

Lightweight Cryptography-Driven Wireless Data Exchange for Aircraft System Using MATLAB

1 Ms. B. Sowmya, 2 N. Gayathri, 3 A.Vasavi, 4 K.Anushka

1 Assistant Professor, Department Of ECE, Vignan's Institute of Management and Technology for Women, Ghatkesar, Telangana.

2,3,4B.Tech Students, Department Of ECE, Vignan's Institute of Management and Technology for Women, Ghatkesar, Telangana.

ABSTRACT

This project designs a secure wireless intra-aircraft communication system using MATLAB and lightweight cryptography. It protects critical sensor data like altitude, temperature, and fuel level during transmission. The data is converted into a 64-bit block and encrypted using the PRESENT algorithm, suitable for low-resource environments. Lightweight cryptography ensures low power usage, minimal memory, and fast processing. The encrypted data is transmitted securely and decrypted at the receiver for accuracy. The system enhances data security and efficiency in avionics and embedded applications.

Keywords: Lightweight Cryptography, PRESENT Algorithm, Wireless Communication, Intra-Aircraft System, Data Security, MATLAB Implementation, Sensor Data Encryption, Embedded Systems, Avionics.

I. INTRODUCTION

Modern aircraft systems require continuous and reliable communication between onboard sensors and control units to ensure safe and efficient flight operations. Important parameters such as altitude, temperature, and fuel level must be transmitted accurately in real time. Traditional wired communication systems, although reliable, increase the overall weight, complexity, and maintenance cost of the aircraft. To overcome these limitations, modern avionics systems are shifting toward wireless communication, which offers greater flexibility, reduced weight, and easier system upgrades.

However, the use of wireless communication introduces several security challenges, including data interception, unauthorised access, and cyber threats. Since aircraft systems are safety-critical, protecting transmitted data is essential. Conventional encryption algorithms like AES provide strong security but are not suitable for resource-constrained environments

due to high power consumption, larger memory requirements, and increased computational complexity. This creates the need for lightweight cryptography, which is specifically designed to provide adequate security while minimising resource usage.

In this project, the PRESENT algorithm, a lightweight block cypher, is implemented using MATLAB to secure wireless communication within aircraft systems. Sensor data, such as altitude, temperature, and fuel level, is converted into a 64-bit data block and encrypted before transmission. At the receiver end, the data is decrypted to retrieve the original information accurately. The proposed system ensures secure, efficient, and reliable communication, making it suitable for avionics, embedded systems, and IoT applications.

II. LITERATURE SURVEY

The literature survey focuses on understanding the existing research and developments in secure wireless communication systems for avionics and embedded applications. With the increasing adoption of wireless technologies in aircraft systems, several studies have highlighted the importance of ensuring data security while maintaining system efficiency. Researchers have explored various communication methods and security mechanisms to protect critical sensor data from potential threats such as interception, tampering, and unauthorised access

1. Arun Kumar, Peter Reji, Devaraj Sheshu E., Shobha K.R., S. Karthik, and Samyuktha Sena I (2020):

The study proposes a wireless intra-aircraft communication system using Wi-Fi (IEEE 802.11n) to replace complex wired networks. It uses Raspberry Pi-3, Node MCU, and IoT sensors for real-time monitoring of parameters like temperature and pressure. Security is ensured using AES-128 encryption, and MATLAB is used to analyse performance such as latency and throughput.

Contribution: Provides a lightweight, scalable, and secure wireless communication system for aircraft.

Limitation: Affected by interference, reliability issues, and requires strict validation for safe implementation.

Contribution: It significantly reduced the waiting time for ambulances at intersections.

Limitation: The system relied on GSM networks, which can be unreliable in low-signal areas, and lacked long-range data communication support.[1]

2. W. H. Zheng, J. T. Armstrong, and M. D. Richards (2010):

The study proposes a flexible wireless spacecraft communication system using WSN and RF that reduces wiring, but faces challenges like interference, signal loss, and radiation affecting reliability.

Contribution: Provides a flexible and modular wireless communication approach for spacecraft systems.

Limitation: Affected by harsh conditions, causing reliability issues, signal attenuation, and radiation effects.[2]

3. Raja Naeem Akram, Konstantinos Markantonakis, Sharadha Kanyawasam, and Shahid Ayub (2015):

The study focuses on securing avionics wireless networks using cryptography and authentication while addressing threats, but highlights added complexity and vulnerabilities.

