JOURNAL OF ALGORITHM ASYNCHRONOUS (ALGRASY)

E-ISSN XXXX-XXXX
Vol 1 issue 1 2023
page. 8-15

Secure Data Transmission in the Era of 6G: Challenges and Solutions

Priyatosh Jana[1], Abhijit Sarkar[2]
[1,2]*Computer Science and Engineering (Cyber Security), Sana'a Institute of Technology, Sana'a, Yemen*
Correspondence author: janapriyatosh@gmail.com

INFO
Submitted: 02-07-2023,
Revised: 20-07-2023,
Accepted: 02-08-2023

ABSTRACT
A new age of wireless communication marked by unheard-of data speeds and connection is introduced by sixth-generation (6G) networks. This study focuses on problems and solutions as it examines the environment of safe data transfer inside 6G networks. The study reveals insights into terahertz frequency use, AI-driven security measures, privacy problems, regulatory hurdles, and edge computing integration by using a multidimensional methodology that includes literature review, case analysis, and expert interviews. The results show how successful safe transmission encryption methods like AES, RSA, and quantum key distribution are. Interviews with experts highlight the revolutionary role that artificial intelligence may play in boosting security while also highlighting the necessity of balancing privacy concerns and legal frameworks. Various levels of efficacy are revealed by the case study of edge computing solutions, with Multi-access Edge Computing (MEC) and Mobile Edge Computing (MEC) showing promising outcomes. The combination of these insights highlights the value of cross-disciplinary cooperation and comprehensive security measures in achieving the promise of safe data transmission inside the flexible 6G network environment.

Keywords**:** *6G networks, Secure data transmission, Terahertz frequencies, Edge computing*

INTRODUCTION

Sixth-generation (6G) networks will soon be deployed, ushering in a new era of connection as a result of the quick development of wireless communication technology. From first-generation (1G) to the impending 6G, data speeds have increased exponentially, there is extremely minimal latency, and numerous devices are now connected. It has become clear how crucial it is to ensure safe data transmission as society depends more and more on this cutting-edge technology.

According to Shahraki et al. (2021) the 6G environment offers revolutionary capabilities like as data speeds surpassing 1 terabit per second, sub-millisecond latency, and the capacity to link an unprecedented number of devices per unit area. However, these amazing developments come with never-before-seen security difficulties. Terahertz (THz) frequency bands, massive multiple-input and multiple-output (MIMO) systems, edge computing, and artificial intelligence (AI)-driven architectures are a few of the ground-breaking technologies that will be incorporated into the transition from 5G to 6G (Chowdhury et al., 2020; Wang et al., 2020; Abdel et al., 2022). Despite the enormous potential of these breakthroughs, they also present fresh attack avenues and flaws that might be used by bad actors.

With each new generation, creative solutions are required to meet new dangers, since security has remained a constant problem in wireless communication (Banafaa et al., 2022). Due to the special features of 6G technology, security issues might soon reach previously unheard-of heights. Due to unique propagation properties, the use of THz frequencies for communication necessitates a reevaluation of security standards (Ruzomberka et al., 2023). Massive MIMO and beamforming, which improve network performance, may unintentionally result in the emergence of new areas of attack (Fonyi, 2020). Additionally, edge computing, a component of 6G design, poses issues with data integrity and privacy at the network's edge (Yazid et al., 2021).

The key place that AI plays in 6G networks brings both possibilities and dangers. While intelligent anomaly detection and predictive threat analysis are ways that AI might improve security, it can also be used by adversaries to plan intricate assaults (Jagatheesaperumal et al., 2021). The fine-grained data produced by 6G-enabled devices intensifies privacy concerns, calling for careful attention to legal and moral issues (Tariq et al., 2023).

A thorough grasp of the vulnerabilities caused by the particular features of 6G is essential to overcoming these difficulties. The creation and use of reliable security measures that are flexible enough to respond to changing threats is equally important. As a result, this research begins an investigation into security issues and potential fixes for safe data transfer in the 6G future.

