JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(4), DECEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Securing the Skies: Blockchain Technology for Cyber Threat Mitigation in Aviation Communication Networks

[1]Augustine Omokhogie Evans, [2]Daniel Aliu, [3]Terhemen Emmanuel Agov
[1]*NeoCloud Technologies, Gwarinpa-Abuja Nigeria*
[2]*Department of Computer Engineering, Edo State University Uzairue, Nigeria*
[3]*Faculty of Air Engineering, Air Force Institute of Technology, Kaduna Nigeria*

ABSTRACT
The aviation communication network is a critical infrastructure that ensures the safety and efficiency of air travel. However, the increasing reliance on digital communication systems has exposed these networks to significant vulnerabilities, including cyber threats and data manipulation attacks. This paper explores the inherent risks associated with traditional aviation communication systems, which often lack robust security measures and are susceptible to unauthorized access and technical failures. It highlights the potential of blockchain technology as a transformative solution to enhance the security, transparency and integrity of aviation communication networks. By leveraging advanced cryptographic techniques and decentralized architecture, blockchain can provide a secure framework that mitigates cyber threats and fosters trust among stakeholders. The integration of blockchain into aviation communication systems promises to revolutionize operational processes, ensuring that critical data remains accurate and reliable, ultimately safeguarding the skies against emerging risks.

ARTICLE INFO
Article History
Received: May, 2024
Received in revised form: July, 2024
Accepted: September, 2024
Published online: December, 2024

KEYWORDS
Aviation communication network, Blockchain, cyber-attacks, Vulnerability, Air transport

INTRODUCTION

Aviation communication network infrastructure has evolved through various stages to meet the continuous soaring demand for an effective and efficient navigation system. Recent advancements in digital communication systems, based on Internet Protocol, have given rise to the use of IP as the de facto standard for the next generation of aeronautical telecommunication networks (Sampigethaya & Poovendran, 2013). Communication on aviation networks can involve a strategic and predictable type of message exchange, for example, routine queries between the aircraft and air traffic control, or an unpredictable type where aircraft and operators receive unsolicited notifications (Nguyen *et al*., 2019). These systems, being used by pilots for the management and monitoring of aircraft systems and air traffic control systems, have both brought enormous economic and operational benefits for airlines and allowed passengers and freight to reach their destinations faster (Kistan *et al*., 2013). However, these changes in technology have initiated a number of vulnerabilities that have become a major cause of global concern for civil aviation. Many incidents have been reported in the recent past where the primary mechanism was technology and specifically Internet-based attacks (Li & Liu 2021). One of the most traditionally secure methods of international travel—air transport—is facing challenges in recovering from the negative effects of these incidents (Woltjer *et al*., 2022). Acknowledging these technological dependencies, the regulatory bodies have been keen to enforce compliance with various safety and security standards. For instance, beginning in 2007, there was a growing focus on the need to secure information technology and communication infrastructure, urging the research community to develop technologies to assist in combating unauthorized access, fraud, and other potential threats to businesses and private

Corresponding author: Augustine Omokhogie Evans
augustineevans75@gmail.com
NeoCloud Technologies, Gwarimpa, Abuja, Nigeria.

individuals. This increased compliance demand, enforced by some of the world's most successful civil aviation authorities, comes from the recognition that an IT infrastructure vulnerable to cyber-attacks can result in significant economic, operational, and reputational loss both for the business and the customers involved. In light of these evolving challenges, the aviation industry finds itself at a critical juncture, where ensuring the security and resilience of its communication networks is paramount (Momoh *et al*., 2021). As cyber threats continue to evolve alongside advancements in technology, the need for innovative and robust solutions becomes ever more pressing (Chinedu *et al*., 2020). This underscores the importance of exploring transformative technologies, such as blockchain, which offer the potential to enhance the integrity, transparency, and security of aviation communication systems, ultimately safeguarding the skies against emerging cyber risks.

