International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Design and Implimentation of an End-To-End Encrypted Communication

[1]Y Akash,[2]M Subharatna raju,[3]D.Sharmila

[1] Student,[2] Student [3]Faculty
[1]Department of E&IT, ANU
[2]Department of E&IT, ANU
[3]Department of E&IT, ANU

https://doi.org/10.55041/ijsmt.v2i4.606

Cite this Article: Akash, Y. & raju, M. S. (2026). Design and Implimentation of an End-To-End Encrypted Communication. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.606

Abstract: The proliferation of embedded systems and the development of IoT (Internet of Things) technology have led to the increased need for safe and timely communication between these technologies. In this regard, this project named "Design and Implementation of End-to-End Encrypted Communication Using ESP32" has come up with a highly efficient security communication system which has been developed with the help of two microcontrollers ESP32 used for the role of a Transmitter (Agent A) and a Receiver (Agent B). This communication network uses the mechanism of E2EE (End-to-End Encryption) with the help of cryptographic techniques like AES (Advanced Encryption Standard) for fast symmetric encryption and RSA for exchanging secret keys.
The input in the proposed system is acquired from sources like keypad, mobile application, or serial monitor. Following data acquisition, the input goes through data preprocessing where the data is preprocessed before it reaches the encryption process.
***IndexTerms*– E2EE, ESP32, end-to-end encrypted**

---

1. INTRODUCTION

The proliferation of Internet of Things (IoT) systems has led to an exponential increase in interconnected embedded devices, necessitating robust security mechanisms for reliable data exchange. The ESP32 microcontroller, featuring integrated Wi-Fi and Bluetooth connectivity along with a dual-core architecture, has become a prominent platform for developing distributed and real-time IoT applications. Despite its capabilities, secure communication between ESP32 nodes remains a significant challenge due to constrained computational resources, limited memory, and exposure to adversarial network environments.
Traditional network-layer security protocols, such as Transport Layer Security (TLS), provide channel-based protection but do not inherently guarantee true end-to-end confidentiality in scenarios involving intermediate brokers or gateways. End-to-end encryption (E2EE) addresses this limitation by ensuring that plaintext data is only accessible at the communicating endpoints, thereby mitigating risks such as man-in-the-middle (MITM) attacks, packet sniffing, and unauthorized data manipulation.

2. Experimental

Recent advancements in IoT security emphasize efficient cryptographic techniques for resource-constrained devices like ESP32. Traditional protocols such as TLS/SSL provide strong encryption but are often unsuitable for embedded systems due to high computational overhead, memory usage, and latency. In common IoT setups using Wi-Fi and MQTT, TLS secures communication channels but does not ensure true end-to-end encryption (E2EE), as intermediaries like brokers or cloud servers can access decrypted data.

ESP-NOW, a lightweight peer-to-peer communication protocol developed for ESP32, eliminates the need for internet connectivity and offers low-latency transmission. However, its built-in encryption has limitations in scalability, key management, and authentication. To address these challenges, this project integrates AES (symmetric encryption) and RSA (asymmetric encryption) to enhance security and achieve E2EE at the application layer.

The proposed system, titled "Design and Implementation of End-to-End Encryption Communication Using ESP32," establishes secure communication between two ESP32 modules: Agent A (Transmitter) and Agent B (Receiver). The system uses ESP-NOW for direct wireless communication, ensuring independence from internet-based vulnerabilities.

The methodology includes requirement analysis, system design, and implementation. The system is structured into three stages: sensing, processing, and output. In the sensing stage, Agent A collects input data from a user interface or sensors. During processing, the data is encrypted using AES and RSA before transmission. In the output stage, Agent B decrypts the received data and presents it to the user.

The data flow involves key generation, key exchange, session key creation, encryption, transmission, and decryption. This ensures confidentiality and secure communication. The system design incorporates hardware components like ESP32 boards and optional sensors, along with a web-based interface developed using HTML, CSS, and JavaScript.

Overall, the project provides a secure, efficient, and low-latency communication model suitable for modern IoT applications.