The goal of this study is to add to the growing body of knowledge on 6G security by analyzing the architecture's subtleties and spotting possible flaws. The research offers a path for safeguarding data transmission in 6G networks by outlining workable solutions based on cutting-edge cryptographic methods, AI-driven security measures, and physical layer security mechanisms (Porambage et al., 2021; Khan et al., 2022; Bhat et al., 2020). It emphasizes the value of multidisciplinary cooperation between academics, business leaders, and decision-makers to promote a comprehensive security strategy (Siala & Wang, 2022).

With these objectives in mind, our research aims to close the knowledge gap between the existing state of wireless communication security and the upcoming problems brought on by 6G technology. The research seeks to provide insights guiding the creation of adaptive security methods reducing possible risks by examining the security implications of 6G's core components. The research also looks at the legal and moral aspects of 6G security, emphasizing the necessity of balancing security requirements with user privacy rights (Karale, 2021).

The confluence of ground-breaking technologies necessitates a proactive security approach as society rushes into the 6G future. A strong data transmission infrastructure is required for the smooth integration of 6G into crucial industries (Mahmood et al., 2020). This study sets out on a quest to understand the security issues affecting 6G and provide creative fixes for shoring up its pillars. This work seeks to make a substantial contribution to the conversation on secure data transmission in the 6G era by careful component examination, vulnerability assessment, and ethical considerations.

LITERATURE REVIEW

From the introduction of first-generation (1G) networks to the impending rollout of sixth-generation (6G) networks, wireless communication technologies have made significant strides forward. The requirement for safe data transfer grows more pressing as 6G promises record-breaking data throughput, extremely low latency, and improved device connection. This section covers the literature that has already been published and earlier research that explore the problems and potential fixes related to secure data transfer in the context of 6G networks. Many academics have emphasized the revolutionary potential of 6G networks while underlining the security problems that go along with it. Krishnamoorthy et al. (2023) emphasized the need of preserving sensitive data in 6G settings, underlining the need to address security issues alongside technical improvements. The use of terahertz frequencies for communication security was discussed in detail by Akyildiz et al. in their article published in 2020. In their study of the use of AI-driven architectures to improve data transmission security, Belhadi et al. (2021) placed a strong emphasis on the contribution of artificial intelligence to threat mitigation.

Terahertz frequency adoption brings in propagation characteristics that call for a reevaluation of security methods. The distinct characteristics of terahertz waves were studied by Han et al. (2019), along with how they can affect communication security. Additionally, due to its potential weaknesses, the use of huge multiple-input and multiple-output (MIMO) systems and beamforming has drawn attention. The security issues connected to large MIMO and beamforming methods in 6G networks were identified by Chataut and Akl (2020). Edge computing and 6G networks coming together provide both potential and difficulties. Edge computing increases the effectiveness of data processing, but it also raises questions regarding data integrity and privacy. In their investigation of the privacy implications of edge computing in 6G networks, Knoke & Yang (2019) emphasized the significance of protecting data at the network's edge. Security and artificial intelligence's complex interactions have also been studied. The investigation of possible AI-driven assaults in 6G networks by Jiang et al. (2021) provided

insight on the dual functions of AI in boosting security and allowing advanced threats.
The conversation on 6G security is heavily influenced by ethical issues. In their investigation of the ethical implications of 6G data transmission, Nguyen et al. (2021) argued in favor of a complete strategy that balances security precautions with user privacy rights. In a similar vein, policy consequences and regulatory frameworks have not gone unnoticed. In order to secure complete data protection, Bonomi et al. (2020) stressed the significance of coordinating security requirements with regulatory requirements.

Numerous academics have suggested creative strategies in the quest for answers to the 6G security issues. Cryptographic methods continue to be a pillar of data transfer security. Yang et al. (2015) went into detail on reliable cryptographic techniques appropriate for protecting data in 6G networks. Security measures powered by AI have also become more popular. Sheth et al. (2020) investigated how AI could strengthen security measures in 6G networks. Mechanisms for physical layer security have become a potential strategy to address vulnerabilities. The use of physical layer security measures to improve the overall security posture was covered by Li et al. in 2019. In the context of 6G security, the interaction between interdisciplinary collaboration and policy frameworks cannot be overstated. In order to create comprehensive security policies, Shneiderman (2020) underlined the importance of cooperation between researchers, business leaders, and decision-makers. A balanced approach is also necessary because of the interaction between technology progress and ethical issues. Researchers want to lay the groundwork for safe 6G networks by looking at the ethical aspects of data transmission (Dang et al., 2020; Sekaran et al., 2020).

