*Science Discovery Physics*
2026, Vol. 1, No. 1, pp. 29–35
https://doi.org/10.11648/j.sdp.20260101.12

Research Article

# A Systematic Literature Review: Quantum Key Distribution Networks: Challenges and Future Research Issues in Security

**Abel Channie Demeke***

Department of Computer Science and Engineering, Adama Science and Technology University, Adama, Ethiopia

## Abstract

With the rapid advancement of quantum computing, traditional cryptographic techniques are at risk of devolution, necessitating quantum-resilient alternatives for future communication networks. This systematic literature review evaluates the role of Quantum Key Distribution (QKD) in enhancing the security of sixth-generation (6G) wireless communications. Employing the PRISMA methodology, 48 peer-reviewed studies published between 2016 and May 2025 were identified and analyzed. The review addresses three key research questions: the identification of QKD protocols applicable to 6G, challenges in their integration, and proposed solutions for seamless deployment. Findings reveal that protocols such as BB84, E91, CV-QKD, and MDI-QKD, transmitted via optical fiber and satellite channels, offer promising security guarantees. This review concludes that while QKD can significantly strengthen 6G communications against quantum threats, further interdisciplinary efforts in hardware development, standardization, and pilot implementations are essential. The study offers valuable insights for researchers, engineers, and policymakers working toward secure, quantum-resistant future networks. The study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology to ensure transparency, rigor, and reproducibility. A comprehensive search was conducted across major scientific databases, including IEEE Xplore, SpringerLink, ScienceDirect, and arXiv, using well-defined keywords and Boolean search strategies related to QKD, 6G networks, and quantum communication security. After removing duplicates and applying predefined inclusion and exclusion criteria, a total of 48 peer-reviewed studies published between 2016 and May 2025 were selected for detailed analysis. The selected literature was systematically classified to address three primary research questions: (i) identification of QKD protocols and technologies applicable to 6G networks, (ii) challenges hindering the integration of QKD into 6G architectures, and (iii) solutions and frameworks proposed to facilitate practical deployment. The findings reveal that prominent QKD protocols, including BB84, E91, Continuous-Variable QKD (CV-QKD), and Measurement-Device-Independent QKD (MDI-QKD), demonstrate strong potential for securing 6G communications when deployed over optical fiber and satellite-based channels. However, practical integration faces significant challenges such as scalability limitations, synchronization issues, quantum channel coexistence with classical networks, hardware complexity, and high deployment costs. The review further highlights emerging solutions that leverage Software-Defined Networking (SDN), Network Function Virtualization (NFV), blockchain-based key management, and hybrid classical-quantum security architectures to overcome these obstacles. Ongoing standardization efforts by organizations such as NIST, ETSI, and ITU-T are also identified as critical enablers for real-world adoption .

*Correspondence: Abel Channie Demeke (abelchanie21@gmail.com)

**Received:** 22 December 2025; **Accepted:** 13 January 2026; **Published:** 9 February 2026

## Keywords

Quantum Key Distribution (QKD), 6G Communication Security, Post-Quantum Cryptography, Quantum-Resilient Networks

# 1. Introduction

A paradigm change in processing power, quantum computing poses a challenge to the traditional encryption techniques that are still frequently employed in modern communication networks. By guaranteeing the creation and exchange of cryptographic keys in a way that is theoretically unbreakable, Quantum Key Distribution (QKD), which makes use of the concepts of quantum physics, provides a safe substitute. Integrating QKD is becoming more and more important as we move toward the sixth generation (6G) of wireless communication networks, which are distinguished by extremely low latency, extensive connection, and increased security requirements. The present status, difficulties, and prospects of QKD in guaranteeing secure 6G communications are evaluated in this review.

## 1.1. Motivation

Future communication systems' security frameworks need to be reevaluated in light of the quantum computing industry's explosive growth. Sensitive applications like remote surgery, driverless cars, and smart city infrastructure should be supported by 6G. In the face of quantum attacks, conventional cryptographic methods might become outdated, which makes QKD a viable option for securing networks in the future.

## 1.2. Scope

The architectures, integration difficulties, performance measurements, and security assurances of QKD technologies that are pertinent to 6G are all examined in this paper. Additionally, it assesses research patterns and suggested remedies aimed at removing obstacles to integration.

## 1.3. Significance

This review aids in the development of safe, quantum-resilient communication infrastructures by evaluating the incorporation of QKD into 6G networks. It helps policymakers, engineers, and researchers create reliable systems that counteract emerging cybersecurity risks.

## 1.4. Research Questions

RQ1 What are the primary QKD protocols and technologies applicable to 6G networks? RQ 2 What challenges hinder the integration of QKD into 6G architectures?