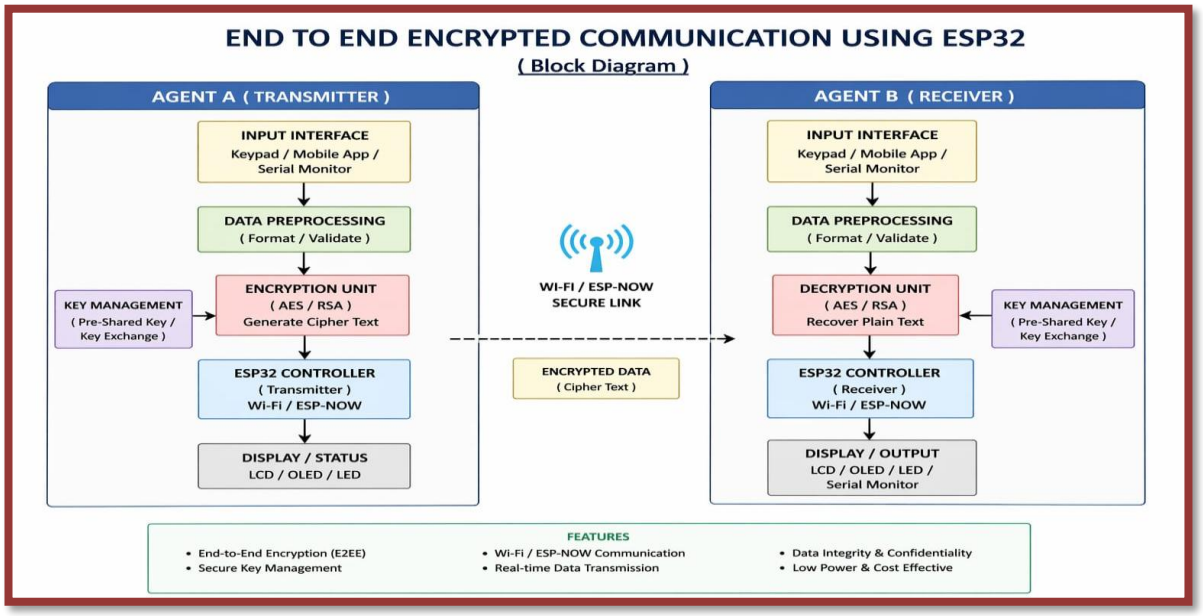

Fig.4.1. Block Diagram

3. Result

- ✓ **Secure End-to-End Communication Achieved**
- ✓ **Successful Encryption and Decryption of Messages**
- ✓ **Reliable Real-Time Data Transmission**
- ✓ **Low-Latency Communication romance**
- ✓ **Effective User Authentication and Access Control**HMI are used for visualization and indicates the water level.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

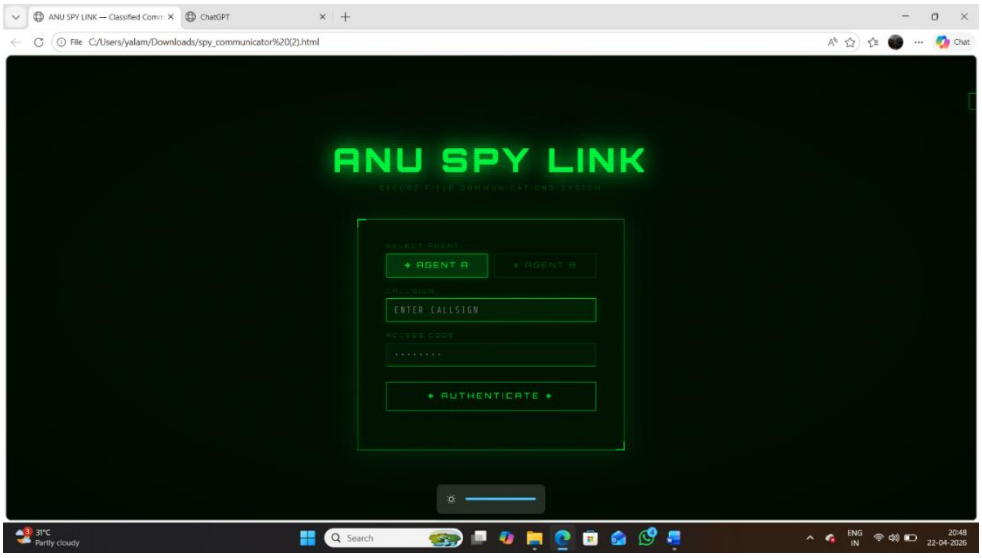

Fig: ANU SPY LIN PAGE

ANU SPY LINK – Secure Field Communication System is an example of a reliable and highly sophisticated secure embedded wireless communication system, which aims to facilitate real-time, end-to-end encryption (E2EE) of data transferred between multiple dispersed nodes via the fast ESP32 dual-core processor and ESP-NOW/Wi-Fi communication technology. The proposed system uses a hierarchical security model that involves the use of AES symmetric encryption algorithm for fast secure transfer of data and RSA asymmetric encryption algorithm for secure key exchange and verification of transmitted information. The process of communication consists of intelligent processing of the data stream, packet generation, data packet validation, and cipher creation on the transmitter side.