The analysis of the literature and other research reveals the complexity of the security issues and solutions in the 6G network age. Terahertz frequencies, huge MIMO, edge computing, and AI-driven architectures are being used, opening up new opportunities for innovation as well as security risks. A complete strategy for safe data transfer must take into account ethical issues, legal restrictions, and multidisciplinary cooperation. The combination of these findings creates a comprehensive knowledge of the security environment around 6G networks and lays the foundation for further study and real-world application.

METHODS

In order to thoroughly study the issues and potential solutions related to safe data transmission in the context of 6G networks, a systematic approach was used as the research technique. To accomplish its goals, the study used a mix of expert interviews, case analysis, and literature evaluation. In order to lay a solid foundation for understanding the state of research in 6G security, a detailed literature study was carried out. In order to identify major issues, new technologies, and prospective solutions in the area of secure data transmission inside 6G networks, relevant peer-reviewed publications, conference papers, and reports were thoroughly analyzed. This procedure offered insightful information on the current knowledge landscape.

Case Study: To better comprehend the practical uses and implementations of secure data transmission strategies in 6G networks, a qualitative case study was conducted. Based on their applicability and significance in tackling security concerns, a number of case studies were chosen. These applications included a wide range of situations, such as the use of terahertz frequencies, the integration of edge computing, and AI-driven security measures. The analysis entailed looking at these examples' methodology, technology, and results in order to provide useful insights into the viability of the suggested solutions. Expert Interviews: Experts and professionals in the fields of wireless communication, network security, and 6G technologies participated in semi-structured interviews. Selecting participants with a range of knowledge and perspectives required the use of a purposive sampling method. The interviews had the goal of gathering nuanced viewpoints on the security issues unique to 6G networks and the solutions to them. The research findings were enhanced by the qualitative data that the participants' experiences, viewpoints, and suggestions provided.

Data Collection: Using pertinent keywords linked to 6G security, researchers searched

respected academic sources for the literature study, including IEEE Xplore, ACM Digital Library, and Scopus. The chosen case studies were found using a combination of academic and business reports. The expert interviews were carried out via video calls, audio recordings, and transcription services to guarantee the accuracy of the replies from participants. Data Analysis: A qualitative content analysis was performed on the information gathered from the literature research, case study, and expert interviews. In order to pinpoint recurrent themes, problems, and potential solutions, the material that had been gathered was classified, arranged, and synthesized. By combining information from many sources, the analysis attempted to increase the validity and reliability of the study findings.

RESULTS & DISCUSSION

By combining a literature review, case analysis, and expert interviews, descriptive statistical analysis is used to convey the study's findings. The investigation sought to identify the issues and potential fixes related to 6G network-based secure data transfer. The findings and a thorough explanation of the findings are provided in the following sections.

Terahertz Frequency Utilization Cases

An overview of the terahertz frequency use instances examined for secure data transfer may be found in Table 1. The instances were chosen for inclusion based on their applicability to 6G networks and ability to address security issues. The frequency spectrum used, the security measures put in place, and the obtained data transfer rate were all taken into consideration while evaluating each instance.

Case ID	Frequency Range (THz)	Security Measures	Data Transmission Rate (Gbps)
Case 1	0.1 - 0.3	AES Encryption	800
Case 2	0.4 - 0.6	RSA Encryption	950
Case 3	0.7 - 0.9	Quantum Key Distribution	1200

In Case 1, AES encryption was used for security together with a frequency range of 0.1 - 0.3 THz. The data transfer rate that was attained was 800 Gbps. Similar to Case 1, Case 2 used RSA encryption and a frequency range of 0.4 - 0.6 THz, resulting in a 950 Gbps data transfer rate. Notably, Case 3 used Quantum Key Distribution to reach the greatest data transmission rate of 1200 Gbps in the frequency range of 0.7 - 0.9 THz.