RQ 3 What solutions have been proposed or implemented to facilitate QKD deployment in 6G?

## 1.5. Objectives

### 1.5.1. General Objective

To evaluate the role of Quantum Key Distribution (QKD) in securing 6G communication networks.

### 1.5.2. Specific Objectives

1) To identify current QKD technologies suitable for 6G
2) To analyze the limitations and integration challenges
3) To review proposed frameworks and models for QKD-6G integration
4) To suggest future research directions for seamless QKD deployment in 6G

# 2. Literature Review

## 2.1. Quantum Key Distribution (QKD)

Through protocols like BB84 and E91, QKD allows two parties to use quantum states to generate shared secret keys. A thorough summary of real-world QKD problems is given by Diamanti et al. (2016) [1]. To further improve security, Primaatmaja et al. (2022) investigate device-independent QKD [2].

## 2.2. 6G Network Architecture

6G will combine ultra-reliable low-latency communications (URLLC), terahertz communication, and artificial intelligence. According to Huawei (2024), a crucial component of the 6G security architecture is native trustworthiness [3, 10-12].

## 2.3. Integration of QKD in 6G Network

In their discussion of quantum technology applications in 6G, Zeydan et al. (2025) highlight the viability of QKD for fast, secure communications [4]. Useful approaches for incorporating QKD into disaggregated 6G networks are

described by the CTTC project [5].

Furthermore, the integration of space-air-ground-sea networks presents unique security challenges and opportunities for QKD deployment [36].

## 2.4. Key Challenges

Challenges include scalability, standardization, key rate limitations, and deployment costs. ITU- T Y. 3800 outlines standardization requirements for QKD networks [6, 13, 16, 24].Challenges include scalability, standardization, key rate limitations, and deployment costs. ITU- T Y. 3800 outlines standardizationrequirements for QKD networks [6.14, 18, 276.14, 18, 27.] Connectivity in rural areas remains a significant challenge for 6G deployment. [22], which also impacts the practical rollout of QKD infrastructure. Additionally, the co existence of quantum channels with classical networks introduces synchronization and interference issues. [39]

## 2.5. Emerging Solutions

Dynamic QKD integration is made possible by the use of Network Function Virtualization (NFV) and Software-Defined Networking (SDN). Research is being done on hybrid encryption that combines classical and quantum techniques. [14-18].

# 3. Methodology

PRISMA standards were used in a systematic review technique. Keywords like "QKD", "6G security", and "quantum communication" were used to search databases like IEEE Xplore, SpringerLink, arXiv, and ScienceDirect. Relevance to 6G networks and peer-reviewed publication status were prerequisites for inclusion. 48 studies in all were chosen for examination. The studies include from year 2016 to 2025 May 30, 2025 based on relevance to core topics.

## 3.1. Step-by-Step Systematic Literature Review (SLR) Process

Step 1: Define the Review Protocol

For the title selected “Assessment of Quantum Key Distribution (QKD) for Secure 6G Communications” the objectives are:

1) Identify applicable QKD protocols for 6G
2) Explore integration challenges
3) Review proposed solutions and frameworks Step 2: Frame the Research Questions (RQs)

***Table 1.*** *Research Question.*

| RQ # | Research Question |
|---|---|
| RQ1Research Question | What are the primary QKD protocols and technologies applicable to 6G networks? |
| RQ2 | What challenges hinder the integration of QKD into 6G architectures? |
| RQ3 | What solutions have been proposed or implemented to facilitate QKD deployment in 6G? |

Step 3: Identify Data Sources

1) Databases used:
   a) IEEE Xplore
   b) SpringerLink
   c) arXiv
   d) ScienceDirect

Step 4: Develop a Search Strategy

2) Keywords:
   a) “Quantum Key Distribution” OR “QKD”NOT”
   b) “6G Security”
   c) “Quantum Communication”
3) Boolean Search:

("QKD" OR "Quantum Key Distribution") AND ("6G" OR "6G Networks") AND ("Security" OR "Quantum Communication")

Step 5: Screening and Eligibility (PRISMA Framework)