Contribution: Emphasises the importance of strong security mechanisms in avionics wireless communication.

Limitation: Complex security implementations may increase system cost and processing overhead[3]

4. Kyle McHugh Jr., Walter Alkpedeye, and Thaier Hayajneh (2017):

The study explores next-generation WLAN using IEEE 802.11 and MIMO for high-speed, reliable aviation communication supporting real-time applications

Contribution: enhances communication with advanced WLAN and MIMO.

Limitation: affected by congestion, interference, and scalability issues.[4]

5. C. W. Zhao, J. Jegatheesan, and S. C. Loon (2015):

The study investigates IoT applications using Raspberry Pi for low-cost smart monitoring systems with sensors and wireless modules, enabling real-time data and automation.

Contribution: provides a scalable, cost-effective IoT-based monitoring approach.

Limitation: limited processing capability and potential security issues in critical systems.[5]

6. U. Schwark and ICAO ACP Members (2013):

The study analyses RF compatibility and EMI/EMC in wireless avionics to prevent interference with onboard systems and ensure safe operation.

Contribution: provides guidelines and standards for safe wireless integration in aircraft.

Limitation: requires extensive testing, certification, and strict regulatory compliance.[6]

Author	Title of the paper	Design approach	Application	Key findings
Zheng et al.(2010)	Wireless Intra-Spacecraft Communication System	WSN+RF communication, embedded system	Spacecraft module communication	Flexible modular design reduces wiring affected by radiation.
Rajanaeem Akram et al.(2015)	Security and Trust in Avionics Wireless Network	Cryptography, authentication, trust management	Secure avionics communication	Strong security needed ; increases complexity
Zhao et al. (2015)	IoT Applications using Raspberry Pi	Raspberry Pi+ sensors+ wireless modules	Monitoring, automation, and avionics systems	Cost-effective and scalable: limited processing and

				security
Kyle McHugh Jr. et al.(2017)	Next generation WLAN for avionics	IEEE 802.11n, MIMO technology, encryption	High-speed aviation data systems	High data rate and reliability; affected by congestion
U. Schwark et al.(2013)	Compatibility of wireless avionics systems	RF analysis, standards	Safe wireless deployment in avionics	Requires strict testing and certification
Arun Kumar et al.(2020)	Wireless Intra-Aircraft Communication System	Wi-Fi(IEEE 802.11n), Raspberry pi, Node MCU, AES	Intra-Aircraft communication & monitoring	Reduce wiring weight , improve scalability, reliability issues

Table 1: Literature Survey

III. PROPOSED METHOD

The proposed system focuses on enabling secure communication between two avionics subsystems using a lightweight cryptographic approach. Initially, data is generated from System A (sender), such as sensor readings or control signals, and is converted into a suitable digital format. This data is then encrypted using the PRESENT algorithm along with a shared secret key. The use of a lightweight cipher ensures minimal computational complexity, making it ideal for avionics environments where power, memory, and processing resources are limited.

Once encrypted, the data (ciphertext) is transmitted through a wireless communication channel within the aircraft. This eliminates the need for complex wiring, thereby reducing system weight and maintenance costs. The wireless transmission is secured because the data is already encrypted, preventing unauthorised access or tampering during transmission. The system ensures that even if the data is intercepted, it cannot be understood without the secret key.

At the receiving end, System B decrypts the received ciphertext using the same PRESENT algorithm and shared key to recover the original data. This decrypted data is then processed and used by the avionics system for monitoring or control purposes. The entire process ensures confidentiality, integrity, and efficiency in intra-aircraft communication, making it a reliable solution for modern wireless avionics systems.