AVIATION COMMUNICATION NETWORKS: VULNERABILITIES AND THREATS

Modern aviation deeply integrates different heterogeneous communication systems to fulfill the high demands of en-route and terminal communication services for both safety and operational aspects of air traffic management (Chen *et al*., 2024). However, these systems and the data they broadcast and receive are valuable targets for adversaries, leading to increased vulnerabilities and threats to aviation communication networks. As a result, leaks or forgeries of aeronautical communication messages can cause false information to be spread across all airspace domains, leading to severe consequences for both safety and security. More specific threats to the communication system might come from, but are not limited to, cyber-attacks or technical failures of system parts. Typical communication protocols and security mechanisms are not suited for adverse environments, and agreement and adherence of all involved stakeholders are critical to creating reliable, secure, or survivable systems. Safety vulnerabilities and threats concerning communication and navigation in aviation were systematically studied (Ferrão *et al*., 2022). Failures in communication and navigation are the top-ranking issues in civil aviation and can manifest themselves in different forms. They can be either cyber-attacks where third-party interference affects communications and navigation signals, posing threats to the safety or security of aircraft (Momoh *et al*., 2021; Ukwandu *et al*., 2022). There are also technical failures within the transmission channels, or even errors due to old data or non-synchronized data retrieved from or to control center personnel by aircraft crews interacting with Air Traffic Management. Furthermore, there are security threats due to unauthorized access to the control center. Different aspects should be taken into account, starting with the poor performance of traditional aviation communication and navigation systems, which are overly dependent on specific vendors, thus posing monopolistic dependencies to various aviation regulation stakeholders. A typical conceptual view of aviation communication network is depicted in Figure 1. The aviation communication network is structured into several layers to manage different types of communication needs effectively, each layer involves different protocols, frequencies, and technologies that work together to create a reliable network, interconnectivity exposes the network to cyber threats, necessitating robust security measures.

.

Corresponding author: Augustine Omokhogie Evans
augustineevans75@gmail.com
NeoCloud Technologies, Gwarimpa, Abuja, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(4), DECEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

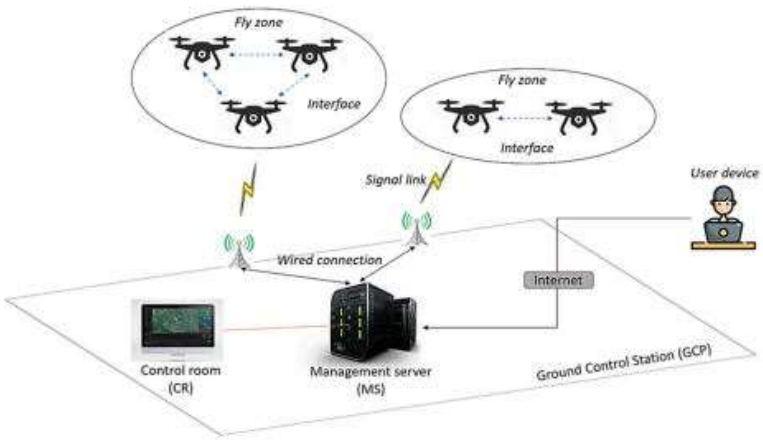

Figure 1: Conceptual view of Aviation Communication Network

TRADITIONAL COMMUNICATION SYSTEMS

When it comes to aviation, the current infrastructure is run over mainly three important communication systems: Aeronautical Telecommunication Network, Very High-Frequency Data Link, Future Aeronautical Communication, and Automated Dependent Surveillance-Broadcast. The communication systems work with the Internet Protocol architecture and have protocols for each layer of the OSI network model (Umoh *et al*., 2019). They primarily use different protocols, and all these communication systems follow certain defined protocols and standards, and any new innovation has to integrate with these standard protocols. Integrating any new innovative technology with the protocols is no small task. One of the major challenges is the interoperability of systems.

Another limitation seen in traditional communication systems is security. Since all these communication systems were established several years ago, the communication techniques have the same lag for security measures. One system uses tunneling protocol for secure communication, but some vulnerabilities have been identified with the protocol, and experts feel it can easily be compromised. Also, the communication in this system does not have end-to-end encryption. There is no end-to-end encryption between pilots and air traffic controllers. Both communication systems face problems with a lack of security measures. In line with this, several threats have also been identified (Daniel & Momoh, 2021). There are several issues with these traditional communication systems. The main issue is that end-to-end security measures are missing. Hackers can easily eavesdrop or tamper with network-intercepted data packages. Due to the missing security measures in these aviation systems, many historical data breaches have been reported. So using only these communication systems can cause chaos and even worse conditions for the aviation industry.

Aerial communication devices are susceptible to physical abduction, damage, or loss. Consequently, ensuring the security of aerial communication networks is a critical concern. Blockchain technology brings unique features that can revolutionize the security framework of aviation communication networks by addressing existing vulnerabilities and mitigating cyber threats. Blockchain secures information using cryptographic algorithms such as public-key encryption and hash functions. It offers the potential to enhance the reliability of stored data while improving the transparency and security of aerial communication networks.

Corresponding author: Augustine Omokhogie Evans
augustineevans75@gmail.com
NeoCloud Technologies, Gwarimpa, Abuja, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(4), DECEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

KEY CHARACTERISTIC OF BLOCKCHAIN TECHNOLOGY

When discussing the application of Blockchain to aviation communication network, there are some key features it possesses that make it suitable. Figure 2 shows the key characteristics of blockchain technology.

