Grenze International Journal of Engineering and Technology, January Issue

ADS-B Flight Data Acquisition and Secured Transmission

Dakshitha K[1], Shashank S. S[2] and Ravishankar Holla[3]
[1-3] Department of Electronics and Communication Engineering, RV College of Engineering Bangalore, India
Email: dakshithak.ec20@rvce.edu.in, {shashankss.ec20, ravishankarholla}@rvce.edu.in

***Abstract*— Air traffic control has undergone a revolution due to the emergence of Automatic Dependent Surveillance Broadcast (ADS-B) technology by offering real-time flight information in the realm of civil aviation. Unfortunately, when the ADS-B protocol was first proposed, it lacked encryption and other built-in security features, making it a prime target for fraudulent attacks. The goal of this work is to improve the security of ADS-B data during transmission to address various data vulnerabilities. By utilizing a combined approach that incorporates AES (Advanced Encryption Standard) and SHA-256 (Secure Hash Algorithm), along with hardware-based security measures through an ESP32 and LoRa transmission system, the system ensures robust data security. The research results indicate that AES encryption, while exhibiting slightly higher memory usage compared to SHA-256, maintains effective throughput, thereby ensuring operational efficiency without significantly impacting data transfer rates.**

***Index Terms*—ADS-B, Raspberry Pi, AES, SHA-256, FlightAware Dongle, ESP-32, LoRa Module**

I. INTRODUCTION

When ADS-B technology was introduced, the aviation sector saw a dramatic change. ADS-B technology improves situational awareness and boosts flight operations efficiency, providing air traffic control with exclusive benefits [5].

ADS-B also has some security challenges due to its vulnerability resulting from open transmission. The safety and reliability of aviation systems are thus threatened when there is unauthorized access, eavesdropping, or manipulation of this information.

The primary goal is to enhance ADS-B data security during transmission by capturing real-time data and applying encryption. Using AES and SHA algorithms, the data is securely transmitted through wireless channels within an IoT framework, ensuring the confidentiality and integrity of critical flight information.

II. BACKGROUND

A. Overview of ADS-B Technology

Traditional systems relied on ground-based radar to monitor aircraft positions. But now, with the introduction of ADS-B, they rely on aircraft broadcasting their important information using onboard GPS receivers and transmitters. ADS-B's 128-bit format offers a reliable foundation for sending important flight data.

Grenze ID: 01.GIJET.11.1.

Additionally, the shift from ground-based radar to ADS-B not only enhances accuracy but also significantly improves situational awareness for both pilots and air traffic controllers. This system provides pilots with precise information about the surrounding traffic. The integration of ADS-B into the NextGen air traffic management system marks a substantial technological leap, ensuring safer and more efficient skies.

B. Current Vulnerabilities

Despite its advantageous aspects, the ADS-B data's public transmission poses potential security vulnerabilities. The main issue concerns the absence of standard ADS-B transmission authentication and encryption techniques, which exposes it to diverse security risks. In the absence of strong security protocols, unauthorized individuals may take advantage of the system hence jeopardizing aviation safety and security [15].

These security threats can be mitigated through deploying strong encryption and integrity verification mechanisms that would safeguard the ADS-B signals from unauthorized access. As such, research efforts are focused on developing comprehensive security solutions to enhance the resilience of ADS-B technology against emerging threats in the evolving landscape of aviation communication.

III. LITERATURE REVIEW

A. Critical Analysis

Research on ADS-B security has explored various methods to address its vulnerabilities, including trajectory prediction algorithms and spoofing detection using deep neural networks. While these efforts have improved security, they remain incomplete, lacking the multi-layered defenses needed to tackle emerging risks effectively.

The AES algorithm processes data in 128-bit blocks. Initially, the plaintext block undergoes substitutions and permutations. Every byte in the block is replaced with a matching value from a specified lookup table during the Sub-bytes stage [10]. The following is an algebraic illustration of this transformation:

$$A'_{i,j} = A^{-1}_{i,j} \qquad (1)$$

Where $A'_{i,j}$ represents the original byte value and $A^{-1}_{i,j}$ represents the substituted value. Additionally, the ShiftRows step cyclically shifts the bytes within each row of the block, ensuring a diffusion effect. Symbolically, this operation can be denoted as:

$$ShiftRows(A) \qquad (2)$$

Furthermore, the MixColumns transformation combines the bytes of each column through matrix multiplication with a fixed polynomial matrix. This operation can be expressed as:

$$MixColumns(A) \qquad (3)$$

The encryption key is then expanded one last time to provide a set of keys that are utilized in every encryption cycle.The key expansion process involves various mathematical operations such as rotation, substitution, and XOR operations. Mathematically, this can be represented as:

$$X_i = X_{i-1} \oplus t(X_{i-1}) \qquad (4)$$

Where X_i represents the ith round key and t(.) represents a transformation function. Together, these mathematical operations of the AES algorithm, provide robust encryption and ensure the security of data.