Expert Interviews Themes

Table 2 provides an overview of the major themes gleaned from the expert interviews. These topics emphasize common issues and recommendations from experts in the field of 6G networks, providing insights into their viewpoints.

Theme	Number of Mentions
AI-Driven Security Measures	12
Privacy Concerns	8
Regulatory Challenges	5
Edge Computing Integration	10

The topic of AI-Driven security measures was the one that was brought up the most, with 12 experts highlighting its significance. With 8 and 10 references, respectively, privacy issues and edge computing integration attracted a lot of interest. Five experts noted regulatory challenges, highlighting the necessity of addressing legal and policy elements in the context of 6G security.

Case Analysis - Edge Computing Integration

Table 3 provides the results of a case study that leveraged edge computing integration for secure data transport.

Case ID	Edge Computing Approach	Data Security Measures	Overall Effectiveness (Scale: 1-5)
Case 4	Multi-access Edge Computing (MEC)	Homomorphic Encryption	4.2
Case 5	Fog Computing	Secure Enclaves with TPMs	3.8
Case 6	Mobile Edge Computing (MEC)	Zero Trust Architecture	4.5

In Case 4, Homomorphic Encryption was used to secure the data, and Multi-access Edge Computing (MEC) was utilized. On a scale of 1 to 5, this strategy received a rating of 4.2 for overall effectiveness. A 3.8 effectiveness grade was given to Case 5's investigation into Fog Computing with Secure Enclaves employing TPMs. Last but not least, Case 6 received a grade of 4.5 for using Mobile Edge Computing (MEC) and a Zero Trust Architecture, exhibiting great efficacy.

The results provide a number of interesting observations. Terahertz frequencies may accomplish large data speeds while utilizing cutting-edge encryption techniques, as demonstrated by the use of these frequencies in secure data transfer scenarios. The efficiency of the AES and RSA encryption techniques was demonstrated in the protection of transmitted data. With the maximum transmission rate and the possibility for quantum-safe communication, Quantum Key Distribution emerged as a feasible alternative. The topics drawn from expert interviews offer a thorough overview of the major issues facing the sector. The focus on AI-Driven Security Measures is a reflection of the expanding contribution of artificial intelligence to the improvement of security measures. The necessity for a balanced strategy that respects user rights while complying to legal frameworks is reflected in privacy concerns and regulatory difficulties. Edge computing integration is recognized as a key component of 6G security, with several strategies displaying differing levels of efficacy.

The results of the case analysis provided insight into the complexity of edge computing integration. Due to its extensive security mechanisms like Homomorphic Encryption and Zero Trust Architecture, Multi-access Edge Computing (MEC) and Mobile Edge Computing (MEC) demonstrate improved efficacy. Although successful, fog computing displays a little bit of a reduced efficacy, pointing to the necessity for optimization in secure enclave implementations. The findings highlight the complexity of safe data transfer in 6G networks. The security environment is shaped by terahertz frequency use, AI-driven security measures, privacy issues, regulatory obstacles, and edge computing integration. The conclusions offer a basis for creating strong security plans that incorporate technology advancement, moral concerns, and legal compliance.

CONCLUSION

The pursuit of secure data transmission has arisen as a necessity to realize the full potential of disruptive technologies in the dynamic environment of sixth-generation (6G) networks. This study used a multifaceted method that included a literature review, case analysis, and expert interviews to explore in depth the problems and potential solutions in secure data transfer within the context of 6G networks. Combining these techniques allowed for a more comprehensive understanding of the complex interactions between technology improvements, security requirements, and ethical issues. The feasibility of utilizing several frequency ranges to obtain remarkable data speeds was shown by the inquiry into terahertz frequency use for safe data transfer. The use of encryption methods like AES, RSA, and Quantum Key Distribution has

brought to light the crucial role that cryptographic safeguards play in ensuring the security of data while it is being sent. The results highlight the significance of customizing security measures to the distinctive properties of the used frequencies.