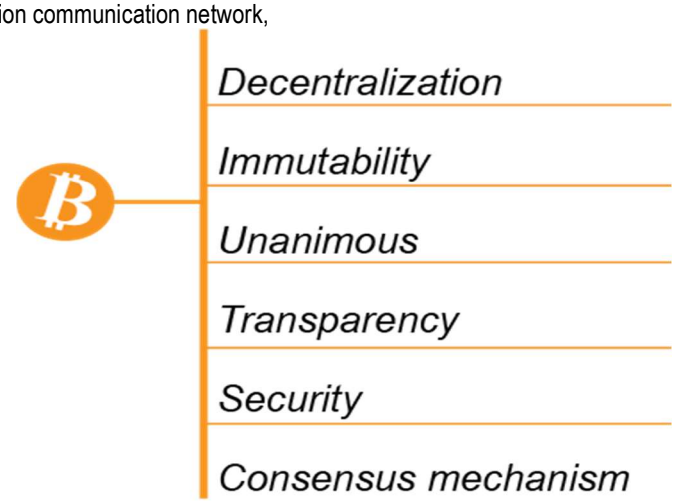

Figure 2: The key characteristics of Blockchain technology

Decentralization

Decentralization refers to the distribution of data and control across a network of nodes, rather than relying on a centralized authority. In the context of aviation communication networks, decentralization can help prevent single points of failure and reduce the risk of cyber-attacks. By distributing data and control across a network of nodes, blockchain technology can ensure that aviation communication networks remain operational even if one or more nodes are compromised.

Immutability

Immutability refers to the ability of blockchain technology to create an immutable record of transactions or data. In the context of aviation communication networks, immutability can help ensure the integrity of data and prevent tampering or alteration. By creating an immutable record of data, blockchain technology can provide a secure and trustworthy record of aviation communication network transactions.

Unanimity

Unanimity refers to the ability of blockchain technology to achieve consensus among nodes on the network. In the context of aviation communication networks, unanimity can help ensure that all nodes on the network agree on the state of the network and the validity of transactions. By achieving consensus among nodes, blockchain technology can provide a secure and trustworthy mechanism for validating transactions and ensuring the integrity of aviation communication networks.

Transparency

Transparency refers to the ability of blockchain technology to provide a clear and visible record of transactions or data. In the context of aviation communication networks, transparency can help ensure that all stakeholders have access to accurate and timely information. By providing a transparent record of transactions and data, blockchain technology can help build trust and confidence in aviation communication networks.

Corresponding author: Augustine Omokhogie Evans
augustineevans75@gmail.com
NeoCloud Technologies, Gwarimpa, Abuja, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(4), DECEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Security

Security refers to the ability of blockchain technology to protect data and transactions from unauthorized access or tampering. In the context of aviation communication networks, security is critical to preventing cyber-attacks and ensuring the integrity of data. By using advanced cryptographic techniques and a decentralized architecture, blockchain technology can provide a secure and trustworthy mechanism for protecting aviation communication networks.

Consensus Mechanisms

Consensus mechanisms refer to the algorithms and protocols used to achieve consensus among nodes on a blockchain network. In the context of aviation communication networks, consensus mechanisms can help ensure that all nodes on the network agree on the state of the network and the validity of transactions. Common consensus mechanisms used in blockchain technology include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).

INTEGRATION OF BLOCKCHAIN IN AVIATION COMMUNICATION NETWORKS

The aviation industry relies heavily on communication networks to ensure safe and efficient air travel. However, these networks are vulnerable to cyber threats, data breaches, and unauthorized access. The integration of Blockchain technology in aviation communication networks offers a promising solution to these challenges. Figure 3 depict a Blockchain based framework for securing aerial communication. Integration of blockchain into aviation communication networks promotes privacy, security and data integrity.

Figure 3: A Blockchain based framework for securing aerial communication

Key aviation cyber security threats include data manipulation attacks, which are facilitated by the radio frequency nature of aviation communication. The integration of multiple Blockchain through the ground infrastructure, in particular, would necessitate the validation of data from other Blockchain to prevent attackers from undermining the integrity of Blockchain. Adoption of Blockchain will hence offer protection against data integrity threats, an enhancement that has

Corresponding author: Augustine Omokhogie Evans
augustineevans75@gmail.com
NeoCloud Technologies, Gwarimpa, Abuja, Nigeria.

resonated among regulatory stakeholders, pilots, and air traffic controllers.

BENEFITS AND CHALLENGES

Aviation networks stand to benefit greatly from interoperable data sharing across organizational boundaries thanks to the many advantages that blockchain provides (Momoh et al., 2022). Intuitively, data record integrity is highly important in cases where lives are at stake – aviation networks require zero false positives. The capabilities of blockchain contribute to enhanced security of any network equipment or services with access to sensitive data. Furthermore, since blockchain is a transaction history journal, an aviation blockchain solution promotes operational transparency while maintaining trust thanks to individual verification nodes that prevent single points of failure (Hawashin et al., 2024). Additionally, every relevant aviation process could rely on the blockchain underlying the data to streamline real-time operations and reduce operational redundancy and costs. Most significantly, border authorities rely on filing data produced through aviation messages.