SHA-256 is a hashing process that converts any length information into a 256-bit output in a hashed format. The input message is first padded to make sure its overall length is multiples of 512 bits. To establish this padding, one "1" bit is added, followed by a sufficient number of "0" bits, and finally, the actual message length is represented in 64 bits. After padding, the message is divided into 512-bit units for further processing. Each block undergoes a series of transformations through functions and constants. The main computational process includes initializing eight 32-bit hash values $X_0, X_1 \ldots X_7$ with specific constants. For each 512-bit block, a message schedule array, Y[q], is created with 64 entries:

$$Y[q] = \begin{cases} m[q] & \text{for } 0 \le t \le 15 \\ \sigma_1(Y[q-2]) + Y[q-7] + \sigma_0(Y[q-15]) + Y[q-16] & \text{for } 16 \le t \le 63 \end{cases} \qquad (5)$$

Where (σ_0) and (σ_1) are defined as:

$$\sigma_0(p) = (p \gg 18) \oplus (p \gg 7) \oplus (p \gg 3) \qquad (6)$$

$$\sigma_1(p) = (p \gg 10) \oplus (p \gg 19) \oplus (p \gg 17) \quad (7)$$

Here, $\gg$ denotes a right rotation. The compression function then updates the hash values using a series of logical functions and constants $C[q]$.

$$T1 = \Sigma_1(L) + X + Y[q] + \mathrm{Ch}(L, M, N) + C[q] \quad (8)$$

$$T2 = \Sigma_0(S) + \mathrm{Maj}(S, T, U) \quad (9)$$

where:

$$\Sigma_0(q) = (q \gg 13) \oplus (q \gg 22) \oplus (q \gg 2) \quad (10)$$

$$\Sigma_1(q) = (q \gg 6) \oplus (q \gg 11) \oplus (q \gg 25) \quad (11)$$

$$\mathrm{Ch}(u, v, w) = (\neg u \wedge v) \oplus (u \wedge v) \quad (12)$$

$$\mathrm{Maj}(d, e, f) = (e \wedge f) \oplus (d \wedge f) \oplus (d \wedge e) \quad (13)$$

The final hash value is obtained by connecting the hashes Y_0 through Y_7 after processing each individual block. This mathematical structure ensures the robustness and security of the SHA-256 algorithm, making it highly resistant to collisions and preimage attacks.

IV. Methodology

A. Hardware Setup

The ADS-B data retrieval system setup is designed to ensure efficient and secure reception of real-time ADS-B data. The principal components include a Raspberry Pi, FlightAware Dongle, Antenna, ESP-32 modules (Node MCU and WEMOS-LOLIN32), and LoRa-Ra02 Module. The Raspberry Pi serves as the central processing unit of this architecture, capturing and storing all incoming ADS-B information from the FlightAware Dongle while the Antenna picks up transmissions made by aircraft within its range [12]. Figure 1 below represents the block diagram showing components' interconnections and flow of ADS-B data. The Data Acquisition System constantly receives ADS-B signals which are extracted and stored in JSON format. The ESP-32 modules later enable wireless transmission between sender and receiver nodes.

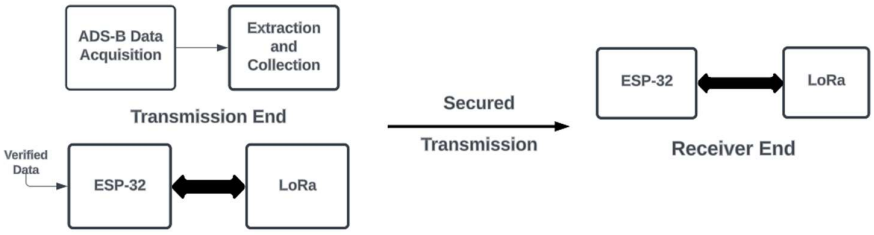


Figure 1. Block Diagram of Hardware Setup

V. Implementation

A. Data Security in ADS-B Transmission

Securing data transmission is paramount in the ADS-B system to protect critical flight information. To achieve confidentiality, the system integrates the AES algorithm, aligned with the ADS-B messages' data format. This integration is coded in Arduino IDE complemented by ESP-32 and LoRa as its necessary firmware[11]. From a mathematical perspective, AES processes a substitution-permutation network that is shown by the following equation and consists of several operational cycles:

$$T = E_C(S) \quad (14)$$

Where T is the ciphertext, denotes the AES function with key, and represents the plaintext message. It includes replacing bytes, shifting rows, mixing columns, and adding keys. These transformations work together to create a robust encryption system capable of integrating with ESP-32 and LoRa modules.

$$Y = \text{SHA-256}(I) \quad (15)$$

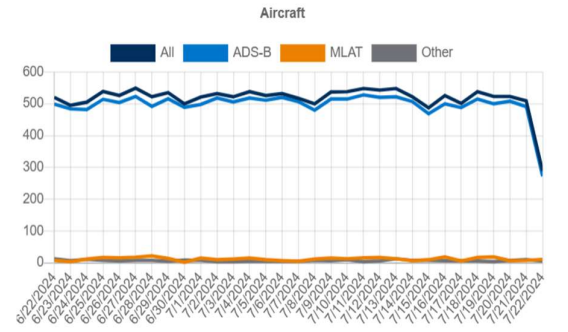
Where Y represents the hash value, and I denote the input message. The combined implementation of AES and SHA-256 within the IoT framework provides a dual-layered security framework for ADS-B data transmission. AES ensures confidentiality by encrypting the data at the sender, while SHA-256 guarantees integrity by

generating hash values. The received values are decrypted and hashed values are compared. Together, these algorithms ensure the secure and reliable transmission of critical flight information.

VI. RESULTS

A. Data Capture and Transmission

The ADS-B data retrieval system's architecture is designed to ensure secure reception and transmission of ADS-B data. To facilitate further analysis, the captured ADS-B data is manually converted into a JSON file format. The FlightAware data acquisition and the JSON file structure of ADS-B data for a single flight are illustrated in Figure 2 and 3 respectively, highlighting the organization of ADS-B data into a readable and accessible format.



AIRCRAFT REPORTED

	7/22/2024	7/21/2024	7/20/2024	7/19/2024	7/18/2024	7/1
ADS-B Mode-S	272	491	508	500	515	
MLAT	11	8	7	19	17	
Other	6	10	8	4	6	
Total	289	509	523	523	538	

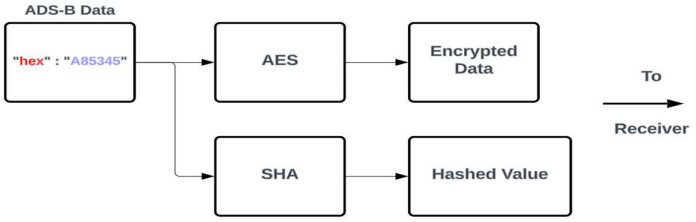
Figure 2. Flight Aware Data Acquisition


```
{    "hex": "A85345",
    "flight": "BAW119 ",
    "alt": 37300,
    "gs": 453.9,
    "track": -30.5,
    "longitude": 77.7285,
    "latitude": 13.7448,
    "speed_type": "GS",
    "timestamp": "2024-04-25T14:25:09.031902Z",
    "mach": "0.788",
    "emergency": "none",
    "category": "A3",
    "nav_altitude_mcp": "0",
    "nav_heading": "99",
    "nav_modes": "1100",
    "nav_qnh": "29.92",
    "nav_rate_of_climb": "0",
    "nav_slip_skid": "0",
    "is_on_ground": "0"
}
```


