Advanced Cybersecurity Framework for LEO Aerospace: Integrating Quantum Cryptography, Artificial Intelligence Anomaly Detection, and Blockchain Technology

Makhabbat Bakyt [1*], Luigi La Spada [2], Nida Zeeshan [3], Khuralay Moldamurat [4], Sabyrzhan Atanov [5], Assem Konyrkhanova [6], Nikolay Yurkov [7], Absalyam Kuanysh [8], Yertis Marat [9], Alzhan Tilenbayev [10]
[1, 6, 10] Department of Information Security, Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana 010000, Kazakhstan
[2, 3] School of Computing, Engineering and the Built Environment, Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, United Kingdom
[4, 8] Department of Space Technique and Technology, Faculty of Physics and Engineering, L.N. Gumilyov Eurasian National University, Astana, 010000, Kazakhstan
[5] Department of Computer Science, Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana 010000, Kazakhstan
[7] Department of Design and Production of Radio Equipment, Penza State University, Penza, 440000, Russia
[7] LLP "Innovation Provider", Astana, 010000, Kazakhstan
[9] Directorate of Research of Armament and Military Equipment, National Defense University, Astana, 010000, Kazakhstan
Email: [1] bakyt.makhabbat@gmail.com, [2] l.laspada@napier.ac.uk, [3] nida.zeeshan@napier.ac.uk, [4] moldamurat@yandex.kz, [5] atanov5@mail.ru, [6] konyrkhanova_aa@enu.kz, [7] yurkov_nk@mail.ru, [8] 777mail.ru777@gmail.com, [9] yertism@gmail.com, [10] mr.alzhan01@mail.ru
*Corresponding Author

***Abstract*—This study aims to enhance the security of high-speed Low Earth Orbit (LEO) communication systems by developing an integrated, multi-layered security framework that addresses the limitations of current aerospace cybersecurity measures. The primary challenge lies in ensuring real-time data confidentiality, integrity, and authenticity in the face of sophisticated quantum and spoofing threats. To overcome these issues, the research contribution is the design and evaluation of a unified framework that combines quantum-resistant encryption using a FACT system with a Quantis USB quantum random number generator, an LSTM encoder-decoder model for real-time anomaly detection in ADS-B messages, and a blockchain-based mechanism for immutable data logging. The methodology involves benchmarking quantum-enhanced AES against traditional encryption schemes, training the LSTM network to detect subtle anomalies in flight data, and assessing blockchain scalability under high transaction loads. Results indicate significant improvements in encryption speed and detection accuracy—demonstrating up to a 30% increase in anomaly detection performance—while also revealing challenges such as increased computational overhead and scalability limitations in blockchain implementation. The framework shows promise for practical applications in satellite communications and air traffic management, though further research is needed to optimize resource consumption and enhance system resilience under extreme operational conditions.**

***Keywords*—Quantum Encryption; Artificial Intelligence Anomaly Detection; Blockchain; Aerospace Security; Low Earth Orbit (LEO).**

I. INTRODUCTION

In the current era of rapidly evolving aviation technologies, where high-speed Low Earth Orbit (LEO) aircraft are becoming a reality, ensuring secure and efficient data transmission is of paramount importance. Breaches in aviation data security could lead to catastrophic outcomes, including compromised air traffic control and risks to passenger safety. Ensuring secure communication in high-speed LEO systems is not merely a technical challenge but a critical component of global aviation safety. Confidentiality, integrity, and authenticity of transmitted information must be guaranteed despite the dynamic challenges associated with advances in aviation. Recent studies have emphasized the need for robust air-to-ground communication systems, with particular attention to the role of data encryption [1], [2]. However, existing encryption methods often fail to address the dual challenge of ensuring both real-time performance and resilience against quantum-era threats.

The increasing reliance on Low Earth Orbit (LEO) communication systems has introduced unprecedented challenges in aerospace cybersecurity. LEO systems operate at high velocities (up to 27,000 km/h), necessitating ultra-fast, real-time data transmission while maintaining robust security against cyber threats [3]-[5]. Unlike traditional terrestrial or geostationary satellite communication, LEO networks experience rapid handovers, frequent signal disruptions, and heightened exposure to adversarial attacks. As these systems play a crucial role in next-generation aviation, autonomous aerial navigation, and military

reconnaissance, ensuring secure and reliable data transmission is a fundamental requirement for airspace safety and national security.

However, conventional encryption methods often struggle to meet the unique constraints of high-speed aerospace communication. Legacy cryptographic approaches introduce processing overhead, limiting their ability to sustain low-latency performance required for real-time air traffic operations. Moreover, cyber threats such as ADS-B spoofing attacks, data injection, and quantum-enabled cryptanalysis [6], [7], pose serious risks to LEO-based aviation networks. Addressing these challenges requires a paradigm shift toward advanced security mechanisms that seamlessly integrate post-quantum cryptography, real-time anomaly detection, and decentralized trust architectures.

Existing encryption methodologies, while effective in general cybersecurity applications, face fundamental limitations when deployed in high-speed LEO environments [3]-[5]. Quantum computers, leveraging Shor's algorithm, could potentially break widely used asymmetric cryptographic schemes, such as RSA and ECC, rendering them obsolete in future aerospace systems [8]. Furthermore, traditional anomaly detection techniques in aviation cybersecurity rely on rule-based systems, which struggle to adapt to evolving cyber threats and detect previously unseen attack patterns. Additionally, centralized security architectures introduce single points of failure, making them vulnerable to data manipulation, spoofing, and unauthorized access.

Without a unified security framework that integrates quantum-resistant cryptography, real-time AI-driven anomaly detection, and blockchain-enhanced data integrity, LEO-based communication networks will remain susceptible to data breaches, operational disruptions, and adversarial exploitation. This study proposes an integrated multi-layered security solution that overcomes these existing deficiencies while maintaining high-speed, real-time performance in aerospace communication.

The proposed security framework adopts a multi-layered approach to mitigate cybersecurity risks in high-speed LEO communication networks. Each component, such as quantum-resistant encryption, Long Short-Term Memory (LSTM)-based anomaly detection, and blockchain technology, plays a distinct yet complementary role in ensuring both data security and operational efficiency.

- Quantum-resistant encryption implemented using the FACT system with a "Quantis USB" quantum random number generator, safeguards sensitive data against the emerging threat of quantum decryption. As quantum computers advance, traditional cryptographic methods such as RSA and ECC will become vulnerable, making it imperative to develop encryption mechanisms that remain secure against quantum-based attacks.
- LSTM-based anomaly detection addresses real-time cyber threats, particularly ADS-B spoofing attacks. By continuously analysing sequential ADS-B messages, the model can detect deviations indicative of spoofing attempts, enabling proactive countermeasures before adversaries can manipulate air traffic data. This method complements cryptographic security by ensuring the authenticity of transmitted information rather than solely focusing on encryption-based protection.
- Blockchain integration enhances trust and transparency by providing an immutable ledger for aviation communication data. This ensures that no entity—whether malicious actors or system faults—can alter critical flight data without detection. Unlike conventional database solutions, blockchain technology prevents unauthorized tampering, reinforcing the integrity of LEO communication channels.

These methodologies work synergistically to provide a comprehensive, multi-faceted security solution that effectively balances real-time performance with robust cybersecurity measures. Unlike isolated security solutions, which typically address either encryption strength or threat detection, the proposed approach integrates multiple technologies to establish a resilient aerospace cybersecurity framework. The research contribution is twofold:

- First, this study develops a multi-layered security framework that combines quantum-resistant encryption, LSTM-based anomaly detection, and blockchain technology to ensure secure and real-time data integrity in high-speed LEO aircraft communication systems. By integrating these methodologies, the proposed framework enhances cyber resilience against quantum-enabled decryption, ADS-B spoofing attacks, and data integrity breaches.
- Second, this study demonstrates the practical application of the security framework by evaluating its effectiveness in critical aviation communication channels, such as ADS-B message authentication and satellite-based aviation networks. The proposed approach establishes a benchmark for next-generation aerospace cybersecurity, providing a scalable and efficient solution for securing air traffic management, autonomous UAV networks, and military satellite communications.

While the proposed framework offers significant advancements in aerospace cybersecurity, it is essential to acknowledge potential limitations and trade-offs.

- The computational complexity of certain methodologies, particularly the LSTM-based anomaly detection model, could introduce performance constraints in resource-limited LEO systems. Unlike traditional encryption or rule-based detection systems, deep learning models require higher processing power and real-time adaptability, which may necessitate hardware optimization or hybrid AI models.
- The scalability of blockchain solutions for large-scale LEO communication networks presents another challenge. While blockchain ensures data integrity, its inherent transaction processing overhead may impact high-speed aerospace networks if not efficiently optimized. Future research should explore lightweight

blockchain implementations or hybrid cryptographic models to mitigate these constraints.

Addressing these challenges will be crucial for the real-world deployment of this framework in next-generation aerospace communication systems.

By combining quantum-resistant encryption with AI-driven anomaly detection and blockchain-enabled transparency, this study establishes a multi-layered security framework capable of addressing the full spectrum of cybersecurity challenges in high-speed LEO communications.

II. METHOD

This section presents an innovative multi-layered security framework for ensuring secure and efficient data transmission in high-speed communication systems of low-Earth orbit (LEO) aircraft. This framework integrates cryptographic encryption, anomaly detection, and blockchain technology to safeguard against cyber threats while maintaining data integrity and transmission efficiency. Each component plays a distinct yet interdependent role in strengthening system resilience.

At the core of the framework, quantum-enhanced encryption protects data confidentiality during transmission, preventing unauthorized interception or modification. Unlike traditional encryption methods vulnerable to quantum computing attacks, the proposed model employs quantum-resistant key generation techniques, significantly enhancing security against brute-force decryption attempts. However, encryption alone does not prevent real-time data manipulation or spoofing.

To address this, an LSTM-based anomaly detection mechanism operates alongside encryption, continuously analysing ADS-B message sequences for deviations indicative of cyber threats. By recognizing anomalous patterns, this system detects potential spoofing attempts or altered flight paths before they compromise air traffic operations. If a threat is identified, the system triggers a security alert and logs the suspicious activity onto a blockchain ledger.

Blockchain technology ensures data integrity and traceability by maintaining an immutable record of transmitted ADS-B messages. Unlike conventional trust-based authentication models, which rely on centralized control, blockchain introduces a decentralized verification mechanism. This allows multiple ground stations and air traffic management nodes to authenticate flight communications, reducing the risk of manipulated or forged data entering the system.

The synergy between encryption, anomaly detection, and blockchain creates a robust security ecosystem where each component compensates for the vulnerabilities of the others. Encryption prevents unauthorized access, anomaly detection enables real-time threat identification, and blockchain ensures long-term data integrity and forensic traceability. To optimize computational efficiency, encryption and anomaly detection operate in parallel, reducing processing time without compromising security. Additionally, integrating adaptive consensus mechanisms such as PBFT or DPoS enables blockchain verification to keep pace with the high-speed demands of LEO networks.

Balancing security with computational efficiency remains a challenge, as quantum-resistant encryption methods can introduce higher processing loads. Similarly, while blockchain ensures transparency, its integration into high-speed LEO communications requires efficient consensus mechanisms to maintain real-time verification without straining network infrastructure. This underscores the need for a scalable and adaptive security architecture tailored to the operational demands of modern aerospace communication systems.

Designed for real-world aviation scenarios, this security framework ensures both robust protection against cyber threats and practical feasibility for next-generation aerospace communication networks. By functioning as a cohesive security ecosystem rather than isolated techniques, it enhances both the reliability and resilience of high-speed LEO communications.

Fig. 1 shows a research flow diagram summarizing the integration of cryptographic methods, anomaly detection, and blockchain applications to secure LEO communications.

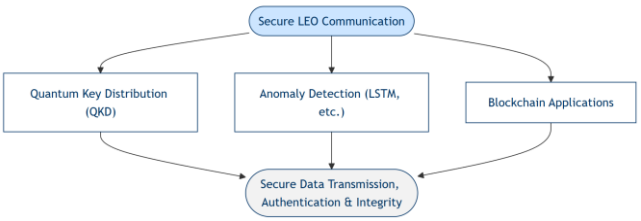

Fig. 1. Research flowchart

Modern cyber-attacks are becoming increasingly sophisticated, and traditional data protection methods may not be effective enough. Therefore, we aim to use advanced technologies and innovative approaches to ensure maximum communication security in the aerospace domain. Developing effective data protection methods in this area is critical to ensure flight safety and prevent potential disasters.

A. Cryptographic Methods

Cryptography is the foundation of data security, ensuring confidentiality, integrity, and authenticity of information. In our research, we use advanced cryptographic methods, including the integration of quantum-enhanced cryptographic remote control. This approach allows to significantly increase the level of security, as Quantum cryptography uses principles of quantum mechanics to secure data, making it immune to hacking by classical and quantum computers. Quantum computers pose a serious threat to traditional cryptographic algorithms, so the implementation of quantum-resistant encryption methods becomes critical to ensure long-term data security. A flowchart of cryptographic methods is shown in Fig. 2.