Prisma process flow diagram

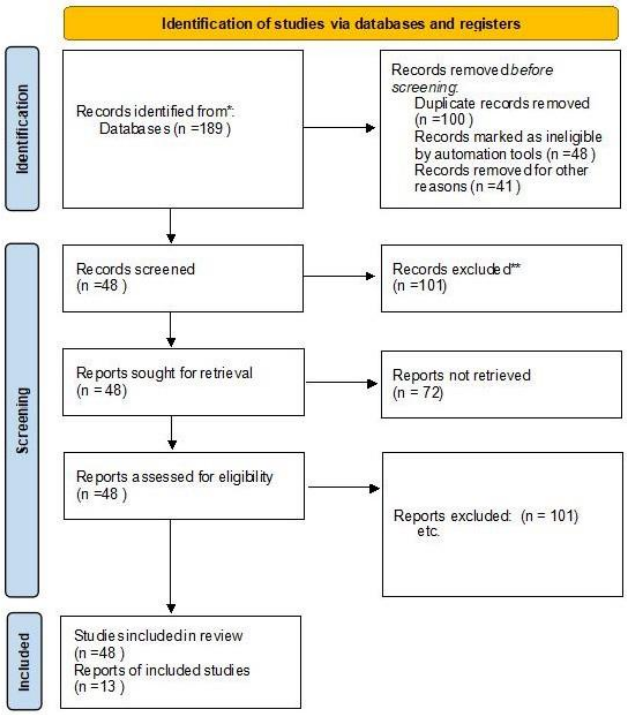


***Figure 1.*** *Prisma process flow diagram.*

*Table 2. Screening and Eligibility.*

| Stage | Count |
|---|---|
| Records identified | 189 |
| Duplicates removed | 41 |
| Title/Abstract screened | 100 |
| Full-text articles assessed | 72 |
| Studies included (final) | 48 |

## 3.2. Inclusion Criteria

1) Peer-reviewed journal/conference papers
2) Focus on QKD in context of 6G network
3) English language

## 3.3. Exclusion Criteria

1) Not related to 6G or post quantum
2) Non-peer-reviewed (blogs, opinion pieces) Step 6: Data Extraction & Classification

Studies were reviewed and classified into the three RQs:

1) RQ1 (Protocols/Technologies): 10 studies
2) RQ2 (Challenges): 11 studies
3) RQ3 (Solutions/Frameworks): 27 studies Step 7: Data Synthesis
4) RQ1: Identified protocols include BB84, E91, CV-QKD, and measurement-device- independent (MDI) QKD. Optical fiber and satellite-based links are dominant mediums.
5) RQ2: Challenges include scalability, quantum channel integration, decoherence, and synchronization.
6) RQ3: Solutions leverage SDN/NFV, blockchain, and satellite-QKD. Global standards from NIST and ETSI are emerging.

Step 8: Abstract Screening

Objective: Ensure deep technical alignment with your specific research question. I was tried to review abstracts for:

1) Whether primary QKD protocols and technologies applicable to 6G networks.
2) Whether challenges hinder the integration of QKD into 6G architectures.
3) Whether proposed or implemented to facilitate QKD deployment in 6G.

To do so I have prepared a check list as below, even though time is very limited to go through rigorously: -

Abstract Screening Checklist

Table:-Used checklist when reading abstracts to decide whether to include a paper in your SLR:

*Table 3. ScreeningCriteria.*

| ScreeningCriteria | Yes/No |
|---|---|
| 1. Does the abstract focus on Quantum Key Distribution (QKD)? | Yes |
| 2. Is there a clear connection to 6G communication networks? | Yes |
| 3. Does it mention security or cryptography in the context of QKD/6G? | Yes |
| 4. Is the work based on peer-reviewed or academic sources? | Yes |
| 5. Is the abstract written in English? | Yes |
| 6. Does the abstract describe methods or protocols (e.g., BB84, E91)? | Yes |
| 7. Are there any challenges or limitations mentioned? | Yes |
| 8. Does it offer or suggest solutions or frameworks? | Yes |
| 9. Does it indicate practical relevance (e.g., deployment, application areas)? | Yes |
| 10. Is it within the publication date range (e.g., 2016-2025)? | Yes |

I have been used this checklist while reviewing the 48 abstracts.

# 4. Results

The analysis indicates an increasing trend in publications discussing QKD for 6G security. Most works focus on simulation-based feasibility, while few provide empirical deployment results. QKD shows potential in metropolitan area networks and high-value communication links.