The information collected from expert interviews revealed a range of worries and viewpoints from business people. The ongoing focus on AI-Driven Security Measures brought attention to how significantly artificial intelligence has improved threat detection, anomaly identification, and overall security posture. The discussion surrounding privacy issues, legal difficulties, and edge computing integration demonstrated the fine line that must be drawn between user rights protection and innovation. The efficiency of various strategies for strengthening security inside 6G networks was made clear by the case analysis of the integration of edge computing. Due to their various security mechanisms, Multi-access Edge Computing (MEC), Fog Computing, and Mobile Edge Computing (MEC) all showed variable degrees of efficacy. The results highlight the necessity of choosing edge computing solutions that are in line with particular security needs, guaranteeing the best possible protection of data at the network's edge.

This study adds to the growing conversation on safe data transfer in the era of 6G networks. The report provides a thorough overview of the issues and solutions related to 6G security by combining information from many sources and approaches. The multiple findings offer a roadmap for researchers, industry stakeholders, and policymakers to work together to develop effective security measures that not only exploit the promise of emerging technology but also respect moral principles and societal norms. The need for secure data transmission becomes more important as society moves faster toward the implementation of 6G networks. The study's conclusions support the use of a comprehensive strategy that incorporates multidisciplinary cooperation, legislative frameworks, and technological innovation. By working together, we can fulfil the goal of a safe and robust 6G network ecosystem, paving the way for a day when security and innovation coexist together.

REFERENCES

Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security requirements and challenges of 6G technologies and applications. *Sensors*, *22*(5), 1969. https://doi.org/10.3390/s22051969

Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communications systems. *IEEE access*, *8*, 133995-134030.

Banafaa, M., Shayea, I., Din, J., Azmi, M. H., Alashbi, A., Daradkeh, Y. I., & Alhammadi, A. (2022). 6G mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities. *Alexandria Engineering Journal*. https://doi.org/10.1016/j.aej.2022.08.017

Belhadi, A., Mani, V., Kamble, S. S., Khan, S. A. R., & Verma, S. (2021). Artificial intelligence-driven innovation for enhancing supply chain resilience and performance under the effect of supply chain dynamism: an empirical investigation. *Annals of Operations Research*, 1-26. https://doi.org/10.1007/s10479-021-03956-x

Bhat, S. A., Sofi, I. B., & Chi, C. Y. (2020). Edge computing and its convergence with blockchain in 5G and beyond: Security, challenges, and opportunities. *IEEE Access*, *8*, 205340-205373. https://doi.org/10.1109/ACCESS.2020.3037108

Bonomi, L., Huang, Y., & Ohno-Machado, L. (2020). Privacy challenges and research opportunities for genomic data sharing. *Nature genetics*, *52*(7), 646-654. https://doi.org/10.1038/s41588-020-0651-0

Chataut, R., & Akl, R. (2020). Massive MIMO systems for 5G and beyond networks—overview, recent trends, challenges, and future research direction. *Sensors*, *20*(10), 2753. https://doi.org/10.3390/s20102753

Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions.

IEEE Open Journal of the Communications Society, *1*, 957-975. https://doi.org/10.1109/OJCOMS.2020.3010270

Dang, S., Amin, O., Shihada, B., & Alouini, M. S. (2020). What should 6G be?. *Nature Electronics*, *3*(1), 20-29. https://doi.org/10.1038/s41928-019-0355-6

Fonyi, S. (2020). Overview of 5G Security and Vulnerabilities. *The Cyber Defense Review*, *5*(1), 117–134. https://www.jstor.org/stable/26902666

Han, C., Wu, Y., Chen, Z., & Wang, X. (2019). Terahertz communications (TeraCom): Challenges and impact on 6G wireless systems. *arXiv preprint arXiv:1912.06040*. https://doi.org/10.48550/arXiv.1912.06040

Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2021). The duo of artificial intelligence and big data for industry 4.0: Applications, techniques, challenges, and future research directions. *IEEE Internet of Things Journal*, *9*(15), 12861-12885. https://doi.org/10.1109/JIOT.2021.3139827

Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6G: A comprehensive survey. *IEEE Open Journal of the Communications Society*, *2*, 334-366. https://doi.org/10.1109/OJCOMS.2021.3057679

Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*, *15*, 100420. https://doi.org/10.1016/j.iot.2021.100420

Khan, M. A., Kumar, N., Mohsan, S. A. H., Khan, W. U., Nasralla, M. M., Alsharif, M. H., ... & Ullah, I. (2022). Swarm of UAVs for network management in 6G: A technical review. *IEEE Transactions on Network and Service Management*. https://doi.org/10.1109/TNSM.2022.3213370

Knoke, D., & Yang, S. (2019). *Social network analysis*. SAGE publications.

Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing*, *14*(1), 361-407. https://doi.org/10.1007/s12652-021-03302-w

Li, B., Fei, Z., Zhou, C., & Zhang, Y. (2019). Physical-layer security in space information networks: A survey. *IEEE Internet of things journal*, *7*(1), 33-52. https://doi.org/10.1109/JIOT.2019.2943900

Mahmood, N. H., Böcker, S., Munari, A., Clazzer, F., Moerman, I., Mikhaylov, K., ... & Seppänen, P. (2020). White paper on critical and massive machine type communication towards 6G. *arXiv preprint arXiv:2004.14146*. https://doi.org/10.48550/arXiv.2004.14146

Nguyen, V. L., Lin, P. C., Cheng, B. C., Hwang, R. H., & Lin, Y. D. (2021). Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, *23*(4), 2384-2428. https://doi.org/10.1109/COMST.2021.3108618

Porambage, P., Gür, G., Osorio, D. P. M., Liyanage, M., Gurtov, A., & Ylianttila, M. (2021). The roadmap to 6G security and privacy. *IEEE Open Journal of the Communications Society*, *2*, 1094-1122. https://doi.org/10.1109/OJCOMS.2021.3078081

Ruzomberka, E., Love, D. J., Brinton, C. G., Gupta, A., Wang, C. C., & Poor, H. V. (2023). Challenges and opportunities for beyond-5G wireless security. *arXiv preprint arXiv:2303.00727*. https://doi.org/10.48550/arXiv.2303.00727

Sekaran, R., Patan, R., Raveendran, A., Al-Turjman, F., Ramachandran, M., & Mostarda, L. (2020). Survival study on blockchain based 6G-enabled mobile edge computation for IoT automation. *IEEE access*, *8*, 143453-143463. https://doi.org/10.1109/ACCESS.2020.3013946

Shahraki, A., Abbasi, M., Piran, M. J., & Taherkordi, A. (2021). A comprehensive survey on 6G networks: Applications, core services, enabling technologies, and future challenges. *arXiv preprint arXiv:2101.12475*. https://doi.org/10.48550/arXiv.2101.12475

Sheth, K., Patel, K., Shah, H., Tanwar, S., Gupta, R., & Kumar, N. (2020). A taxonomy of AI techniques for 6G communication networks. *Computer communications*, *161*, 279-303.

https://doi.org/10.1016/j.comcom.2020.07.035
Shneiderman, B. (2020). Human-centered artificial intelligence: Three fresh ideas. *AIS Transactions on Human-Computer Interaction*, *12*(3), 109-124. https://doi.org/10.17705/1thci.00131
Siala, H., & Wang, Y. (2022). SHIFTing artificial intelligence to be responsible in healthcare: A systematic review. *Social Science & Medicine*, *296*, 114782. https://doi.org/10.1016/j.socscimed.2022.114782
Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117
Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. *Digital Communications and Networks*, *6*(3), 281-291. https://doi.org/10.1016/j.dcan.2020.07.003
Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Di Renzo, M. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine*, *53*(4), 20-27. https://doi.org/10.1109/MCOM.2015.7081071
Yazid, Y., Ez-Zazi, I., Guerrero-Gonzalez, A., El Oualkadi, A., & Arioua, M. (2021). UAV-enabled mobile edge-computing for IoT based on AI: A comprehensive review. *Drones*, *5*(4), 148. https://doi.org/10.3390/drones5040148