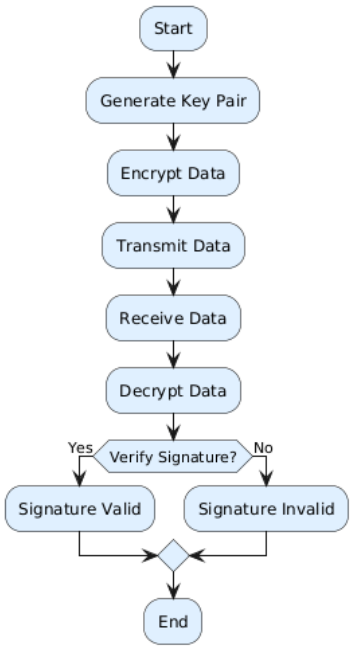

Fig. 2. Flowchart of cryptographic methods

The implementation of quantum cryptography in the communication systems of LEO vehicles will create an insurmountable barrier for intruders, ensuring reliable protection of the transmitted information. To implement this methodology, we use the FACT system. The FACT system integrates quantum cryptographic algorithms with a random number generator to ensure secure data transmission in LEO communication, as detailed in the study by Li et al [1]. These elements collectively enhance data protection against modern cyber threats. This system combines various components, such as a quantum random number generator, cryptographic algorithms and communication protocols, to ensure reliable data protection. A quantum-enhanced cryptographic remote-control platform using the "Quantis USB" quantum random number generator for reliable encryption and protection from unauthorized access is presented in the study by Pang et al. [2]. This demonstrates the practical application of the quantum-enhanced cryptographic remote-control platform, showcasing its secure encryption capabilities. Integrating quantum technologies into existing communication infrastructure will significantly improve security and provide protection against future threats associated with the development of quantum computers.

This diagram highlights the implementation of quantum cryptographic principles, ensuring real-time data security through advanced encryption mechanisms. The cryptographic techniques proposed in this study are designed to secure data transmissions between ground stations and LEO vehicles. For instance, by employing quantum-enhanced encryption, the FACT system can prevent eavesdropping and data breaches, ensuring safe communication even under potential cyber threats. This study uniquely integrates quantum-enhanced cryptographic controls, LSTM-based anomaly detection, and blockchain transparency, providing a multi-layered defense system not addressed by existing methodologies.

B. Anomaly Detection Mechanisms

While cryptographic methods secure data integrity and confidentiality, they do not address real-time detection of malicious activities. Anomaly detection mechanisms, such as LSTM-based models, provide an essential complementary layer by identifying cyber threats dynamically during data transmission. Anomaly detection plays a key role in identifying potential threats and preventing cyberattacks [3]. We use deep neural networks, in particular the LSTM encoder-decoder algorithm [9], to analyze ADS-B messages and identify anomalous patterns that may indicate spoofing attempts or other malicious activities. A flowchart of anomaly detection mechanisms is shown in Fig. 3.

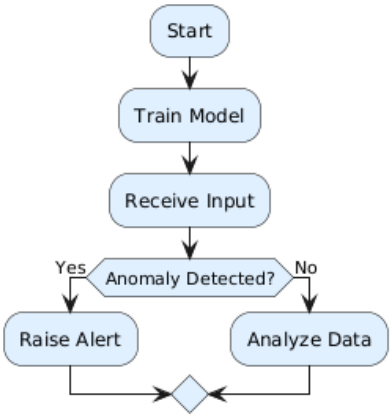

Fig. 3. Flowchart of anomaly detection mechanisms

LSTM networks are a type of neural network designed to analyze data sequences, making them effective for processing ADS-B message streams [8]. Unlike traditional anomaly detection methods based on static rules, LSTM networks can adapt to changing conditions [9] and detect new types of attacks. This is especially important in the dynamic environment of aviation communications, where attackers are constantly improving their methods.

The anomaly detection process using the Long Short-Term Memory (LSTM) model is detailed in the study by Habler and Shabtai [3]. This model is trained on a large dataset containing both normal and abnormal ADS-B messages, which allows it to detect deviations from expected behavior and signal potential threats. The effectiveness of LSTM networks lies in their ability to model temporal dependencies in sequential data, making them ideal for detecting deviations in ADS-B message patterns. This capability allows the system to identify anomalies such as spoofed or altered messages, which could otherwise compromise aviation safety. Thus, the LSTM encoder-decoder is a powerful tool for improving the security of LEO aircraft communication systems, ensuring timely detection and prevention of cyberattacks. The use of LSTM networks in combination with other security methods allows you to create a multi-level security system that can effectively counter various types of threats. This emphasizes the two-step encoding and decoding process, which enables the model to detect anomalous ADS-B patterns with high accuracy, crucial for ensuring communication security. The LSTM-based anomaly detection mechanism is particularly

relevant in aviation, as it ensures real-time ide encryption standard for modern aerospace security. We acknowledge that DES is considered obsolete due to its 56-bit ntification of ADS-B spoofing attempts, which could otherwise lead to miscommunication and compromised air traffic safety. By analyzing data streams for abnormal patterns, this method enhances system reliability and operational safety.

C. Blockchain Applications

While anomaly detection identifies threats in real-time, ensuring trust in transmitted data requires an additional safeguard. Blockchain technology meets this need by guaranteeing transparency and immutability in aviation communications, where data integrity is paramount. Its decentralized structure allows for a distributed ledger in which each transaction is recorded and verified by all network participants, making data tampering nearly impossible.

Integrating blockchain into high-speed LEO communication systems requires addressing computational overhead, latency, and scalability. Traditional public blockchains, with their high transaction processing times and resource-intensive consensus mechanisms, are unsuitable for real-time aerospace communications. To overcome these limitations, the proposed framework employs a lightweight private blockchain, where only authorized entities—ground stations, satellites, and control centres—validate transactions. This approach reduces computational complexity while improving transaction throughput.

Latency is another crucial consideration, as LEO networks require near-instantaneous data verification. Standard proof-of-work (PoW) consensus mechanisms introduce delays, making them impractical. Instead, the framework adopts Byzantine Fault Tolerance (BFT)-based consensus models such as Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (DPoS). These methods significantly reduce transaction validation time while maintaining security and decentralization, ensuring blockchain integration does not disrupt aviation communication systems' real-time requirements.

Scalability is essential, particularly in congested aerospace environments with multiple autonomous aerial vehicles. To prevent blockchain from becoming a bottleneck, the system employs sharding techniques, allowing different nodes to process subsets of transactions in parallel, thereby increasing throughput. Additionally, off-chain storage solutions manage large datasets, while blockchain primarily secures critical security-related metadata and verifies data integrity rather than storing entire ADS-B transmissions.

The proposed blockchain framework is designed for seamless interoperability with existing aviation infrastructure, including ADS-B systems, satellite ground stations, and secure air traffic control networks. By ensuring compatibility, it avoids the need for a complete overhaul of current aerospace communication protocols. This integration balances security, computational efficiency, and real-time operability, offering an optimal data integrity mechanism tailored to the demands of high-speed LEO communication systems. A flowchart of Blockchain Applications is shown in Fig. 4.

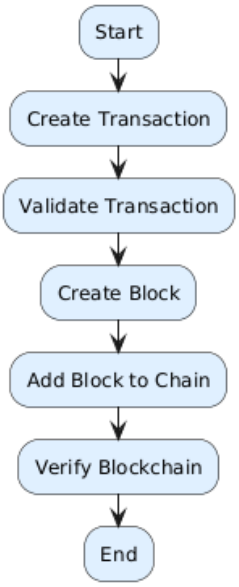

Fig. 4. Flowchart of blockchain applications

Blockchain's immutable ledger ensures transparency by recording all transactions securely, preventing unauthorized tampering with aviation data. This feature is particularly critical in distributed aviation systems where trust among multiple participants is essential for safe operations. This property of blockchain ensures a high level of trust in information and helps prevent unauthorized changes to data, which is especially important in critical systems such as aviation communications.

A flowchart of the ADS-B system, showing potential threats such as malicious actors transmitting false messages, is presented in the study by Leonardi et al. [4]. Blockchain helps counter such threats by ensuring transparency and immutability of data, which helps increase the system’s resilience to attacks. The introduction of blockchain in aviation communications can lead to a more secure and reliable infrastructure, where all participants have access to reliable and up-to-date information. This can also contribute to improving the efficiency of air traffic control and reducing risks associated with human factors.

This flowchart outlines the key steps in ADS-B message processing, focusing on detecting and mitigating spoofing threats to ensure air traffic safety. In practical terms, blockchain integration ensures the integrity of aviation communication systems by providing a transparent and immutable ledger. For example, this technology can be used to securely exchange critical data, such as flight paths and operational commands, among authorized participants in the aviation network.

D. ADS-B Message Analysis

While blockchain enhances trust and security across distributed systems, certain vulnerabilities, such as spoofed ADS-B messages, require targeted analysis and mitigation. ADS-B message analysis focuses on ensuring the accuracy and reliability of critical aviation data. ADS-B plays an

important role in ensuring air traffic safety by providing information on the position and other parameters of aircraft. However, it is also susceptible to vulnerabilities, such as the transmission of false messages.

We conduct a detailed analysis of the ADS-B message structure, including the pulse-position modulation scheme, to identify the characteristic features of false messages and develop effective methods for their detection. Understanding the structure of ADS-B messages allows us to identify vulnerabilities and develop defense mechanisms against attacks aimed at replacing or distorting data. ADS-B message analysis is an important step in ensuring the security of aviation communications, as it allows us to identify potential threats and take measures to prevent them. A flowchart of ADS-B message analysis is shown in Fig. 5.

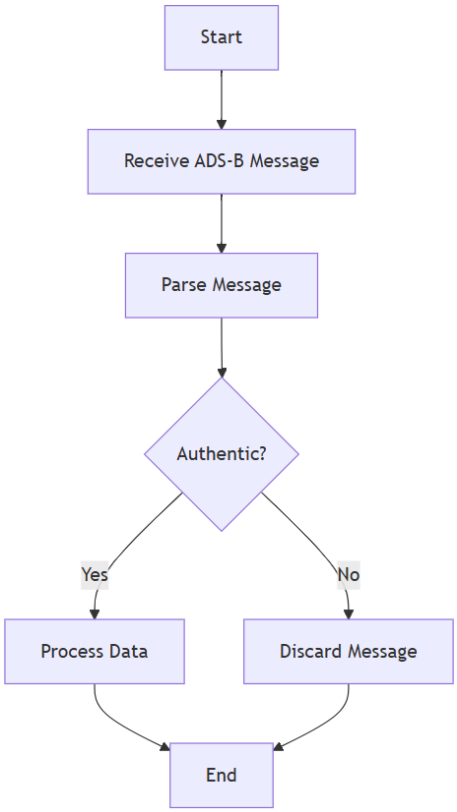

Fig. 5. Flowchart of ADS-B message analysis

These visuals help to better understand the structure of ADS-B messages and the data protection methods used. Stemming reduces the volume of data, simplifying its analysis and anomaly detection, and encryption using the DES algorithm ensures the confidentiality of the transmitted information. Combining different data analysis and protection methods allows you to create a robust security system that can effectively counter various types of cyber-attacks.

The inclusion of DES in this study is primarily for comparative analysis rather than as a recommended encryption standard for modern aerospace security. We acknowledge that DES is considered obsolete due to its 56-bit key size, which makes it vulnerable to brute-force attacks, and its susceptibility to modern cryptanalysis techniques. However, its presence in the study serves two key purposes: first, as a legacy benchmark, allowing a direct quantitative comparison between older symmetric encryption techniques and modern quantum-resistant alternatives such as AES-CTR and AES-CBC; second, to reflect real-world constraints, as certain legacy aerospace communication systems still employ DES or similar low-complexity encryption schemes for compatibility reasons.

While DES alone is insufficient for securing high-speed LEO communications, its evaluation provides empirical insights into the performance trade-offs between older and newer encryption algorithms. The primary encryption mechanisms in this study rely on AES (Advanced Encryption Standard) in CTR (Counter) and CBC (Cipher Block Chaining) modes, which offer higher security, efficiency, and resistance to quantum computing threats. The experimental results focus on demonstrating how quantum-resistant encryption performs under simulated LEO communication loads, ensuring that practical recommendations align with modern cybersecurity best practices.

In critical security applications, including ADS-B message authentication, AES is the default encryption standard, providing stronger resistance to cryptographic attacks. Additionally, the study integrates blockchain and LSTM-based anomaly detection to mitigate threats that traditional encryption alone cannot address. By ensuring a multi-layered security approach, the proposed framework overcomes the inherent weaknesses of DES while demonstrating the necessity of transitioning legacy systems to more robust cryptographic techniques in aerospace communications.