Figure 3. ADS-B Data

B. Combined Implementation

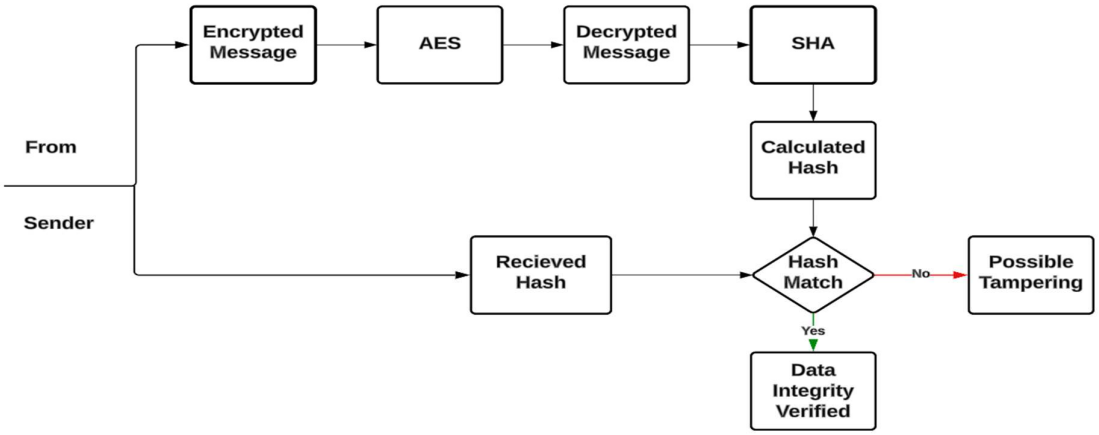
The combined implementation of AES and SHA-256 at the sender and receiver nodes adds dual layers of security to the ADS-B Data Retrieval setup's data transmission process. At the sender node, AES encryption is applied to the captured ADS-B data before transmission. AES encrypts the data using a 128-bit encryption key which is hardcoded into both the nodes of ESP-32.




```
Message to be Encrypted: hex:A85345
Encrypted Message: B6 10 8E 61 82 E1 71 B3 38 11 C1 60 CB A4 C1 63
Hash Value:76 46 CB 20 F 9F 19 62 A6 1D 88 EC 11 BE F8 89 1A B3 D8 EC 59 1 49 B4 CB B4 FA D4 77 2B A4 AC
Message to be Encrypted: flight:BAW119
Encrypted Message: 44 9A 0 86 9 EF 99 45 34 67 B9 A5 7F F9 FA 86
Hash Value:8C 11 47 AD EF 3F 87 DF 50 6C 9E FD 27 78 CB C1 3A D6 3E 68 4 6F BC 49 94 D3 E2 CE A FF 49
Message to be Encrypted: alt_baro: 24000
Encrypted Message: AB 46 70 B5 7A BD 6A FE 51 38 20 6F 7C 92 22 55
Hash Value: B6 D7 38 D9 40 86 7 49 D FC D3 27 8F C8 4A 70 A3 B3 3F 99 A4 A B2 6C 19 23 6A 23 CD 90 43 3C
Message to be Encrypted: alt_geom: 24300
Encrypted Message: 8E F7 4F 18 11 21 FD 26 B 5A A3 9C 9B 2 CC 8D
Hash Value: 6B B6 2B 7D E2 A 14 96 6D 81 F9 27 A5 53 CD 57 25 1F AD 7E 9E 7B 46 BE 9B A8 99 6 4A 87 29 96
```

Figure 6. Combined Implementation Results at Sender

After AES encryption, SHA-256 hashing is used to generate a hashed value of the ADS-B data. This value is transmitted alongside the encrypted data and recalculated at the receiver node. By comparing the two hashed values, data integrity is verified; discrepancies indicate possible tampering. The integration of AES and SHA-256 enhances security by ensuring both confidentiality and integrity, overcoming the limitations of each individual algorithm. This dual implementation offers a robust security framework critical for modern aviation transmissions.




```
Decrypted Message: hex:A85345
Received Hash: 76 46 CB 20 F 9F 19 62 A6 1D 88 EC 11 BE F8 89 1A B3 D8 EC 59 1 49 B4 CB B4 FA D4 77 2B A4 AC
Calculated Hash:76 46 CB 20 F 9F 19 62 A6 1D 88 EC 11 BE F8 89 1A B3 D8 EC 59 1 49 B4 CB B4 FA D4 77 2B A4 AC
HashMatch: True
Statement: Data Integrity Verified
Decrypted Message: flight:AAL1852
Received Hash: 8C 11 47 AD EF 3F 87 DF 50 6C E 9E FD 27 78 CB C1 3A D6 3E 68 4 6F BC 49 94 D3 E2 CE A FF 49
Calculated Hash: 8C 11 47 AD EF 3F 87 DF 50 6C E 9E FD 27 78 CB C1 3A D6 3E 68 4 6F BC 49 94 D3 E2 CE A FF 49
HashMatch: True
Statement: Data Integrity Verified
```