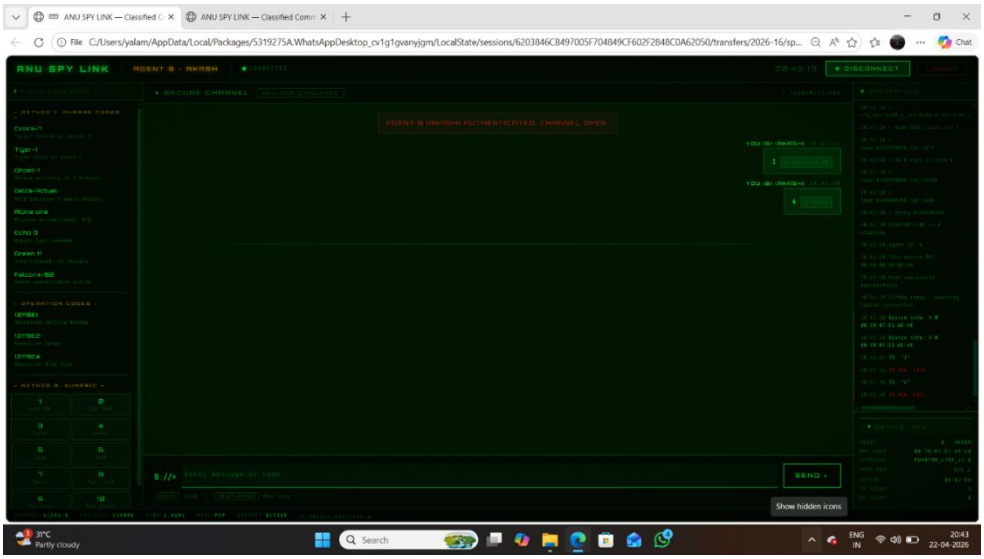

Fig: OUTPUT

The future scope for ANU SPY LINK – Secure Field Communication System would be to evolve the system into an intelligent tactical communication system by making use of emerging technologies like Artificial Intelligence (AI), Machine Learning (ML), and security through blockchain technology. Threats and intrusions can be detected using AI-based systems, which would detect any anomalies in the communication network.

ACKNOWLEDGMENT

The author is highly obliged to Dr. D. Sharmila, Faculty, Dept. of Electronics & Instrumentation Technology, Acharya Nagarjuna University for her valued guidance and insightful discussions throughout the course of his project study.

REFERENCES

1. Espressif Systems, ESP32 Technical Reference Manual, 4th Edition, 2023.
(Extensive manual detailing the architecture of ESP32, GPIO pin programming, Wi-Fi/Bluetooth modules, and interfacing of peripheral devices.)
2. Arduino, Arduino Programming Reference Manual and Language Guide, 2024.
(The official programming guidebook on embedded C/C++ programming language and concepts in microcontroller programming.)
3 **Dabola, S., Tomer, V., Singh, N., Madan, P., & Jhinkwan, A. (2024).** Chat secure-messaging application based on secure encryption algorithm. *International Journal of Research in Advent Technology (IJRASET), 12*(III), 1–10. DOI: 10.22214/ijraset.2024.58817
4 **Goel, A., Baliyan, H., Tyagi, S., & Bansal, N. (2024).** End to end encryption of chat using advanced encryption standard-256. *International Journal of Science and Research Archive, 12*(1), 2018–2025. DOI: 10.30574/ijsra.2024.12.1.0923
5 **Julianto, A. I., Rimbawa, H. A. D., & Asnar, Y. D. W. (2023).** Study and analysis of end-to-end encryption message security using Diffie-Hellman key exchange encryption. *International Journal of Progressive Sciences and Technologies (IJPSAT), 42*(1), 173–183.
6 **Saharan, M., Kumar, N., Kumar, V., & Juneja, A. (2024).** Secure end-to-end chat application: A comprehensive guide. *Review of Computer Engineering Studies, 11*(3), 1–8. DOI: 10.18280/rces.110302 [1, 2, 3]
7 **Wang, J., et al. (2025).** Design and optimization of hybrid end-to-end encryption for modern web applications. *Journal of Web Engineering, 24*(2), 1–20.