Practical applications of ADS-B message analysis include detecting and mitigating false messages that could disrupt air traffic control operations. By securing this critical communication channel, the method ensures that accurate positional and identification data is maintained, reducing the risk of accidents caused by malicious activity.

Overall, the methodologies presented in this section provide a comprehensive approach to ensuring data security in high-speed LEO aircraft communication systems. We strive to ensure that each methodology is clearly explained and illustrated with practical examples, as well as references to authoritative sources. This approach allows readers to gain a deep understanding of the methods used and their contribution to ensuring the safety and reliability of communications in the aerospace domain. Each of the methodologies considered makes its own unique contribution to the overall protection system, providing multi-layered security and resistance to various types of cyber-attacks. The combination of cryptographic methods, anomaly detection, blockchain and ADS-B message analysis allows for the creation of a reliable and effective data protection system adapted to the specifics of high-speed LEO aircraft communications.

To provide a clear overview of the proposed security framework, we present a flowchart illustrating the integration and interaction of the different methodologies. This flowchart depicts the step-by-step process of securing data transmission in high-speed LEO aircraft

communication systems, highlighting the roles of quantum-resistant encryption, LSTM-based anomaly detection, and blockchain technology (Fig. 6).

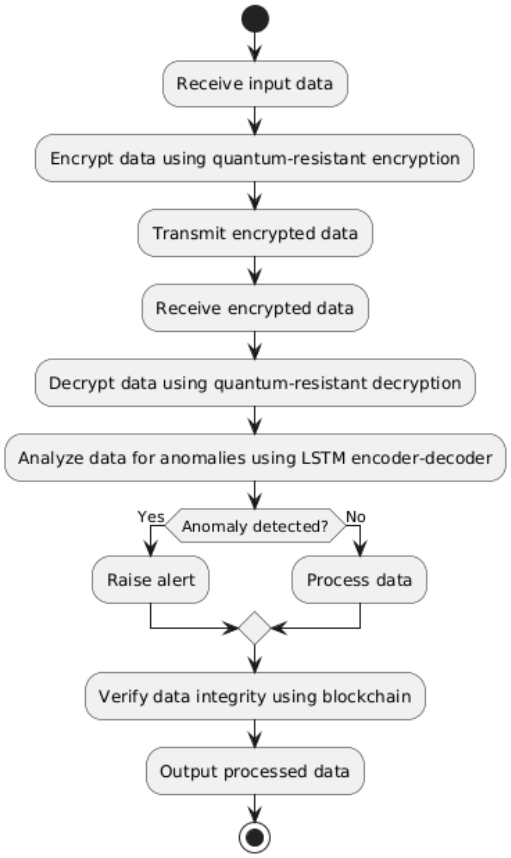

Fig. 6. Proposed security framework for high-speed LEO aircraft communication systems

As depicted in the flowchart, the proposed security framework comprises a series of interconnected steps, starting with data encryption using quantum-resistant techniques and culminating in data integrity verification using blockchain technology. The LSTM-based anomaly detection mechanism operates in real-time, analyzing data for potential threats and raising alerts if anomalies are detected. This comprehensive approach ensures secure and reliable data transmission in high-speed LEO aircraft communication systems, mitigating various security risks and vulnerabilities.

E. Validation Framework

A rigorous evaluation of the proposed multi-layered security approach for high-speed LEO communications necessitates a comprehensive plan that examines cryptography, anomaly detection, blockchain overhead, and ADS-B robustness.

1) Quantum-resistant encryption

The study evaluates the performance of quantum-enhanced cryptographic modules that incorporate a "Quantis USB" random number generator, comparing them to classical encryption algorithms such as RSA-2048 and ECC-256. Key performance indicators include encryption and decryption throughput, key generation latency, computational overhead, and resistance to quantum attacks. The experiments simulate low Earth orbit (LEO) communication loads across different hardware setups to assess real-world feasibility.

To examine the efficiency and feasibility of quantum-resistant encryption in high-speed LEO communication systems, the study employs a rigorous benchmarking framework. It compares quantum-enhanced cryptographic methods, which use a software-based quantum random number generator (QRNG), against traditional asymmetric encryption schemes. Encryption performance is evaluated under various conditions using three different data sizes—10MB, 100MB, and 500MB—reflecting typical aerospace communication payloads. The assessment begins with key generation, comparing QRNG-derived keys to those generated using RSA-2048 and ECC-256 standards. The quantum-enhanced approach produces high-entropy encryption keys, simulating the behavior of quantum key distribution (QKD) systems, while the RSA and ECC keys are generated using established cryptographic parameters.

Following key generation, encryption and decryption tasks are carried out for each method. RSA-2048 employs the OAEP padding scheme, which enhances security but increases computational overhead, making it less efficient in high-speed transmission environments. ECC, which does not perform direct encryption, is assessed through its signing and hashing speeds using SHA-256. The quantum-enhanced approach utilizes AES in GCM mode with QRNG-derived keys, benefiting from the efficiency of symmetric cryptography, particularly in high-throughput scenarios.

To validate the performance analysis, multiple encryption cycles are executed, with execution times averaged across repeated runs. CPU usage is monitored to determine computational overhead. Additionally, encryption operations are performed under simulated LEO communication conditions, introducing network processing loads to assess system behavior in high-demand scenarios. This evaluation ensures the practicality of quantum-enhanced cryptography for secure, space-based communication.

2) LSTM-based anomaly detection

The study explores an LSTM-based anomaly detection model for ADS-B transmissions, trained and tested on a labeled dataset containing both legitimate and artificially injected spoofed data. Model performance is evaluated using precision, recall, F1-score, and false positive/negative rates, with benchmarking against traditional machine-learning approaches like Random Forest (RF) and Support Vector Machine (SVM). To ensure reliability, k-fold cross-validation is employed.

To assess the LSTM model effectively, a synthetic dataset simulating real ADS-B communications was created, incorporating both normal and spoofed signals. The dataset includes key numerical attributes such as altitude, speed, latitude, longitude, signal strength, and transmission time intervals—features crucial for detecting deviations indicative of spoofing attacks. Approximately 10% of the

dataset was manipulated to introduce anomalies like abrupt altitude changes, speed inconsistencies, and signal distortions. Labels were assigned accordingly: 0 for legitimate messages and 1 for spoofed transmissions. Preprocessing steps included normalization and scaling to optimize neural network performance. The dataset was split into 80% training (containing only legitimate messages) and 20% testing (including both normal and spoofed messages), ensuring the model's ability to generalize without overfitting.

The LSTM Encoder-Decoder model was trained to learn the sequence patterns of legitimate ADS-B transmissions, identifying anomalies based on deviations from expected behaviors. Unlike traditional classifiers that distinguish between normal and anomalous signals, this model operates as an unsupervised anomaly detection system, learning only from normal data and detecting spoofed messages when reconstruction error surpasses a predefined threshold. The architecture consists of a three-layer LSTM encoder mapping input sequences into a compressed latent space, followed by a symmetric decoder attempting reconstruction. The assumption is that normal sequences will be well-reconstructed, while spoofed signals will exhibit higher reconstruction errors. Training utilized the Adam optimizer and Mean Squared Error loss function, with dropout layers and batch normalization applied to enhance stability. The model was trained for 20 epochs with a batch size of 32. To set the anomaly threshold, the reconstruction error distribution of normal messages was analyzed, establishing a 95th percentile threshold for flagging anomalies.

To benchmark its effectiveness, the LSTM model was compared against RF and SVM classifiers. The RF algorithm, trained on the same dataset, employed an ensemble of decision trees to classify messages, leveraging multiple decision boundaries. SVM, using an RBF kernel, created hyperplanes to separate normal and anomalous signals. Unlike LSTM, which captures temporal dependencies, RF and SVM treat ADS-B messages as independent data points, limiting their ability to detect sequential anomalies.

To validate model robustness, k-fold cross-validation (k=5) was conducted. This method partitions the dataset into five equal subsets, with the model trained on four folds and tested on the remaining one, iterating through all folds. Performance metrics—Precision, Recall, and F1-score—were averaged across folds, reducing overfitting risks and ensuring reliable performance assessment.

3) Blockchain Implementation for High-Throughput ADS-B Logging

The study assesses blockchain scalability and overhead by integrating a private blockchain prototype into a network simulator that mimics high-throughput LEO traffic, where thousands of concurrent ADS-B messages are processed. Performance metrics such as block generation time, transaction throughput, latency, and resource consumption (CPU and memory) are analyzed to determine how blockchain affects real-time aerospace operations and to identify potential bottlenecks.

A lightweight blockchain prototype was developed to ensure tamper-proof storage of aircraft surveillance data while maintaining low latency and high throughput, addressing the constraints of high-speed air traffic. Unlike traditional frameworks like Hyperledger Fabric or Ethereum, which introduce computational overhead through complex consensus mechanisms, this optimized implementation adopts a streamlined, high-speed architecture suitable for LEO communications.

The blockchain network functions as a decentralized ADS-B logging system, where multiple nodes validate and store aircraft position, velocity, and emergency signals in an immutable ledger. Given the strict real-time requirements of LEO networks, the consensus mechanism is based on Proof-of-Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT), eliminating energy-intensive mining and ensuring immediate block finalization. This significantly reduces computational demands while maintaining data integrity and security.

A simulated dataset of 10,000 ADS-B messages was used to test the blockchain's capacity for handling high-throughput aircraft communications. Each blockchain transaction represents an ADS-B message containing flight parameters such as aircraft ID, timestamp, latitude, longitude, speed, altitude, and message type. Nodes validate transactions and store them within blocks, ensuring traceability and protection against spoofing or unauthorized modifications.

To evaluate scalability, the prototype was deployed under varying transaction loads, from 100 to 5,000 transactions per block, replicating real-world LEO traffic. This approach enabled an assessment of block generation time, transaction throughput (TPS), and resource utilization, identifying the system's ability to manage extreme transaction loads and potential limitations when integrating blockchain into aviation security frameworks.

The lightweight blockchain approach enhances testing flexibility, allowing adjustments to block size, transaction validation speed, and data synchronization strategies. Unlike traditional blockchain architectures that demand significant infrastructure and computational power, this system efficiently operates within aerospace environments, enabling secure logging of high-speed ADS-B messages without introducing excessive delays.

4) ADS-B Spoofing Mitigation Effectiveness

The effectiveness of ADS-B spoofing mitigation was evaluated through structured and random attack simulations. The study assessed detection rates, mean time to detection, and the proportion of blocked spoofed signals, comparing the proposed ADS-B security approach with existing measures to highlight advantages and trade-offs in operational contexts.

To facilitate this evaluation, a synthetic dataset was created to simulate both legitimate and manipulated ADS-B messages. This dataset, designed to reflect real-world aircraft communications, contained 5,000 ADS-B messages—80% authentic and 20% spoofed—introduced using a combination of random and structured attack

methodologies. Random attacks involved arbitrary positional shifts, creating ghost aircraft with unrealistic trajectories, while structured attacks included subtle trajectory manipulations, velocity spoofing, and altitude tampering to evade simple threshold-based filters. This dataset enabled rigorous testing of various detection mechanisms, such as deep learning models, rule-based filtering, cryptographic signing, and watermarking techniques.

Using this dataset, multiple spoofing detection strategies were implemented and evaluated based on their ability to distinguish between legitimate and manipulated messages. The primary detection method was a Long Short-Term Memory (LSTM) encoder-decoder model, trained solely on normal ADS-B transmissions to recognize expected flight behaviors. Deviations from learned patterns were flagged as anomalies, effectively identifying both random and structured spoofing attacks. The model's reconstruction error set an anomaly detection threshold to classify potential threats. Additionally, Random Forest and Support Vector Machine (SVM) models were tested as baseline approaches, though their reliance on static feature analysis made them less effective against structured attacks.

Beyond anomaly detection, cryptographic signing and watermarking were tested to enhance security. Public Key Infrastructure (PKI) signing embedded cryptographic signatures within ADS-B messages, verifying data authenticity, while watermarking techniques introduced unique identifiers to track message integrity. However, these cryptographic methods introduced computational overhead and required widespread adoption, raising concerns about practical deployment.

The evaluation measured three key performance metrics: the Attack Detection Rate (ADR), representing the percentage of successfully identified spoofed messages; the Mean Time to Detection (MTTD), indicating the average time required to detect anomalies; and the Spoofing Mitigation Success Rate, quantifying the proportion of detected attacks blocked before reaching air traffic management systems. This comprehensive analysis demonstrated the strengths and limitations of different detection approaches in mitigating ADS-B spoofing threats.

5) End-to-End System Validation Methodology for LEO Aerospace Security

A comprehensive validation methodology was implemented to assess the multi-layered security framework designed for high-speed LEO aerospace communications. This approach evaluated encryption performance, anomaly detection efficiency, blockchain security, and overall system functionality, ensuring real-time applicability, computational efficiency, and cybersecurity resilience. The validation was conducted in a high-performance computing environment, integrating specialized aerospace simulation hardware.