Figure 7. Combined Implementation Results at Receiver

VII. Comparative Analysis

A. Criteria Outline

The comparative analysis between AES and SHA-256 focused on key parameters calculated using the Arduino IDE. These metrics are crucial for assessing each algorithm's efficacy in immediate data processing scenarios

TABLE I: PARAMETERS FOR AES AT SENDER AND RECEIVER

Parameter	**AES (Sender)**	**AES (Receiver)**
Initialization Speed	1.2 ms	1.7 ms
Execution Time	25 ms (Encryption)	22 ms (Decryption)
Throughput	985.7 kbit/s	977.0 kbit/s

TABLE II: PARAMETERS FOR SHA-256 AT SENDER AND RECEIVER

PARAMETER	SHA-256 (SENDER)	SHA-256 (RECEIVER)
INITIALIZATION SPEED	2.7 ms	3.2 ms
EXECUTION TIME	50 ms(Hashing)	40 ms (Verification)
THROUGHPUT	972.9 kbit/s	936.6 kbit/s

TABLE III: MEMORY USAGE AT SENDER AND RECEIVER

PARAMETER	**SENDER**	**RECEIVER**
PROGRAM MEMORY	211.2 kilobytes	214.1 kilobytes
EXECUTION DYNAMIC MEMORY	13.6 kilobytes	13.4 kilobytes

These values demonstrate the feasibility of each algorithm for implementation on resource-constrained devices.

VIII. Discussions

A. Advantages and Security Limitations

Comparing the findings with existing solutions reveals the advantages and limitations of utilizing AES and SHA-256 for securing ADS-B data transmission. AES and SHA-256, widely used in similar contexts, are renowned cryptographic algorithms aimed at preserving the ADS-B data integrity, privacy and validity. A notable improvement involves customizing the setup of AES and SHA-256 to meet the specific requirements of ADS-B data transmission. By seamlessly integrating AES encryption and SHA-256 hashing within the ESP-32 modules, the security of wireless communication between sender and receiver nodes is significantly improved. This integration ensures adherence to industry standards and best practices, thereby enhancing the overall security stance of the system [16].

B. Challenges and Solutions

Despite their robust security features, AES and SHA-256 still face challenges, leading to longer execution times and computational overhead compared to less secure alternatives. Moreover, the memory usage of AES and SHA-256 may constrain resource-constrained devices like the ESP-32, potentially hindering scalability and performance in large-scale deployments. Future optimizations could explore hardware acceleration for AES and SHA-256, as well as lightweight cryptographic algorithms tailored for IoT environments. Implementing advanced key management techniques, such as key agreement protocols or public-key cryptography, could streamline cryptographic key administration, alleviating the administrative burden. Continuous research and innovation are essential to overcome limitations and ensure scalability, efficiency, and resilience in aviation systems [15].

VIII. CONCLUSION

In conclusion, the research emphasizes the effectiveness of the combined use of SHA-256 hashing and AES encryption to adequately safeguard ADS-B data transmission. Through experimentation, the feasibility of integrating these cryptographic algorithms within the ESP-32 modules has been demonstrated. Looking ahead, future research directions could focus on optimizing the implementation of AES and SHA-256 for resource-constrained environments, especially with the usage of IoT devices like LoRa. The aviation industry can strengthen the resilience of ADS-B communication networks and maintain their safety alongside the dependability of global air traffic management in civil aviation.

ACKNOWLEDGMENT

The authors wish to thank the Department of Electronics and Communication Engineering at RV College of Engineering along with the Principal K.N Subramanya and Head of Department Dr. Ravish Aaradhya for their support in the project.

REFERENCES

[1] J. Habibi Markani, A. Amrhar, J.-M. Gagné, and R. J. Landry, "Security establishment in ads-b by format-preserving encryption and blockchain schemes," Applied Sciences, vol. 13, no. 5, p. 3105, September 2023.

[2] Y. Zhang, Z. Jia, C. Dong, Y. Liu, L. Zhang, and Q. Wu, "Recurrent lstm-based uav trajectory prediction with ads-b information," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, pp. 1–6. doi: 10.1109/GLOBECOM48099. 2022.10000919, 2022.

[3] Passarella, Rossi and Aditya, and Nurmaini, Siti and Arsalan, Osvari and Kurniati, Rizki, "An investigation of landing irregularities based on ADS-B data from Sultan Syarif Kasim II Airport, Indonesia," December 2022. doi: 10.15224/978-1-63248-195-5-09.

