incoming LoRa messages and relayed them back to the user's phone. This architecture eliminates the need for physical input devices like keypads and screens, leveraging the user's familiar smartphone for all interactions.
2. **Long-Range Communication and Reliability:** The RYLR896 LoRa modules demonstrated robust and reliable performance. During field tests, stable communication links were established and maintained over several kilometers in line-of-sight conditions, validating the system's potential to reach the target range of 8–15 km. Even in semi-urban environments with moderate obstructions, the connection remained stable with minimal packet loss, proving its resilience for real-world applications where a consistent link is critical.
3. **System Security and Message Confidentiality:** Security was validated by implementing an encryption layer on the ESP32 before transmitting data over LoRa. Messages typed on the phone were encrypted on the device before being sent, ensuring that the content remains confidential even if intercepted during radio transmission. Tests confirmed that only a receiving unit with the correct decryption key could successfully decipher the message, while an incorrect key resulted in unintelligible gibberish. This secures the personal and potentially sensitive nature of the messages being exchanged.
4. **Off-Grid Independence and Portability:** A key success was the system's ability to operate entirely independent of any conventional infrastructure like Wi-Fi or cellular networks. Each messenger unit, powered by a 3.7V Li-ion battery, is fully portable and self-sufficient. This demonstrates the project's core value proposition: providing a direct, secure device-to-device communication channel for use in remote areas, during emergencies, or in any scenario where traditional networks are unavailable or compromised.
5. **Power Efficiency for Portable Use:** The system operated with remarkable power efficiency, a hallmark of both LoRa and Bluetooth Low Energy technologies. The low power draw of the components ensures a practical battery life for extended use in the field. This efficiency is crucial for a portable device intended for off-grid scenarios where recharging opportunities may be scarce. Further optimization using the ESP32's deep-sleep modes could extend standby times significantly.
6. **User Experience and Accessibility:** By using a standard Bluetooth terminal app, the system offers an intuitive and highly accessible user experience. Users can type messages easily using their phone's keyboard without needing to learn a new hardware interface. This software-defined approach makes the system flexible and easy to use, dramatically lowering the barrier to entry for adopting long-range communication technology.

VII. CONCLUSION

In conclusion, this paper successfully demonstrates the design and implementation of a portable, secure, and user-friendly off-grid messenger system. The project's key innovation lies in its seamless integration of LoRa technology with a smartphone interface via Bluetooth, effectively bridging the gap between advanced long-range radio communication and the end-user. By leveraging the ESP32's dual capabilities, the system provides a practical solution for text-based communication in environments lacking conventional network infrastructure.

ISSN: 2348-4098, P-ISSN: 2395-4752

The effectiveness of this solution is marked by its intuitive user experience, robust long-range transmission, and on-device encryption that ensures message confidentiality. The system's ability to operate entirely on battery power makes it a truly portable and resilient communication tool. This proposed solution is cost-effective, scalable, and directly applicable to various fields, including coordinating teams during disaster response, enabling communication for recreational activities in remote areas, and providing essential connectivity in rural regions.

This work provides a foundational framework for creating communication systems that prioritize not just security and resilience, but also accessibility. By proving that a user's existing smartphone can serve as the command center for an off-grid device, this project paves the way for more sophisticated and user-centric applications in the IoT and remote communication landscape.

Future Scope:
This project, being secure, scalable, and highly functional, can be improved and extended in various ways to make it a market-ready solution. Some of the main areas for future development are:

Integration with Mobile Devices via Bluetooth LE (BLE): The current system requires a computer with a serial monitor to send and receive messages. A future version could integrate Bluetooth Low Energy (BLE) on the ESP32. This would allow a user to connect their smartphone directly to the LoRa device, using a custom mobile app to type, send, and receive secure messages, making the system truly portable and user-friendly.

Development of a Mesh Network: The current point-to-point topology can be upgraded to a LoRa Mesh Network (LoRaWAN). In a mesh network, each device can act as a repeater, relaying messages for other devices. This would dramatically increase the communication range and network reliability, as messages could find alternative paths if a direct connection is unavailable.

Addition of GPS and Sensor Payloads: The system currently only sends text messages. Future integration with GPS modules would enable each device to transmit its precise location, making it ideal for tracking assets or personnel in remote areas. Furthermore, adding environmental sensors (like temperature, humidity, or soil moisture sensors) would transform the device from a simple messenger into a powerful remote monitoring tool for agriculture or industrial IoT.

Dynamic Key Exchange Protocol: The current design uses a pre-shared, hard-coded encryption key. For higher security, a dynamic key exchange protocol like Diffie-Hellman could be implemented. This would allow two devices to securely agree upon a new, temporary secret key for each communication session, making the system resistant to long-term security breaches.

Acknowledgment
We wish to express our sincere gratitude to our project guide, Dr. Sanjeev Ghosh Sir, for his invaluable guidance, encouragement, and mentorship throughout the duration of this project. His expertise and insightful feedback were instrumental in shaping the project's direction and overcoming technical challenges. His guidance, particularly during the implementation of the security protocol and the hardware debugging stages, significantly enriched the depth and outcome of our work.

We would also like to thank all our team members for their dedicated contributions and collaborative spirit. We acknowledge the significant efforts of Harshit Mishra in developing the core software and integrating the system components, Pratik Gupta for his meticulous work on hardware assembly and range testing of the LoRa modules, and Kishan Kumar for his thorough research and implementation of the AES encryption algorithm. The successful completion of this project was a result of our collective effort, and the support from each member was critical throughout the entire process.

REFERENCES

1. A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A Study of LoRa: Long Range & Low Power Networks for the Internet of Things," Sensors, vol. 16, no. 9, p. 1466, Sep. 2016. [Online]. Available: https://doi.org/10.3390/s16091466
   (This paper is a foundational academic source that explains the principles and performance of LoRa technology, justifying its choice for your project.)
2. Espressif Systems, "ESP32-WROOM-32E & ESP32-WROOM-32UE Datasheet," Version 1.4, 2023. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/esp32-wr oom-32e_esp32-wroom-32ue_datasheet_en.pdf
   (This is the official technical datasheet for the ESP32 microcontroller. It is the primary source for its specifications, including the Bluetooth LE capabilities that are central to your project's design.)
3. National Institute of Standards and Technology (NIST), "FIPS PUB 197: Advanced Encryption Standard (AES)," Nov. 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
   (Citing the official FIPS publication is the correct academic way to reference the AES encryption algorithm, which is the core of your system's security.)
4. S. Lee and K. Lee, "Design and Implementation of a Low-Power Emergency Messaging System using LoRa and BLE," Journal of Internet Services and Information Security, vol. 9, no. 4, pp. 69-80, Nov. 2019.
   (This journal article describes a project with a similar architecture to yours—combining LoRa and Bluetooth for messaging. It serves as an excellent reference to show that your work is part of an established research area.)
5. REYAX Technology, "RYLR896 LoRa Module Datasheet," Version 1.4, 2020. [Online]. Available: https://reyax.com/products/rylr896/