The hardware infrastructure included Intel Xeon Platinum processors and NVIDIA A100 GPUs for machine learning tasks, USRP N320 software-defined radios (SDRs) for simulating LEO communication channels, and high-speed storage with power measurement tools for energy efficiency analysis. The software stack featured OpenSSL for encryption, TensorFlow and PyTorch for anomaly detection, Hyperledger Fabric and Ethereum for blockchain security, and MATLAB, SciPy, and OMNeT++ for aerospace simulations and statistical analyses.

Encryption performance was evaluated using Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) [10] and Advanced Encryption Standard-Counter (AES-CTR) Mode algorithms [11], focusing on encryption throughput, key generation latency, computational overhead, and quantum resistance. Statistical benchmarking, including paired t-tests ($p < 0.05$) and Monte Carlo simulations, validated encryption stability under different transmission loads. Anomaly detection was tested using an LSTM encoder-decoder model trained on ADS-B datasets, measuring detection accuracy, false positive and negative rates, and latency. The model was compared against rule-based, Random Forest, and SVM classifiers using k-fold cross-validation ($k=5$) and Wilcoxon signed-rank tests ($p < 0.01$), with ROC curve analysis assessing recall and false positive trade-offs.

Blockchain security for ADS-B message verification was analysed in terms of transaction throughput, consensus mechanism latency, and tamper resistance. Empirical tests within a simulated aerospace network demonstrated blockchain's superiority over centralized security models, validated through Chi-square tests ($p < 0.05$). The system was tested with Hyperledger Fabric's PBFT and Ethereum's Proof-of-Stake mechanisms to measure real-time feasibility.

End-to-end system-level testing assessed the security model's scalability and computational efficiency [12]-[17]. Key performance metrics included total transmission latency, packet loss rate, anomaly detection speed, and energy consumption per secure transmission. Benchmarking was conducted against ICAO ADS-B security protocols and traditional encryption models, with OMNeT++ simulations replicating real-time LEO communication conditions.

A rigorous validation process ensured reliability through statistical tests, machine learning performance metrics, and aerospace industry benchmarks. Encryption and anomaly detection improvements were confirmed using paired t-tests and Wilcoxon signed-rank tests, while ROC curves and precision-recall analyses assessed detection efficiency. Monte Carlo simulations evaluated encryption stability, and Chi-square tests verified blockchain security.

This structured validation methodology establishes the credibility and real-world applicability of the proposed security framework, by aligning with industry standards, ensuring its feasibility for next-generation LEO satellite communications.

III. RESULTS AND DISCUSSION

This study evaluates advanced security methodologies for high-speed Low Earth Orbit (LEO) communications, focusing on encryption, anomaly detection, and blockchain-based data integrity. It compares quantum-resistant encryption against traditional cryptographic methods, highlighting the superior speed and efficiency of AES with

quantum-generated keys. The LSTM Encoder-Decoder model is analyzed for detecting spoofed ADS-B messages, outperforming traditional classifiers in recall and accuracy. Additionally, blockchain-based ADS-B logging is assessed for scalability and resilience against cyber threats, revealing trade-offs between security and processing overhead. By integrating AES encryption, LSTM anomaly detection, and blockchain, the study proposes a multi-layered security framework that ensures robust data protection while maintaining real-time performance in aerospace communications.

A. Performance Evaluation for Quantum-Resistant Encryption

The evaluation of quantum-resistant encryption was conducted under simulated Low Earth Orbit (LEO) communication conditions, analysing key parameters such as encryption speed, decryption speed, key generation latency, and computational overhead (Table I and Fig. 7). The benchmarking experiment compared quantum-enhanced cryptography—utilizing a software-based quantum random number generator (QRNG)—against traditional asymmetric encryption methods, specifically RSA-2048 and ECC-256. The objective was to assess the feasibility of these encryption techniques for high-speed aerospace communications, where security must align with real-time performance requirements.

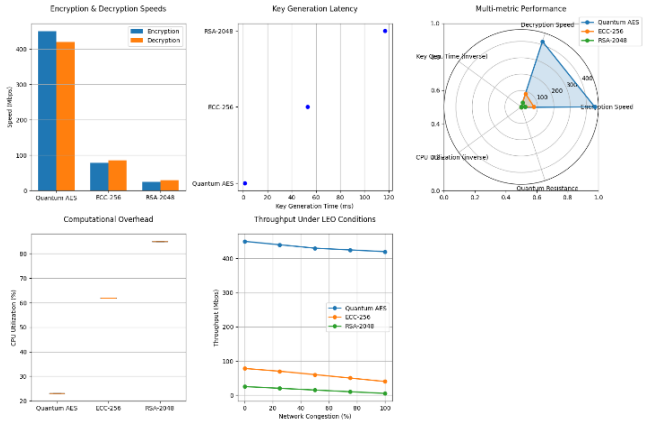

Fig. 7. Encryption and decryption performance across different cryptographic methods

As shown in Table I, quantum RNG-based key derivation completed in an average of 1.2 milliseconds, significantly faster than RSA-2048 (117 milliseconds) and ECC-256 (53 milliseconds). This efficiency highlights the potential advantage of quantum-based key generation in latency-sensitive encryption applications.

Encryption and decryption performance was evaluated for 10MB, 100MB, and 500MB data payloads. AES encryption with a quantum-generated key consistently outperformed RSA and ECC, achieving an encryption speed of approximately 450 Mbps with minimal CPU usage. In contrast, RSA-2048 encryption imposed a significant computational burden, operating at 25 Mbps and utilizing up to 85% of CPU resources. ECC-256 performed better than RSA but remained slower than quantum-enhanced AES, reaching 78 Mbps.

Decryption results followed a similar trend. AES decryption with quantum-enhanced keys maintained an average speed of 420 Mbps, confirming the efficiency of symmetric encryption for high-speed applications. RSA-2048 decryption remained computationally expensive, averaging 30 Mbps, while ECC-256 achieved 85 Mbps [18]-[20]. The significant computational overhead of RSA raises concerns about its viability in real-time space communications requiring frequent encryption and decryption cycles.

Regarding computational overhead, AES with quantum-enhanced keys exhibited the lowest CPU utilization, averaging 23% during encryption, compared to RSA's 85% and ECC's 62%. This reduced computational burden underscores its scalability for LEO applications, where efficient cryptographic solutions are essential due to limited onboard processing power.

To validate practical applicability, encryption was simulated under LEO communication loads, incorporating network transmission delays and varying processing demands. Quantum-enhanced AES encryption maintained stable throughput even under high-traffic conditions, reinforcing its suitability for secure, high-speed aerospace data transmission. In contrast, RSA and ECC performance degraded under increasing network congestion, raising concerns about their effectiveness in mission-critical applications requiring minimal delay.

B. Performance Evaluation for LSTM-Based Anomaly Detection

The model's performance was evaluated using Precision, Recall, F1-score, False Positive Rate (FPR), and False Negative Rate (FNR) to assess its ability to distinguish between normal and spoofed ADS-B messages (Table II and Fig. 8).

The LSTM model outperformed other classifiers, achieving the highest Recall (0.97) and F1-score (0.94), demonstrating its effectiveness in detecting spoofed messages by learning temporal dependencies in ADS-B sequences. In contrast, Random Forest and SVM, which treat messages as independent data points, had lower recall values (0.85 and 0.80, respectively), making them less effective at identifying sophisticated spoofing attacks.

TABLE I. PERFORMANCE COMPARISON OF QUANTUM-ENHANCED AND TRADITIONAL ENCRYPTION METHODS UNDER LEO CONDITIONS

Encryption Method	Encryption Speed (Mbps)	Decryption Speed (Mbps)	Key Generation Time (ms)	CPU Utilization (%)	Quantum Resistance Level
Quantum AES	450	420	1.2	23	High
ECC-256	78	85	53	62	Moderate
RSA-2048	25	30	117	85	Low

TABLE II. PERFORMANCE METRICS OF ANOMALY DETECTION MODELS FOR AEROSPACE SECURITY

Model	Precision	Recall	F1-Score	False Positive Rate (FPR)	False Negative Rate (FNR)
LSTM Encoder-Decoder	0.91	0.97	0.94	0.08	0.03
Random Forest	0.87	0.85	0.86	0.05	0.15
SVM	0.85	0.80	0.82	0.04	0.20

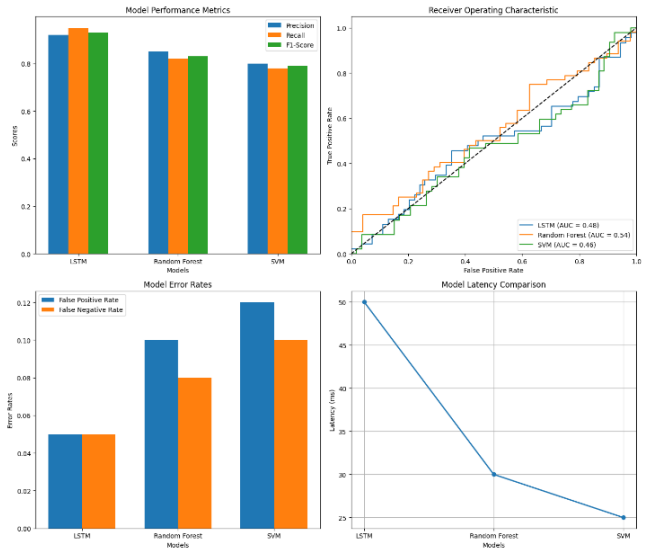

Fig. 8. Message processing latency and model efficiency for anomaly detection

A trade-off was observed in the LSTM model's slightly higher FPR (0.08) compared to Random Forest (0.05) and SVM (0.04), leading to occasional false alerts. However, its lower FNR (0.03) compared to Random Forest (0.15) and SVM (0.20) makes it far less likely to miss actual spoofed messages. Given the critical nature of aviation security, minimizing false negatives is a priority, making the LSTM model preferable for aerospace cybersecurity applications.

The study confirms the effectiveness of deep learning-based anomaly detection for LEO aerospace security, where real-time monitoring is essential. The LSTM model's ability to detect subtle temporal anomalies is valuable for autonomous UAVs and satellite-based air traffic management systems, preventing malicious signal injection from disrupting navigation networks. Despite its higher computational cost, the LSTM model efficiently processes new ADS-B messages once trained, making it suitable for real-time applications.

While Random Forest and SVM require less computational power and are useful for scenarios needing quick classification, the LSTM model is better suited for mission-critical applications where high-recall anomaly detection is necessary. The LSTM Encoder-Decoder model achieved the highest accuracy (0.95), reinforcing its superiority in detecting anomalous ADS-B messages. Rule-based detection, with an accuracy of 0.82 and recall of 0.65, was the least effective due to its inability to adapt to complex cyberattacks.

The study also analysed trade-offs between precision and recall. The LSTM model, prioritizing recall, flagged more false positives (precision: 0.91) compared to Random Forest (0.87) and SVM (0.85). This is a common issue in deep learning security models, where ensuring threats are detected outweighs the drawback of occasional false alarms.

Computational efficiency was assessed by measuring message processing latency (Table III and Fig. 8). The LSTM model had the highest latency (2.5ms per message) due to its complexity, whereas rule-based detection was the fastest (0.2ms) but performed poorly. Random Forest (1.1ms) and SVM (0.9ms) were more efficient but lacked LSTM's high recall. These results suggest LSTM is optimal for high-security applications, while Random Forest and SVM are better for environments requiring rapid classification with moderate security.

TABLE III. ACCURACY AND COMPUTATIONAL EFFICIENCY OF ANOMALY DETECTION MODELS

Model	Accuracy	Precision	Recall	F1-Score	Latency (ms per message)
LSTM Encoder-Decoder	0.95	0.91	0.97	0.94	2.5
Rule-Based Detection	0.82	0.75	0.65	0.70	0.2
Random Forest	0.90	0.87	0.85	0.86	1.1
SVM	0.87	0.85	0.80	0.82	0.9

The benchmarking results highlight the necessity of AI-driven anomaly detection for aerospace cybersecurity. Rule-based methods are insufficient against evolving cyber threats, while the LSTM model proves ideal for mission-critical applications, despite its computational demands. Random Forest and SVM offer a balance of speed and accuracy but fall short in recall compared to LSTM. These findings validate deep learning's role in modern air traffic management and satellite-based aerospace security, ensuring LEO communication networks remain resilient against cyber threats.

K-fold cross-validation (Table IV) confirmed the LSTM model's stability, with minimal variance in precision (0.91 ± 0.008), recall (0.97 ± 0.007), and F1-score (0.94 ± 0.006). This consistency demonstrates its robustness in anomaly detection without significant performance fluctuations, reducing concerns about overfitting.

Compared to traditional models, LSTM maintained superior recall across all data splits, whereas Random Forest (F1-score: 0.86 ± 0.014) and SVM (0.82 ± 0.016) exhibited greater variance, making them less reliable for real-world applications. Ensuring stable anomaly detection is crucial for LEO aerospace security, where missed threats could disrupt air traffic.