Implementation of a systemic change, such as the joint adoption of blockchain by the aviation community, however, will be of high technical complexity. Moreover, such a powerful transformative process will require significant regulatory coordination and political capital to drive (Hawashin et al., 2024). Some aviation communication actors may accrue competitive advantage by blockchain-secured data-as-a-service, for which they might be willing to pay intellectual property dues. Lastly, the blockchain-as-a-service model for aviation intercommunication services would require direct participants to place their trust in the service provider, who could then indirectly read the data they transmit. Consequently, it is important for all stakeholders to weigh potentially competitive benefits against the acknowledged challenge of implementation. This goal is to inform this discussion for those involved in aviation practitioners to make more informed decisions about this revolutionary project.

CONCLUSION

The aviation industry stands at a pivotal moment where the integration of innovative technologies, such as blockchain, is essential to address the growing challenges of cyber threats and vulnerabilities in communication networks. The traditional systems currently in use are inadequate in providing the necessary security measures, leaving them exposed to various risks that can have severe implications for safety and operational efficiency. Blockchain technology offers a promising avenue for enhancing the resilience of aviation communication networks by ensuring data integrity, promoting transparency, and preventing unauthorized access. However, the successful implementation of blockchain will require significant collaboration among regulatory bodies, industry stakeholders, and technology providers to navigate the complexities of integration and establish a unified approach. As the aviation sector continues to evolve, embracing such transformative solutions will be crucial in maintaining the safety and security of air travel in an increasingly digital world.

REFERENCES

Chen, Y., Zhao, Y., & Wu, Y. (2024). Recent progress in air traffic flow management: A review. *Journal of Air Transport Management*, *116*, 102573.

Chinedu, P. U., Nwankwo, W., Aliu, D., Shaba, S. M., & Momoh, M. O. (2020). Cloud security concerns: assessing the fears of service adoption. *Archive of Science and Technology*, *1*(2), 164-174.

Daniel, A., & Momoh, M. O. (2021). A computer security system for cloud computing based on encryption technique. *Computer Engineering and Applications Journal*, *10*(1), 41-54.

Ferrão, I. G., Espes, D., Dezan, C., & Branco, K. R. L. J. C. (2022). Security and safety concerns in air taxis: a systematic literature review. *Sensors*, *22*(18), 6875.

Hawashin, D., Nemer, M., Gebreab, S. A., Salah, K., Jayaraman, R., Khan, M. K., & Damiani, E. (2024). Blockchain

Corresponding author: Augustine Omokhogie Evans
augustineevans75@gmail.com
NeoCloud Technologies, Gwarimpa, Abuja, Nigeria.

applications in UAV industry: Review, opportunities, and challenges. *Journal of Network and Computer Applications*, *230*, 103932.

Kistan, T., Gardi, A., Sabatini, R., Ramasamy, S., & Batuwangala, E. (2017). An evolutionary outlook of air traffic flow management techniques. *Progress in aerospace sciences*, *88*, 15-42.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Momoh, M. O., Chinedu, P. U., Nwankwo, W., Aliu, D., & Shaba, M. S. (2021). Blockchain Adoption: Applications and Challenges. *International Journal of Software Engineering and Computer Systems*, *7*(2), 19-25.

Momoh, M. O., Shobowale, K. O., Abubakar, Z. M., Yahaya, B., & Ibrahim, Y. (2022). Blockchain Adoption in Aviation: Opportunities and Challenges. International Journal of Electrical Engineering and Computing, Vol. 6, No. 2 (2022), pp.92-97.

Nguyen, T., Lim, C. P., Nguyen, N. D., Gordon-Brown, L., & Nahavandi, S. (2019). A review of situation awareness assessment approaches in aviation environments. *IEEE Systems Journal*, *13*(3), 3590-3603.

Sampigethaya, K., & Poovendran, R. (2013). Aviation cyber–physical systems: Foundations for future aircraft and air transport. *Proceedings of the IEEE*, *101*(8), 1834-1855.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), 146.

Umoh, I. J., Marufat, G. O., Basira, Y., Abdulfatai, A. D., & Muyideen, M. O. (2019). BANM: A Distributed Network Manager Framework for Software Defined Network-On-Chip (SDNoC). Covenant Journal of Informatics and Communication Technology.

Woltjer, R., Johansson, B. J., Oskarsson, P. A., Svenmarck, P., & Kirwan, B. (2022). Air transport system agility: The Agile Response Capability (ARC) methodology for crisis preparedness. *Infrastructures*, *7*(2), 11.

Corresponding author: Augustine Omokhogie Evans
augustineevans75@gmail.com
NeoCloud Technologies, Gwarimpa, Abuja, Nigeria.