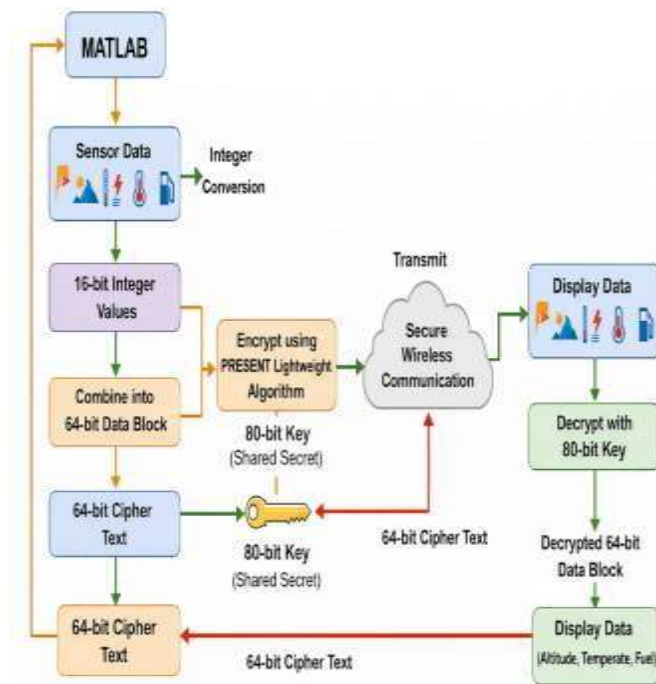


Fig:2 Block Diagram

FLOWCHART:

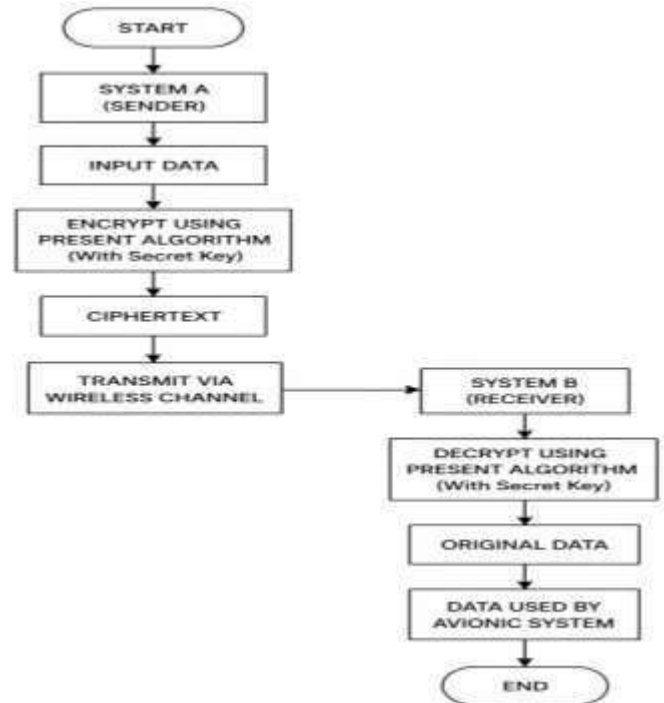


Fig: Flow chart of how data flows from sensors to the MFD display.

IV. SYSTEM IMPLEMENTATION

Working Principle:

Sensor Data Generation: Sensor values like altitude, temperature, and fuel are generated using MATLAB. These values simulate real-time aircraft conditions. MATLAB helps in testing without physical sensors. Data can change dynamically to represent real scenarios.

Data Pre-processing: Generated data is usually in analog or floating-point format. It is converted into integer values for easier processing. This reduces complexity in embedded systems. Ensures uniform data representation for further steps.

Binary Conversion (16-bit): Each parameter is converted into a 16-bit binary format. Binary representation uses 0s and 1s. Fixed length ensures consistency in processing. Maintains accuracy while controlling data size.

Data Block Formation (64-bit): All 16-bit values are combined into one 64-bit block. Includes altitude, temperature, fuel, and an extra parameter. This block becomes input to encryption. Matches PRESENT algorithm requirements.

Key Initialisation: A secret key (80-bit or 128-bit) is initialised. The same key is used at the transmitter and receiver. It generates round keys for encryption. Ensures secure communication.

Initial Key Mixing: The data block is combined with the key using the XOR operation. This step is called key mixing. Makes encryption dependent on the key. Adds initial security layer.

Substitution (S-Box): Data passes through the S-Box for substitution. Bits are replaced using a predefined table. Introduces non-linearity in data. Makes patterns hard to detect.

Permutation Process: Bits are rearranged in a specific pattern. Spreads information across the data block. Improves diffusion of data. Small changes create large output differences.

Repeated Rounds (31): Key mixing, substitution, and permutation are repeated. A total of 31 rounds are performed. Each round uses a different key. Increases overall encryption strength.

Cipher Text Generation: Final output after rounds is cipher text. Data becomes unreadable and secure. Cannot be understood without the key. Ready for safe transmission.