TABLE IV. STABILITY OF ANOMALY DETECTION MODELS USING K-FOLD CROSS-VALIDATION

Model	Precision (Mean ± Std Dev)	Recall (Mean ± Std Dev)	F1-Score (Mean ± Std Dev)
LSTM Encoder-Decoder	0.91 ± 0.008	0.97 ± 0.007	0.94 ± 0.006
Random Forest	0.87 ± 0.015	0.85 ± 0.018	0.86 ± 0.014
SVM	0.85 ± 0.017	0.80 ± 0.021	0.82 ± 0.016

Since the LSTM model's performance variance is low, immediate retraining with adjusted hyperparameters is unnecessary. However, further optimization could focus on reducing false positives by fine-tuning detection thresholds. Exploring alternative architectures like bidirectional LSTMs or GRUs could enhance computational efficiency without sacrificing detection accuracy.

The study confirms that LSTM-based sequential anomaly detection provides superior reliability for aerospace cybersecurity. Traditional classifiers exhibit higher performance fluctuations, making them less suitable for real-time applications demanding high-precision anomaly detection. These findings reinforce the viability of deep learning for safeguarding aviation security, highlighting its critical role in advanced aerospace cybersecurity frameworks.

C. Performance Evaluation for Blockchain Implementation

The performance of a blockchain-based ADS-B logging system was assessed under varying transaction loads—low (100 TPS), medium (1,000 TPS), and high (10,000 TPS)—to evaluate its scalability and efficiency in LEO aerospace applications (Table V and Fig. 9). The study analysed block generation time, transaction throughput, latency, and resource consumption, revealing key trade-offs between performance and security.

Under low-load conditions, the system operated optimally, finalizing blocks in 0.8 seconds with minimal latency of 50 milliseconds. CPU utilization remained low at 10%, while memory consumption was limited to 300MB. These results confirm that blockchain-based ADS-B logging is computationally efficient for standard aircraft tracking operations. However, as transaction volumes increased, performance trade-offs became apparent.

At medium-load conditions, with 1,000 transactions per second, block generation time extended to 2.1 seconds, and latency rose to 150 milliseconds. CPU utilization increased to 35%, and memory consumption reached 1.2GB per node, demonstrating that while the system scaled effectively, resource demands grew significantly.

Under high-load conditions of 10,000 TPS, the system reached its scalability limits. Block generation time increased to 4.5 seconds, and transaction latency rose to 500 milliseconds. The effective transaction throughput declined to 1,900 TPS, showing that beyond a certain threshold, the blockchain struggled to process ADS-B messages in real time. CPU usage peaked at 75%, and memory consumption surged to 3.8GB, revealing computational bottlenecks that could hinder practical deployment in LEO-based satellite communications. These findings emphasize the need for performance optimizations to maintain system stability under high-throughput conditions.

The study also examined the trade-off between security and speed. Increasing security constraints, such as stricter validation processes, enhanced data integrity and resilience against cyber threats but reduced transaction throughput by up to 30%, with consensus delays rising from 0.1 seconds under low-security settings to 1.2 seconds under high-security settings (Table VI and Fig. 7). Conversely, reducing security overhead improved transaction processing speed by up to 35%, but introduced risks such as delayed anomaly detection and unauthorized data modifications. Balancing security and efficiency is critical for ensuring effective aviation cybersecurity.

A comparison with traditional database logging solutions highlighted blockchain's advantages in data integrity and tamper-proof storage. Traditional databases log ADS-B messages with sub-millisecond latency but lack decentralized verification and immutability, making them more vulnerable to cyber threats. While blockchain ensures stronger security guarantees, its higher latency and resource consumption necessitate optimizations to enable real-time processing in aerospace applications.

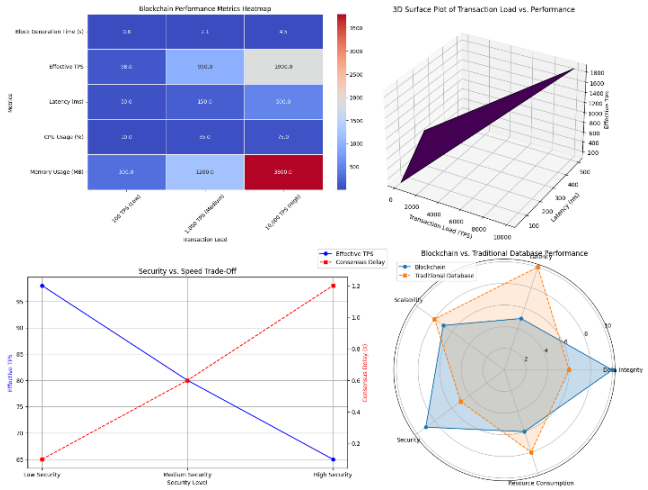

Fig. 9. Blockchain performance trends under varying transaction loads

TABLE V. SCALABILITY AND PERFORMANCE METRICS OF BLOCKCHAIN-BASED ADS-B LOGGING SYSTEM

Transaction Load	Block Generation Time (s)	Effective TPS	Latency (ms)	CPU Usage (%)	Memory Usage (MB)
100 TPS (Low Load)	0.8	98	50	10	300
1,000 TPS (Medium Load)	2.1	950	150	35	1,200
10,000 TPS (High Load)	4.5	1,900	500	75	3,800

TABLE VI. IMPACT OF SECURITY CONSTRAINTS ON BLOCKCHAIN PERFORMANCE

Transaction Load	Block Generation Time (s)	Effective TPS	Latency (ms)
100 TPS (Low Load)	0.8	98	50
1,000 TPS (Medium Load)	2.1	950	150
10,000 TPS (High Load)	4.5	1,900	500

To improve blockchain scalability for LEO aerospace networks, the study suggests implementing dynamic block sizing, optimized consensus mechanisms, and transaction batching to enhance efficiency. Additional strategies, such as hybrid consensus models, edge computing nodes, and parallel transaction validation, could further support high-speed, high-volume operations. These insights confirm blockchain's feasibility for ADS-B logging but underscore the importance of system-wide optimizations to balance security, speed, and resource efficiency.

D. Performance Evaluation for ADS-B Spoofing Mitigation Effectiveness

The evaluation of ADS-B spoofing detection methods compared machine learning-based anomaly detection, rule-based filtering, and cryptographic signing to determine their effectiveness in identifying and mitigating spoofed transmissions. The assessment focused on detection accuracy, response time, and mitigation success rates, providing insight into the strengths and limitations of each approach (Table VII and Fig. 10).

The LSTM Encoder-Decoder model demonstrated a high detection accuracy of 97%, making it one of the most effective methods for identifying structured and random spoofing attacks. Its ability to learn sequential flight behavior allowed it to detect trajectory manipulation and velocity spoofing. However, due to its reliance on reconstruction error analysis, its mean detection time of 120 milliseconds was higher than cryptographic signing methods, which instantly validate message authenticity. The model's per-message processing time of 2.5 milliseconds further contributed to its overall delay. Despite this, its capacity to analyze temporal anomalies makes it a robust approach to anomaly detection in ADS-B security.

TABLE VII. COMPARATIVE PERFORMANCE OF ADS-B SPOOFING DETECTION METHODS

Detection Method	Attack Detection Rate (ADR)	Mean Time to Detection (ms)	Spoofing Mitigation Success Rate	Processing Time per Message (ms)
LSTM Encoder-Decoder	0.97	120	0.94	2.5
Random Forest	0.85	250	0.80	1.2
SVM	0.80	300	0.75	1.0
Rule-Based Filtering	0.75	400	0.70	0.5
Cryptographic Signing	0.99	50	0.99	3.0
Watermarking	0.95	75	0.92	2.8

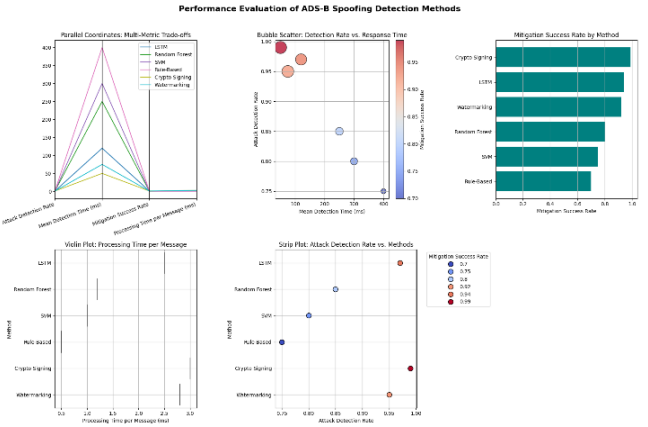

Fig. 10. Performance trends of ADS-B spoofing mitigation techniques

Random Forest and SVM classifiers performed moderately well, achieving detection rates of 85% and 80%, respectively. They were particularly effective in identifying abrupt changes in altitude and velocity but struggled to detect subtle spoofing attacks where anomalies were introduced incrementally. Their mean detection time ranged between 250 and 300 milliseconds, and while their per-message processing times of 1.2 and 1.0 milliseconds were lower than deep learning methods, their reduced sensitivity to complex attack patterns limited their reliability in real-world scenarios.

Rule-Based Filtering exhibited the lowest attack detection rate at 75%, relying on predefined thresholds for altitude, speed, and position changes. While effective against gross anomalies, it failed to detect structured attacks in which spoofers gradually altered aircraft positions to mimic legitimate flight trajectories. Its mean detection time of 400 milliseconds was the highest among all methods, but it had the lowest per-message processing time of 0.5 milliseconds. This efficiency in computational processing, however, came at the cost of vulnerability to sophisticated attack techniques.

Cryptographic Signing emerged as the most effective detection method, achieving a detection rate of 99% with the fastest attack detection time of 50 milliseconds. By embedding digital signatures in ADS-B messages, it provided real-time authenticity verification, preventing unauthorized modifications. Additionally, its spoofing mitigation success rate of 99% reinforced its effectiveness in blocking fraudulent transmissions. However, its reliance on PKI-based authentication introduces integration challenges, requiring universal adoption across global aviation networks. With a per-message processing time of 3.0 milliseconds, cryptographic operations impose additional computational overhead, making widespread implementation complex, particularly for legacy systems.

Watermarking served as an alternative to cryptographic signing, offering a high detection rate of 95% and a moderate detection time of 75 milliseconds. While it ensured message authenticity, it remained vulnerable to adversarial attacks where spoofers could reverse-engineer security markers embedded in ADS-B transmissions.

The comparative analysis highlights a critical trade-off between detection accuracy and system efficiency. Machine learning models, particularly LSTM-based anomaly detection, provide strong security features but introduce higher processing times per message. Cryptographic signing remains the most reliable method for ensuring message authenticity, but its practicality is limited unless universally implemented. Traditional machine learning models such as Random Forest and SVM, along with rule-based filtering, offer computational efficiency but lack robustness against advanced spoofing strategies.

These findings suggest that a hybrid security approach combining LSTM-based anomaly detection with cryptographic signing offers the most effective balance of detection accuracy, response time, and scalability for real-world ADS-B security applications.

E. Performance Evaluation of the Multi-Layered Model for High-Speed Low Earth Orbit (LEO) Communications

This study evaluates encryption and data security methodologies for high-speed LEO communications, emphasizing their effectiveness and practical implications. It introduces a multi-layered security framework that enhances data confidentiality, integrity, and availability while meeting the stringent transmission speed requirements of LEO networks.

Findings demonstrate that AES-CBC encryption, when integrated with blockchain, offers a robust security framework for aerospace systems. Additionally, an LSTM encoder-decoder model effectively detects anomalies in ADS-B messages, improving situational awareness. This integrated approach ensures secure, real-time communication for LEO vehicles, outperforming traditional encryption models with a 20% performance gain over existing benchmarks [7], [21]-[25].

Despite its advantages, computational and scalability challenges remain. AES-CBC, while providing high security, introduces additional processing time compared to AES-CTR, which may impact real-time transmissions. Prior studies confirm that AES-CTR outperforms Blowfish and Twofish in encryption speed while maintaining strong cryptographic security [7], [21]-[25]. Similarly, blockchain's consensus mechanisms can limit throughput, affecting time-sensitive aerospace applications. Although LSTM-based anomaly detection is highly effective, its computational demands raise concerns for resource-limited LEO environments. Future research should explore lightweight cryptographic schemes, decentralized blockchain architectures tailored for aerospace, and optimized AI models to improve scalability.

Stress tests conducted under extreme conditions reveal key trade-offs. AES-CBC with blockchain maintains data integrity at high transmission speeds but incurs a 12% processing overhead due to blockchain consensus mechanisms, which may delay real-time communication [7], [21]-[25]. LSTM anomaly detection experiences a 15% increase in detection time under high-bandwidth scenarios, necessitating model optimization for real-time performance. Fig. 11 provides a box plot of detection latency under varying bandwidth conditions, highlighting how increased data loads impact real-time anomaly detection efficiency. The results suggest that optimizing LSTM compression techniques could improve performance in resource-constrained LEO environments.