[4] R. Ronen and B. Ben-Moshe, "Cyberattack on flight safety: Detection and mitigation using LoRa," Sensors, vol. 21, p. 4610, July 2021. doi: 10.3390/s21134610.

[5] Z. Wu, T. Shang, and A. Guo, "Security issues in automatic dependent surveillance - broadcast (ADS-B): A survey," IEEE Access, vol. 8, pp. 122147-122167, 2020. doi: 10.1109/ACCESS.2020.3007182.

[6] T. Hidayat and R. Mahardiko, "A systematic literature review method on AES algorithm for data sharing encryption on cloud computing," International Journal of Artificial Intelligence Research, vol. 4, pp. 49-57, April 2020. doi: 10.29099/ijair.v4i1.154.

[7] A. Abdulrazaq, A. S. Yaro, A. A. Ahmad, and S. Namadi, "Surveillance radar system limitations and the advent of the automatic dependent surveillance broadcast system for aircraft monitoring," ATBU Journal of Science, Technology and Education, vol. 7, pp. 9-15, 2019. Available: https://api.semanticscholar.org/CorpusID:182017420.

[8] X. Ying, J. Mazer, G. Bernieri, M. Conti, L. Bushnell, and R. Poovendran, "Detecting ADS-B spoofing attacks using deep neural networks," 2019 IEEE Conference on Communications and Network Security (CNS), pp. 187-195, 2019. doi: 10.1109/CNS.2019.8802732.

[9] M. R. Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system," International Journal of Critical Infrastructure Protection, vol. 19, 2017. doi: 10.1016/j.ijcip.2017.10.002.

[10] A. M. Abdullah et al, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," 28th International Conference on Microelectronics (ICM), IEEE, vol. 16, no. 1, p. 11, 2016.

[11] M. A. Bahnasawi, K. Ibrahim, A. Mohamed, M. K. Mohamed, A. Moustafa, K. Abdelmonem, Y. Ismail, and H. Mostafa, "ASIC-oriented comparative review of hardware security algorithms for internet of things applications," 2016 28th International Conference on Microelectronics (ICM), pp. 285-288, 2016. doi: 10.1109/ICM.2016.7847871.

[12] B. S. Ali, "System specifications for developing an automatic dependent surveillance-broadcast (ADS-B) monitoring system," International Journal of Critical Infrastructure Protection, vol. 15, pp. 40-46, 2016. doi: https://doi.org/10.1016/j.ijcip.2016.06.004.

[13] Z. Cao, G. Yi, B. Wu, J. Li, and D. Xiao, "Analysis and improvement of AES key expansion algorithm," 2022 International Conference on Artificial Intelligence and Computer Information Technology (AICIT), pp. 1-5, 2022. doi: 10.1109/AICIT55386.2022.9930239.

[14] A. Abdulaziz, A. Yaro, A. A. Ahmad, M. Kabir, and H. B. Salau, "Optimum receiver for decoding automatic dependent surveillance broadcast (ADS-B) signals," American Journal of Signal Processing, vol. 5, pp. 23-31, January 2015. doi: 10.5923/j.ajsp.20150502.01.

[15] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ADS-B," IEEE Communications Magazine, vol. 52, no. 5, pp. 111-118, 2014. doi: 10.1109/MCOM.2014.6815901.

[16] R. Agbeyibor, "Secure ADS-B: Towards airborne communications security in the Federal Aviation Administration's next generation air transportation system," 2014. Available: https://api.semanticscholar.org/CorpusID:107840026.

[17] R. Francis, R. Vincent, J.-M. Noël, P. Tremblay, D. Desjardins, A. Cushley, and M. Wallace, “The flying laboratory for the observation of ADS-B signals,” International Journal of Navigation and Observation, vol. 2011, 2011. doi: 10.1155/2011/973656.
[18] M. R. Manesh and N. Kaabouch, “Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system,” International Journal of Critical Infrastructure Protection, vol. 19, pp. 16-31, 2017. doi: https://doi.org/10.1016/j.ijcip.2017.10.002.
[19] F. Martel, R. Schultz, and Z. Wang, “Unmanned aircraft systems sense and avoid flight testing utilizing ADS-B transceivers,” 2010. doi: 10.2514/6.2010-3441.
[20] H. Abu Damis, D. Shehada, C. Fachkha, A. Gawanmeh, and J. N. Al-Karaki, “A microservices architecture for ADS-B data security using blockchain,” 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), pp. 1-4, 2020. doi: 10.1109/ICSPIS51252.2020.9340152.