Secure Data Transmission: Cipher text is transmitted wirelessly. Uses RF or Wi-Fi communication. Encryption protects data from attackers. Ensures a safe communication channel.

Data Reception: The receiver collects encrypted data. The same secret key must be available. Data remains secure during reception. Ready for the decryption process.

Decryption Process: Reverse operations of encryption are applied. Includes inverse permutation and

substitution. Key mixing is also reversed. Done for 31 rounds to recover data.

Data Separation: 64-bit block is split into 16-bit values. Each part represents a parameter. Separates altitude, temperature, fuel data. Prepares for final conversion.

Conversion to Original Values: Binary values are converted back to decimal. Represents real-world sensor readings. Restores original data format. Ensures accuracy of information.

Data Display: Final values are displayed on system or MATLAB. Can use LCD or monitoring interface. Confirms successful transmission. Ensures reliable and secure communication.

RESULTS:

Time	Altitude (ft)	Temp (C)	Fuel (%)
1	35002.69	-44.63	79.93
2	35007.00	-44.57	79.86
3	35004.83	-44.50	79.85
4	35018.68	-44.77	79.83
5	35022.31	-44.78	79.79
6	35021.28	-44.81	79.75
7	35028.33	-44.52	79.71
8	35022.29	-44.38	79.68
9	35024.73	-44.17	79.63
10	35023.22	-44.12	79.57

Fig 6: Data collected from sensors.

Ciphertext

2314874388433447517
12676155840537925062
13706456981032765145
1971163341437381828
4150891225335914517
2009731034173554453
4510761210053071211
9367510449315074102
6896698569477552803
4503891363840272635

Fig. 7: Encrypted Data

Dec_Alt	Dec_Temp	Dec_Fuel
35003.00	-44.60	79.90
35007.00	-44.60	79.90
35005.00	-44.50	79.90
35019.00	-44.80	79.80
35022.00	-44.80	79.80
35021.00	-44.80	79.80
35028.00	-44.50	79.70
35022.00	-44.40	79.70
35025.00	-44.20	79.60
35023.00	-44.10	79.60

Fig 8: Decrypted Data

V.CONCLUSION

This project presents a secure and efficient approach for intra-avionic communication using lightweight cryptography, specifically the PRESENT algorithm. It ensures data confidentiality and integrity while operating with minimal computational and memory requirements, making it highly suitable for resource-constrained avionics systems. The use of wireless communication helps reduce system complexity, wiring, and overall aircraft weight, while encryption protects the data from unauthorised access and cyber threats during transmission. The MATLAB implementation successfully validates the encryption and decryption processes, demonstrating reliable performance. Overall, this work highlights the effectiveness of lightweight cryptographic techniques in enabling secure, low-power, and efficient communication in modern wireless avionics systems.

REFERENCES

- [1]. A. Kumar, P. Reji, D. Sheshu E., S. K. R., S. Karthik, and S. S. I, "Wireless Intra-Aircraft Communication System using Wi-Fi and IoT," International Journal of Engineering and Advanced Technology (IJEAT), vol. XX, no. XX, pp. XX-XX, 2020.
- [2]. W.H Zheng, J.t Armstrong," Wireless intra-spacecraft communication: the benefits and Systems,2010, pp.75-78. The challenges ", Adaptive Hardware.
- [3]. Raja Naeem Akram, Konstantinos Markantonakis, Sharadha Kanyawasam, Shahid Ayub, Amar Seam, Robert Atkinson, "Challenges of Security and Trust in Avionics Wireless Networks", 978-1-4799 8940-9/15/\$31.00, IEEE Conference,2015.
- [4]. Kyle McHugh, Jr., Walter Alkpedeye, Thaier Hayajneh, "Next Generation Wireless-LAN: Security Issues and Performance Analysis", 978-1-5090-4228-9/17/\$31.00, IEEE Conference, 2017.
- [5]. CW Zhao, J Jegatheesan, Sc Loon, "Exploring IoT Application Using Raspberry Pi", International Journal of Computer ..., 2015 - Ijcna.Org
- [6].U. Schwark, "Update on Compatibility Studies Between W Alc Systems And Radio Altimeters in the Frequency Band 4 200-4 400 Mhz," Icao Aeronautical Communications Panel (Acp), Lima, Peru, Sep. 2013.