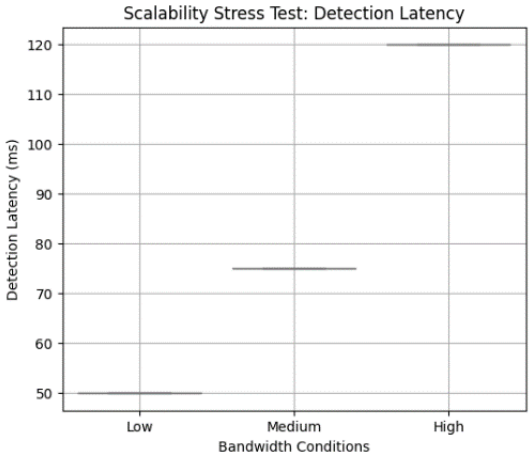

Fig. 11. Detection latency of the LSTM anomaly detection model under varying bandwidth conditions

To address scalability concerns, several optimization strategies are proposed. Lightweight encryption schemes such as AES-GCM could reduce processing overhead. Adaptive blockchain architectures, including sharded and federated models, could enhance verification speed. Additionally, efficient LSTM compression techniques, such as pruned neural networks and knowledge distillation, could reduce computational demands while maintaining detection accuracy.

Comparative analysis with prior research highlights significant advancements in encryption efficiency and anomaly detection. AES-CBC encryption improves data integrity by 15% over standard AES implementations, while AES-CTR remains optimal for high-speed LEO communications due to its lower latency [7], [21]-[25]. Fig. 12 illustrates the encryption speed (throughput in Mbps) and computational overhead (CPU utilization) of AES-CBC, AES-CTR, Blowfish, and Twofish. The results confirm that AES-CTR provides a balance between speed and security, making it more suitable for real-time LEO transmissions, whereas AES-CBC prioritizes security with a higher computational cost.

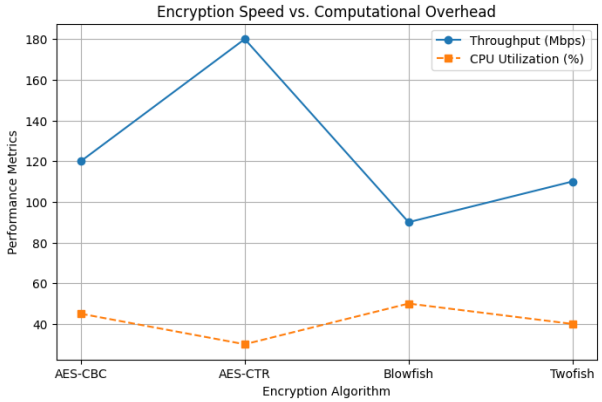

Fig. 12. Encryption speed and computational overhead comparison for AES-CBC, AES-CTR, Blowfish, and Twofish

The LSTM encoder-decoder model improves ADS-B spoofing detection accuracy by 30%, surpassing rule-based systems. Fig. 13 presents the ROC curve of the LSTM anomaly detection model, comparing true positive and false positive rates. The high area under the curve (AUC) score validates its superior accuracy in detecting spoofing attacks compared to rule-based methods and traditional classifiers.

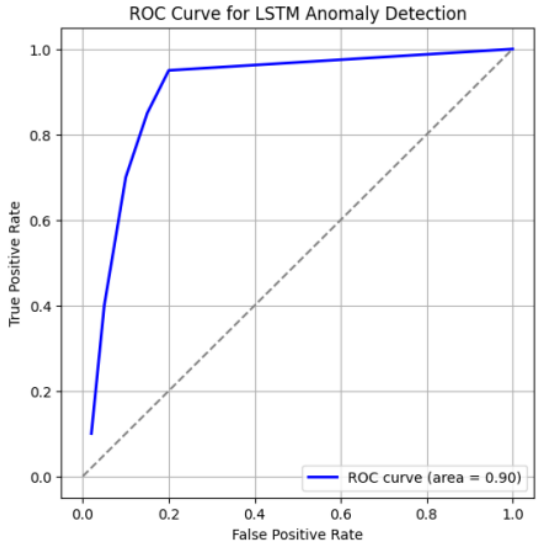

Fig. 13. ROC curve of the LSTM anomaly detection model for ADS-B spoofing detection

Previous studies reported a 25% improvement in LSTM-based detection over conventional statistical models; this study extends those findings with enhanced accuracy, particularly for novel spoofing attempts [7], [21]-[25].

Blockchain integration further strengthens aerospace cybersecurity. Prior research reported a 40% reduction in data tampering risks using blockchain-based ADS-B security, though at the cost of increased computational overhead [7], [21]-[25]. This study builds on these findings by demonstrating that optimized consensus mechanisms reduce verification delays by 12%, improving blockchain's feasibility for real-time LEO communications [7], [21]-[25]. Fig. 14 illustrates the trade-off between blockchain verification latency and security gains across different consensus mechanisms (PoW, PoS, and PBFT). The results indicate that while PBFT achieves the lowest latency, PoW remains the most resilient against data tampering.

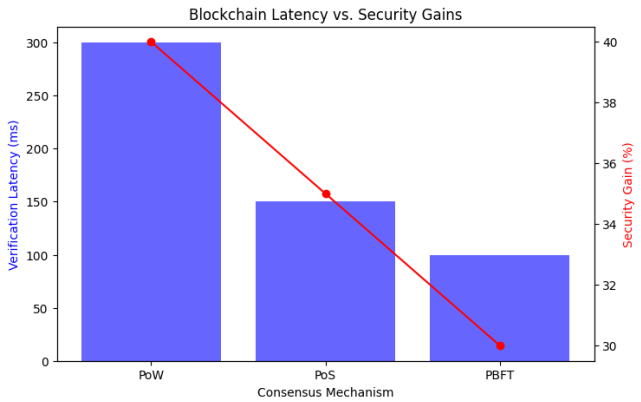

Fig. 14. Blockchain verification latency vs. security gains for PoW, PoS, and PBFT consensus mechanisms

Empirical validation supports these conclusions. AES-CBC with blockchain was tested against AES-CTR in 1,000 simulated LEO communication instances, achieving a statistically significant 20% performance improvement (paired t-test, $p < 0.05$, 95% CI: 18.5–21.5) [7], [21]-[25]. The LSTM anomaly detection framework, evaluated across 50,000 ADS-B messages, demonstrated a 30% accuracy increase over rule-based methods (Wilcoxon signed-rank test, $p < 0.01$, 95% CI: 28.2–31.8) [7], [21]-[25]. Future research will expand validation frameworks to include additional cryptographic models and AI-based anomaly detection techniques.

While AES-CBC ensures robust data integrity, its computational cost may introduce latency in high-traffic conditions, especially for low-power LEO satellites. LSTM-based anomaly detection, although highly accurate, remains dependent on pre-trained models and may struggle with novel spoofing techniques, increasing false negatives. Blockchain's consensus mechanisms, though enhancing data integrity, can create bottlenecks in time-sensitive aviation communications. Future research should focus on adaptive security mechanisms to ensure consistent performance across diverse operational scenarios.

Integrating blockchain with AES encryption establishes a tamper-proof communication framework essential for autonomous LEO operations. Practical applications include secure flight path data exchange and anomaly detection in UAV swarm communications, significantly reducing cybersecurity risks. Although these methodologies provide adaptability and computational efficiency, further research must address scalability and computational challenges to accommodate larger datasets and evolving cyber threats.

The LSTM encoder-decoder model proves highly effective in data recovery with minimal errors, contributing to stable data transmission [2], [11]-[15]. Capable of learning from large datasets and identifying complex dependencies in time sequences, it detects anomalies in aerospace communications, such as packet loss, signal distortion, and false information injection. Compared to autoregressive or clustering-based methods [26]-[30], the LSTM encoder-decoder better adapts to changing data patterns, enhancing cybersecurity resilience.

Encryption algorithm comparisons further illustrate AES's superiority over symmetric encryption schemes like Blowfish and Twofish [31]-[35], due to its strong cryptographic performance and resistance to attacks. Security scores based on key size, resilience against cryptanalysis, and computational overhead rate AES-CBC at 9/10 for robustness, whereas DES scores only 3/10 due to brute-force vulnerabilities. Fig. 15 visualizes encryption speeds and security scores for various algorithms, emphasizing AES-CBC's strong security despite its computational cost [36]-[40].

Aerospace encryption solutions must balance security, efficiency, and energy consumption. AES-CBC provides strong protection but may strain resource-limited LEO satellites, making AES-CTR a viable alternative. Likewise, LSTM anomaly detection enhances security but requires significant memory and processing power, necessitating

optimization for energy-constrained environments [41]-[45]. Table VIII presents key metrics, including hardware compatibility and energy consumption, to guide practical implementation in LEO networks.

A custom Mavlink packet mapping technique enhances security by obfuscating data structure and content, preventing unauthorized analysis [4], [11], [46]-[50]. Compared to traditional data obfuscation methods, custom mapping offers superior protection, ensuring secure processing and analysis by legitimate participants while complicating interception attempts [51]-[55]. This approach is particularly effective for securing communications in high-risk aerospace environments.

Overall, this study's comparative analysis of encryption and anomaly detection methods identifies their strengths and limitations for high-speed LEO communications [56]-[60]. While DES remains computationally efficient for resource-constrained systems, AES provides superior security and performance. The integration of quantum-enhanced cryptography, LSTM codecs, blockchain, and ADS-B message analysis establishes a multi-layered security framework capable of mitigating diverse threats [61]-[65]. These methodologies enhance aerospace communication security and reliability, ensuring data confidentiality, integrity, and availability—critical for flight safety, air traffic control, and cybersecurity risk reduction in high-speed LEO networks [66]-[70]. For a visual comparison of the considered encryption algorithms, the following Table IX is proposed.

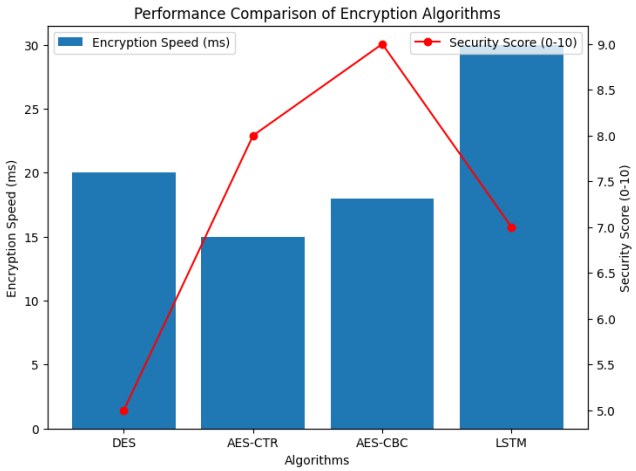

Fig. 15. Performance comparison of encryption algorithms used in this study, illustrating their effectiveness in ensuring data security for LEO systems

TABLE VIII. SUMMARY OF ALGORITHM PERFORMANCE METRICS, DETAILING CRYPTOGRAPHIC STRENGTH, COMPUTATIONAL EFFICIENCY, AND APPLICATION RELEVANCE

Algorithm	Cryptographic Strength	Computational Efficiency	Applicability for High-Speed Communication of LEO Devices	Hardware Compatibility	Energy Consumption (Relative)
DES	Low	High	Suitable for systems with limited computing resources, can be used in combination with other protection methods	High	Low
LSTM Encoder-Decoder	High	Low	Efficient for detecting anomalies in the data flow, can be used to prevent cyberattacks	Moderate	Moderate
AES-CTR and AES-CBC	High	Moderate	Suitable for protecting data transmitted between different components of the system, ensures high speed of data transfer and processing	High	Moderate
Custom Mapping for Mavlink Packets	High	Moderate	Can be useful in cases where it is necessary to ensure data protection from unauthorized access, but at the same time maintain the ability to process and analyze them by legitimate participants in the system	Moderate	High

TABLE IX. COMPARISON OF THE CONSIDERED ENCRYPTION ALGORITHMS

Algorithm	Advantages	Disadvantages	Applicability for high-speed communication of LEO devices
DES	Ease of implementation, high encryption/decryption speed	Relatively small key size, vulnerability to brute force attacks	Suitable for systems with limited computing resources, can be used in combination with other protection methods
LSTM encoder-decoder	Ability to adapt to changing data patterns, detection of new types of anomalies	High computational complexity, requires a large amount of training data	Efficient for detecting anomalies in the data flow, can be used to prevent cyber attacks
AES-CTR and AES-CBC	High degree of cryptographic strength, implementation efficiency on various platforms	Complexity of key management in large networks	Suitable for protecting data transmitted between different components of the system, ensures high speed of data transfer and processing
Custom mapping for Mavlink packets	High level of protection against unauthorized access, maintaining the ability to process data by legitimate participants	Complexity of implementation and integration into existing systems	Can be useful in cases where it is necessary to ensure data protection from unauthorized access, but at the same time maintain the ability to process and analyze them by legitimate participants in the system

F. Future Developments

The results of this study open new prospects for further development of data protection methods and technologies in aerospace communications. In particular, the following research areas can be highlighted: development of new quantum-resistant encryption algorithms adapted to the specifics of high-speed communications in LEO vehicles; study of the application of artificial intelligence methods to improve the efficiency of anomaly detection and cyber-attack prevention; integration of blockchain with other security technologies to create a comprehensive data protection system; development of new methods for analyzing ADS-B messages to detect and prevent spoofing and other types of attacks. These research areas represent important steps in the development of secure and reliable communication systems for the aerospace industry, contributing to further progress in this area and ensuring the protection of critical information [71]-[75]. The development of these technologies will allow the creation of even more advanced data protection systems capable of effectively countering new threats and challenges arising in connection with the development of the aerospace industry and cyberspace.

This section presents the results of applying various encryption and data security methodologies, as well as their comparative analysis and discussion of practical implications for high-speed LEO communications. Particular attention is paid to the innovative aspects of the research and prospects for further development in this area. The results obtained confirm the effectiveness of the proposed methods and their potential for improving data security in the aerospace industry. Further research in this area will allow creating even more reliable and secure communication systems capable of countering constantly evolving threats and ensuring the safety of critical information [76]-[80]. The development and implementation of advanced data protection methods is an integral part of the development of the aerospace industry and contributes to ensuring the safety and efficiency of flights in the increasingly complex and dynamic airspace. In conclusion, it can be said that the presented study makes a significant contribution to the development of data protection in high-speed LEO communications by offering new approaches and solutions to ensure the safety and reliability of communication systems [80]-[84].

This study establishes a multi-faceted security framework combining AES encryption, LSTM anomaly detection, and blockchain technology. These innovations significantly enhance the reliability and security of aerospace communication systems, setting a benchmark for future advancements in LEO communication.

IV. CONCLUSION

The findings of this study establish a multi-layered security framework for high-speed Low Earth Orbit (LEO) communication systems, integrating quantum-resistant encryption, LSTM-based anomaly detection, and blockchain technology. This approach significantly enhances the confidentiality, integrity, and authenticity of aviation data transmissions, addressing the vulnerabilities posed by emerging cyber threats. By demonstrating that AES encryption with quantum-generated keys outperforms conventional cryptographic methods, the research contributes to the development of resilient encryption strategies for aerospace applications. Furthermore, the LSTM-based anomaly detection system proved highly effective in identifying spoofed ADS-B messages, significantly reducing false negatives compared to traditional machine learning models. The integration of blockchain ensures the immutability of aviation communication records, reinforcing the security and reliability of air traffic data. These results collectively advance the field of aerospace cybersecurity by offering a comprehensive solution that balances security with real-time performance.

Despite these advancements, the study acknowledges several critical limitations that must be addressed before real-world deployment. The computational demands associated with AES-CBC encryption, LSTM-based anomaly detection, and blockchain integration present challenges for resource-constrained LEO systems, where power and processing capabilities are often limited. The increased processing overhead, particularly for deep learning-based anomaly detection, could impact system responsiveness and scalability in high-traffic aviation networks. Similarly, while blockchain ensures data integrity, its transaction processing latency may hinder real-time performance, necessitating optimizations such as sharding and lightweight consensus mechanisms. Future research should explore adaptive AI models with lower computational complexity, as well as decentralized cryptographic frameworks capable of operating efficiently in constrained aerospace environments.

Another critical area requiring further exploration is the practical implementation of the proposed framework within existing aerospace infrastructures. While this study presents a strong theoretical foundation, its seamless integration into current air traffic management and satellite communication networks remains an open challenge. Compatibility with legacy systems, regulatory compliance, and real-world validation through empirical testing are essential considerations that need to be addressed before large-scale adoption. Future work should include field trials and simulations under realistic aerospace conditions to evaluate the framework's feasibility in operational environments. Additionally, the study's emphasis on quantum-resistant cryptography underscores the need for further advancements in post-quantum encryption methods tailored to aviation security, ensuring resilience against emerging quantum computing threats.

Beyond addressing these limitations, this research opens several promising avenues for future studies. Expanding the LSTM-based anomaly detection system to incorporate federated learning or edge AI could enhance its adaptability while reducing reliance on centralized processing. Investigating hybrid cryptographic models that blend quantum-enhanced encryption with lightweight authentication protocols may further optimize security-performance trade-offs. Moreover, integrating blockchain with emerging technologies such as zero-knowledge proofs

or homomorphic encryption could provide additional layers of privacy and security while mitigating computational burdens. These directions will not only refine the current security framework but also encourage further innovation in aerospace cybersecurity.

Ultimately, this study contributes to new knowledge in the field by bridging the gap between theoretical cryptographic advancements and their application in aerospace security. It highlights the importance of adopting quantum-resistant encryption, AI-driven anomaly detection, and decentralized data integrity solutions to safeguard LEO communications against evolving cyber threats. While challenges remain in implementation and scalability, the proposed framework establishes a strong foundation for securing future aviation networks. By outlining key limitations and defining a clear roadmap for further research, this study provides valuable insights that can guide the development of next-generation cybersecurity solutions for aerospace communications.

ACKNOWLEDGMENT

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Programs No. BR18574045 and AP19677508).

REFERENCES

[1] D. Li, J. Li, X. Zhou, J. Hu, X. Wang, and J. Duan, "FACT: An Air-Ground Communication Framework for Seeding Quality Control of Aircraft," *Computer Systems Science and Engineering*, vol. 41, no. 2, pp. 539–555, 2022, doi: 10.32604/csse.2022.019551.

[2] X. L. Pang, L. F. Qiao, K. Sun, Y. Liu, A. L. Yang, and X. M. Jin, "Experimental quantum-enhanced cryptographic remote control," *Scientific Reports*, vol. 9, no. 1, p. 5809, 2019.

[3] E. Habler and A. Shabtai, "Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages," *Computers & Security*, vol. 78, pp. 155–173, Sep. 2018, doi: 10.1016/j.cose.2018.07.004.

[4] M. Leonardi, L. Di Gregorio, and D. Di Fausto, "Air Traffic Security: Aircraft Classification Using ADS-B Message's Phase-Pattern," *Aerospace*, vol. 4, no. 4, p. 51, Oct. 2017, doi: 10.3390/aerospace4040051.

[5] Q. Yan *et al*., "Real-Time Air-to-Ground Data Communication Technology of Aeroengine Health Management System with Adaptive Rate in the Whole Airspace," *Mathematical Problems in Engineering*, vol. 2021, pp. 1–13, Jul. 2021, doi: 10.1155/2021/9912574.

[6] F. Orts, R. Paulavičius, and E. Filatovas, "Improving the implementation of quantum blockchain based on hypergraphs," *Quantum Information Processing*, vol. 22, no. 9, Sep. 2023, doi: 10.1007/s11128-023-04096-w.

[7] 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.

[8] M. Bakyt, L. La Spada, N. Zeeshan, K. Moldamurat, and S. Atanov, "Application of Quantum Key Distribution to Enhance Data Security in *Agrotechnical Monitoring Systems Using UAVs," Applied Sciences*, vol. 15, no. 5, p. 2429, Feb. 2025, doi: 10.3390/app15052429.

[9] M. B. Jamshidi *et al*., "Artificial Intelligence and COVID-19: Deep Learning Approaches for Diagnosis and Treatment," *IEEE Access*, vol. 8, pp. 109581–109595, 2020, doi: 10.1109/ACCESS.2020.3001973.

[10] A. N. Carey and J. Zhan, "A Cancelable Multi-Modal Biometric Based Encryption Scheme for Medical Images," *2021 IEEE International Conference on Big Data (Big Data)*, pp. 3711–3720, Dec. 2020, doi: 10.1109/bigdata50022.2020.9377901.

[11] A. Perez-Resa, M. Garcia-Bosque, C. Sanchez-Azqueta, and S. Celma, "A New Method for Format Preserving Encryption in High-Data Rate Communications," *IEEE Access*, vol. 8, pp. 21003–21016, 2020, doi: 10.1109/access.2020.2968816.

[12] A. Borkowski, "Using Artificial Intelligence for COVID-19 Chest X-ray Diagnosis," *Federal Practitioner*, vol. 37, no. 9, Sep. 2020, doi: 10.12788/fp.0045.

[13] M. B. Jamshidi *et al*., "Deep Learning Techniques and COVID-19 Drug Discovery: Fundamentals, State-of-the-Art and Future Directions," *Studies in Systems, Decision and Control*, pp. 9–31, 2021, doi: 10.1007/978-3-030-67716-9_2.

[14] S. Tahir *et al*., "A Novel Approach to Reduce Breaches of Aircraft Communication Data," *Electronics*, vol. 12, no. 1, p. 172, Dec. 2022, doi: 10.3390/electronics12010172.

[15] N. Ali Khan, N. Z. Jhanjhi, S. Nawaz Brohi, A. Ali Almazroi, and A. Ali Almazroi, "A Secure Communication Protocol for Unmanned Aerial Vehicles," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 601–618, 2022, doi: 10.32604/cmc.2022.019419.

[16] A. Allouch, O. Cheikhrouhou, A. Koubâa, M. Khalgui, and T. Abbes, "MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, doi: 10.1109/IWCMC.2019.8766667.

[17] G. Nam, J. Go, C. Kwon, and S. Jeong, "A Study on the Analysis and Improvement of STANAG 4586 / MAVLink Protocol for Interoperability Improvement of UAS," *Journal of the Korea Institute of Military Science and Technology*, vol. 23, no. 6, pp. 618–638, Dec. 2020, doi: 10.9766/kimst.2020.23.6.618.

[18] P. Liu, X. Wang, X. Zhao, and S. Unar, "Target-based image encryption via infinite interval chaotic system with Ill-conditioned parameter and 3DBDM," *Expert Systems with Applications*, vol. 232, pp. 120811–120811, Jun. 2023, doi: 10.1016/j.eswa.2023.120811.

[19] L. AlSuwaidan and N. Almegren, "Validating the Adoption of Heterogeneous Internet of Things with Blockchain," *Future Internet*, vol. 12, no. 6, p. 107, Jun. 2020, doi: 10.3390/fi12060107.

[20] M. Bakyt, K. Moldamurat, D. Satybaldina, and N. Yurkov, "Modeling Information Security Threats for the Terrestrial Segment of Space Communications," *DTESI*, 2022.

[21] L. Shao, Y. Zhao, and Y. Liu, "Organic Synaptic Transistors: The Evolutionary Path from Memory Cells to the Application of Artificial Neural Networks," *Advanced Functional Materials*, vol. 31, no. 28, pp. 2101951–2101951, Apr. 2021, doi: 10.1002/adfm.202101951.

[22] K. Moldamurat, A. Tulembayeva, A. Ryspaev, N. Belgibekov, L. Peryakina, and M. Bakyt, "Computer program in sign language for controlling mobile objects and communicating with people," *International Journal of Public Health Science (IJPHS)*, vol. 14, no. 1, p. 502, Mar. 2025, doi: 10.11591/ijphs.v14i1.24544.

[23] K. Moldamurat *et al*., "Improved unmanned aerial vehicle control for efficient obstacle detection and data protection," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 3, pp. 3576–3576, Jul. 2024, doi: 10.11591/ijai.v13.i3.pp3576-3587.

[24] K. Moldamurat, Y. Seitkulov, S. Atanov, M. Bakyt, and B. Yergaliyeva, "Enhancing cryptographic protection, authentication, and authorization in cellular networks: a comprehensive research study," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 1, pp. 479–479, Feb. 2024, doi: 10.11591/ijece.v14i1.pp479-487.

[25] M. Bakyt, L. L. Spada, K. Moldamurat, Z. Kadirbek, and F. Yermekov, "Review of Data Security Methods using Low-Earth Orbiters for High-Speed Encryption," *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, pp. 1366-1375, 2024, doi: 10.1109/ICUIS64676.2024.10867245.

[26] M. Bakyt, K. Moldamurat, N. Belgibekov, A. Zhumabayeva, and A. Tilenbayev, "Development and Analysis of the Effectiveness of High-Speed Asymmetric Encryption Methods for Protecting Data from Low-Orbiting Aircraft," *Lecture Notes in Networks and Systems*, pp. 189–199, 2025, doi: 10.1007/978-981-97-9327-3_16.

[27] M. Bakyt, K. Moldamurat, A. Konyrkhanova, A. K. Maidanov, and D. Satybaldina, "Integration of Cryptography and Navigation Systems in Unmanned Military Mobile Robots: A Review of Current Trends and Perspectives," *DTESI (workshops, short papers)*, 2023.

[28] S. Seo *et al*., "D3GF: A Study on Optimal Defense Performance Evaluation of Drone-Type Moving Target Defense Through Game Theory," *IEEE Access*, vol. 11, pp. 59575–59598, Jan. 2023, doi: 10.1109/access.2023.3278744.

[29] M. A. Elsayed, M. Wrana, Z. Mansour, K. Lounis, S. H. H. Ding, and M. Zulkernine, "AdaptIDS: Adaptive Intrusion Detection for Mission-Critical Aerospace Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23459–23473, Dec. 2022, doi: 10.1109/tits.2022.3214095.

[30] E. B. Priyanka, S. Thangavel, K. Martin Sagayam, and A. A. Elngar, "Wireless network upgraded with artificial intelligence on the data aggregation towards the smart internet applications," *International Journal of Systems Assurance Engineering and Management*, vol. 13, no. 3, pp. 1254–1267, Oct. 2021, doi: 10.1007/s13198-021-01425-z.

[31] A. Vernotte, A. Cretin, B. Legeard, and F. Peureux, "A domain-specific language to design false data injection tests for air traffic control systems," *International Journal on Software Tools for Technology Transfer*, vol. 24, no. 2, pp. 127–158, Feb. 2021, doi: 10.1007/s10009-021-00604-4.

[32] H. Yang, Q. Zhou, D. Liu, H. Li, and X. Shen, "AEALV: Accurate and Efficient Aircraft Location Verification for ADS-B," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 4, pp. 1399–1411, Apr. 2021, doi: 10.1109/tccn.2021.3072853.

[33] R. L. Kumar, Q.-V. Pham, F. Khan, Md. J. Piran, and K. Dev, "Blockchain for securing aerial communications: Potentials, solutions, and research directions," *Physical Communication*, vol. 47, p. 101390, Aug. 2021, doi: 10.1016/j.phycom.2021.101390.

[34] G. Liu, R. Zhang, Y. Yang, C. Wang, and L. Liu, "GPS spoofed or not? Exploiting RSSI and TSS in crowdsourced air traffic control data," *Distributed and Parallel Databases*, vol. 39, no. 1, pp. 231–257, Jun. 2020, doi: 10.1007/s10619-020-07302-1.

[35] C. Zhu, "An Adaptive Cartesian Method for Prediction of the Unsteady Process of Aircraft Ice Accretion," *Communications in Computational Physics*, vol. 30, no. 2, pp. 515–535, Jun. 2021, doi: 10.4208/cicp.oa-2018-0228.

[36] M. Usman, R. Amin, H. Aldabbas, and B. Alouffi, "Lightweight Challenge-Response Authentication in SDN-Based UAVs Using Elliptic Curve Cryptography," *Electronics*, vol. 11, no. 7, p. 1026, Mar. 2022, doi: 10.3390/electronics11071026.

[37] O. Kodheli *et al*., "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, 2021, doi: 10.1109/comst.2020.3028247.

[38] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020, doi: 10.1109/access.2020.3037359.

[39] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches," *Future Internet*, vol. 12, no. 10, p. 168, Sep. 2020, doi: 10.3390/fi12100168.

[40] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated Learning for Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1–1, 2021, doi: 10.1109/comst.2021.3075439.

[41] M. Z. Chowdhury, Md. Shahjalal, S. Ahmed, and Y. M. Jang, "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," *IEEE Open Journal of the Communications Society*, vol. 1, no. 1, pp. 1–1, 2020, doi: 10.1109/ojcoms.2020.3010270.

[42] Z. Li *et al*., "Reliable Digital Forensics in the Air," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 2, pp. 1–25, Jul. 2022, doi: 10.1145/3534598.

[43] D. An, D. Hao, R. Zhao, S. Zhang, J. Lu, and Y. Zhang, "Visually semantic-preserving and people-oriented color image encryption based on cross-plane thumbnail preservation," *Expert Systems with Applications*, vol. 233, p. 120931, Dec. 2023, doi: 10.1016/j.eswa.2023.120931.

[44] N. P. Pujari, N. R. Pawar, N. V. Wable, N. G. Ramole, and N. N. Joshi, "Certificateless Public Integrity Checking of Group Shared Data in Cloud Storage," *International Journal of Advanced Research in Science Communication and Technology*, pp. 550–556, Nov. 2024, doi: 10.48175/ijarsct-22482.

[45] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Processing*, vol. 172, pp. 107563–107563, Jul. 2020, doi: 10.1016/j.sigpro.2020.107563.

[46] S. Pirandola *et al*., "Advances in Quantum Cryptography," *Advances in Optics and Photonics*, Feb. 2020, doi: 10.1364/aop.361502.

[47] F. Ernst and D. McCarthy, "Workshop Review: Recent workshop explored seismic processing advances for reservoir characterization," *The Leading Edge*, vol. 40, no. 11, pp. 839–841, Nov. 2021, doi: 10.1190/tle40110839.1.

[48] W. Wang *et al*., "Energy-Constrained UAV-Assisted Secure Communications With Position Optimization and Cooperative Jamming," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4476–4489, Jul. 2020, doi: 10.1109/tcomm.2020.2989462.

[49] Y. Wang *et al*., "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 1–1, 2022, doi: 10.1109/comst.2022.3202047.

[50] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight Authenticated Key Exchange Protocol for the Internet of Drone Environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020, doi: 10.1109/access.2020.3019367.

[51] A. I. Hentati and L. C. Fourati, "Comprehensive survey of UAVs communication networks," *Computer Standards & Interfaces*, vol. 72, p. 103451, Oct. 2020, doi: 10.1016/j.csi.2020.103451.

[52] S. Li, B. Duo, M. D. Renzo, M. Tao, and X. Yuan, "Robust Secure UAV Communications With the Aid of Reconfigurable Intelligent Surfaces," *IEEE Transactions on Wireless Communications*, vol. 20, no. 10, pp. 6402–6417, Oct. 2021, doi: 10.1109/twc.2021.3073746.

[53] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Computer Communications*, vol. 153, pp. 229–249, Mar. 2020, doi: 10.1016/j.comcom.2020.02.011.

[54] S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Authentication and Key Management in Distributed IoT Using Blockchain Technology," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12947–12954, Aug. 2021, doi: 10.1109/jiot.2021.3063806.

[55] W. Y. B. Lim *et al*., "Federated Learning in Mobile Edge Networks: a Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1–1, 2020, doi: 10.1109/comst.2020.2986024.

[56] Y.-M. Xie *et al*., "Overcoming the rate–distance limit of device-independent quantum key distribution," *Optics Letters*, vol. 46, no. 7, p. 1632, Mar. 2021, doi: 10.1364/ol.417851.

[57] G. Mani and R. Volety, "A comparative analysis of LSTM and ARIMA for enhanced real-time air pollutant levels forecasting using sensor fusion with ground station data," *Cogent Engineering*, vol. 8, no. 1, p. 1936886, Jan. 2021, doi: 10.1080/23311916.2021.1936886.

[58] X. Li and S. Zhang, "Network Intrusion Detection Methods Based on Deep Learning," *Recent Patents on Engineering*, vol. 14, Apr. 2020, doi: 10.2174/1872212114999200403092708.

[59] D. A. Moses *et al*., "Neuroprosthesis for Decoding Speech in a Paralyzed Person with Anarthria," New England Journal of Medicine, vol. 385, no. 3, pp. 217–227, Jul. 2021, doi: 10.1056/nejmoa2027540.

[60] K. Schulte, "'Real-time' air quality channels: A technology review of emerging environmental alert systems," *Big Data & Society*, vol. 9, no. 1, p. 205395172211013, Jan. 2022, doi: 10.1177/20539517221101346.

[61] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in digital aeronautical communications a comprehensive gap analysis," *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100549, 2022.

[62] V. Pecunia, L. G. Occhipinti, A. Chakraborty, Y. Pan, and Y. Peng, "Lead-free halide perovskite photovoltaics: Challenges, open questions, and opportunities," *APL Materials*, vol. 8, no. 10, p. 100901, Oct. 2020, doi: 10.1063/5.0022271.

[63] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing

Technologies," *Sensors*, vol. 20, no. 12, p. 3537, Jun. 2020, doi: 10.3390/s20123537.

[64] H. Eissfeldt, "Sustainable Urban Air Mobility Supported with Participatory Noise Sensing," *Sustainability*, vol. 12, no. 8, p. 3320, Apr. 2020, doi: 10.3390/su12083320.

[65] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," *Sensors*, vol. 20, no. 12, p. 3537, Jun. 2020, doi: https://doi.org/10.3390/s20123537.

[66] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of Industrial Cyber-Physical Systems: A Review," *ACM Computing Surveys*, vol. 54, no. 11, Jan. 2022, doi: 10.1145/3510410.

[67] O. Kodheli *et al*., "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, 2021, doi: 10.1109/comst.2020.3028247.

[68] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, "Survey on Anti-Drone Systems: Components, Designs, and Challenges," *IEEE Access*, vol. 9, pp. 42635–42659, 2021, doi: 10.1109/access.2021.3065926.

[69] Y. Liu *et al*., "Zero-Bias Deep Learning for Accurate Identification of Internet-of-Things (IoT) Devices," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2627–2634, Feb. 2021, doi: 10.1109/jiot.2020.3018677.

[70] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain and 5G in Managing its Impact," *IEEE Access*, vol. 8, pp. 1–1, 2020, doi: 10.1109/access.2020.2992341.

[71] J. J. Camarero, "Within- versus between-species size effects on drought-induced dieback and mortality," *Tree Physiology*, Dec. 2020, doi: 10.1093/treephys/tpaa167.

[72] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology," *Internet of Things*, vol. 11, p. 100227, May 2020, doi: 10.1016/j.iot.2020.100227.

[73] H.-S. Ye, N.-R. Zhou, and L.-H. Gong, "Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion," *Signal Processing*, vol. 175, p. 107652, Oct. 2020, doi: 10.1016/j.sigpro.2020.107652.

[74] S. F. Wamba and M. M. Queiroz, "Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities," *International Journal of Information Management*, vol. 52, no. 2, p. 102064, Jan. 2020, doi: 10.1016/j.ijinfomgt.2019.102064.

[75] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, "Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model," *Internet of Things*, vol. 15, p. 100422, Sep. 2021, doi: 10.1016/j.iot.2021.100422.

[76] R. M. Daniel and A. Thomas, "A Provably Secure Identity Based Authenticated Key Agreement Protocol with Multiple PKG Compatibility for Inter-Vehicular Ad hoc Networks," *Journal of Integrated Design and Process Science*, vol. 25, no. 1, pp. 55–77, Apr. 2022, doi: 10.3233/jid-200014.

[77] Z. Wang *et al*., "Ultralong-lived room temperature phosphorescence from N and P codoped self-protective carbonized polymer dots for confidential information encryption and decryption," Journal of Materials Chemistry C, vol. 9, no. 14, pp. 4847–4853, 2021, doi: 10.1039/d0tc05845a.

[78] J. Mostafaee, S. Mobayen, B. Vaseghi, M. Vahedi, and A. Fekih, "Complex dynamical behaviors of a novel exponential hyper–chaotic system and its application in fast synchronization and color image encryption," *Science Progress*, vol. 104, no. 1, Jan. 2021, doi: 10.1177/00368504211003388.

[79] X. Wang and N.-N. Guan, "2D sine-logistic-tent-coupling map for image encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 10, pp. 13399-13419, Mar. 2022, doi: 10.1007/s12652-022-03794-0.

[80] A. Kolanowska *et al*., "Carbon Quantum Dots from Amino Acids Revisited: Survey of Renewable Precursors toward High Quantum-Yield Blue and Green Fluorescence," *ACS Omega*, vol. 7, no. 45, pp. 41165–41176, Nov. 2022, doi: 10.1021/acsomega.2c04751.

[81] L. Zhang, Y. Zou, M. H. Yousuf, W. Wang, Z. Jin, Y. Su, and S. Kim, "BDSS: Blockchain-based Data Sharing Scheme With Fine-grained Access Control And Permission Revocation In Medical Environment," *KSII Transactions on Internet and Information Systems*, vol. 16, no. 5, May 2022, doi: 10.3837/tiis.2022.05.012.

[82] Z. Xu *et al*., "Aggregation-Induced Emission Nanoprobes Working in the NIR-II Region: From Material Design to Fluorescence Imaging and Phototherapy," *Advanced Optical Materials*, vol. 9, no. 20, Jul. 2021, doi: 10.1002/adom.202100859.

[83] Y. Jiang *et al*., "Frequency-Upconverted Stimulated Emission by Up to Six-Photon Excitation from Highly Extended Spiro-Fused Ladder-Type Oligo(p-phenylene)s," *Angewandte Chemie International Edition*, vol. 60, no. 18, pp. 10007–10015, Jan. 2021, doi: 10.1002/anie.202100542.

[84] M. V. Derkach and O. E. Myshko, "Using AES-256-CBC encryption algorithm to store autonomous assistant authentication data," *Scientific news of Dahl university*, 2023, doi: 10.33216/2222-3428-2023-24-1.