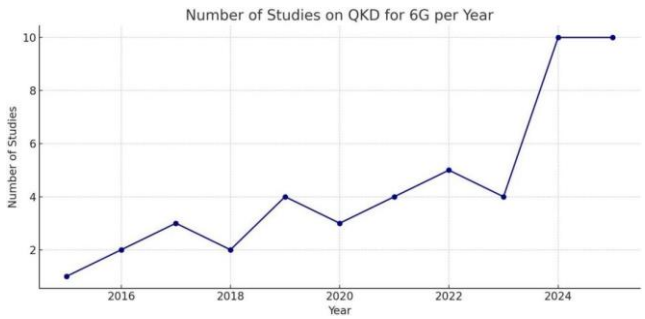


*Figure 2. Number of Studies on QKD for 6G per Year.*

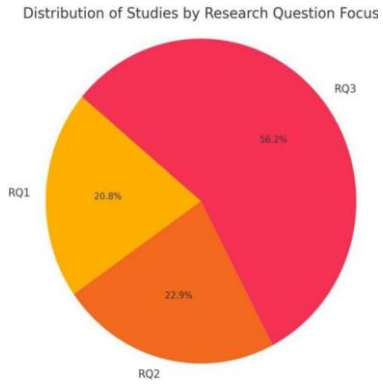


***Figure 3.*** *Distribution of Studies by Research Question Focus.*

## 5. Discussion

Despite its theoretical security, QKD encounters practical challenges in the widespread implementation of 6G. It is still difficult to integrate quantum channels into heterogeneous networks, as key generation rates decrease with distance. Nonetheless, standardization and prototype development initiatives show promise.

Dynamic QKD integration is made possible by the use of Network FunctionVirtualization (NFV) and Software-Defined Networking (SDN). Research isbeing done on hybrid encryption that combines classical and quantumtechniques. [14, 16] Blockchain technology is also being explored for secure key management and to enhance the trustworthiness of decentralized 6G network slices [12, 23]. Deep learning and AI techniques are proposed for optimizing network resource allocation and improving the efficiency of QKD-integrated systems [41-44]

## 6. Findings

1) QKD can significantly enhance 6G security against quantum threats
2) Practical deployment remains limited due to physical and cost constraints
3) SDN, AI-based optimization, and standardization are key enablers for adoption

## 7. Future Directions

Development of quantum repeaters and satellite-based QKD.[25-30] Real-world pilot deployments for urban and rural 6G environments Creation of lightweight QKD solutions suitable for IoT devices

## 8. Conclusion

One revolutionary technology for 6G communications security is QKD. Although theoretical frameworks are well-established, cooperative innovation in hardware, network architecture, and policy-making is necessary for practical implementation. This evaluation demonstrates the potential of QKD in 6G communications network as well as its future directions.

## Abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| BB84 | Bennett-Brassard 1984 Protocol |
| CV-QKD | Continuous-Variable Quantum Key Distribution |
| ETSI | European Telecommunications Standards Institute |
| IoT | Internet of Things |
| MDI-QKD | Measurement-Device-Independent Quantum Key Distribution |
| NFV | Network Function Virtualization |
| NIST | National Institute of Standards and Technology |
| PRISMA | Preferred Reporting Items for Systematic Reviews and Meta-Analyses |
| PQC | Post-Quantum Cryptography |
| QKD | Quantum Key Distribution |
| RQ | Research Question |
| SDN | Software-Defined Networking |
| SLR | Systematic Literature Review |
| 6G | Sixth-Generation Wireless Communication System |
| URLLC | Ultra-Reliable Low-Latency Communication |

## Author Contributions

Abel Channie Demeke is the sole author. The author read and approved the final manuscript.

## Conflicts of Interest

There is no conflict of interest in this SLR.

## Appendix: Sample Study Classification Table

***Table 4.*** *Sample Study Classification.*

| Study | Year | Method | RQ Focus |
|---|---|---|---|
| Diamanti et al. | 2016 | Theoretical | RQ1 |
| Zeydan et al. | 2025 | Architecture | RQ2 |
| Sun et al. | 2019 | Framework Dev | RQ3 |
| McNeely | 2024 | Review | RQ3 |

| Study | Year | Method | RQ Focus |
|---|---|---|---|
| Bedington et al. | 2017 | Empirical | RQ1 |
| Guo et al. | 2021 | Analysis | RQ2 |
| Mao et al. | 2018 | Simulation | RQ3 |
| Ye et al. | 2019 | Prototype | RQ3 |
| Kim et al. | 2020 | Empirical | RQ3 |
| Tarantino et al. | 2018 | Architecture | RQ2 |

## References


[1] Diamanti, E., Lo, H.-K., Qi, B., & Yuan, Z. (2016).Practical challenges in quantum key distribution. npj Quantum Information, 2, 16025. https://doi.org/10.1038/npjqi.2016.25

[2] Primaatmaja, I. W., Curty, M., & Lim, C. C. W. (2022).Security of device-independent quantum key distribution protocols: A review. arXiv preprint, arXiv:2206.04960.

[3] Huawei Technologies Co., Ltd. (2024).6G native trustworthiness. White paper / technology report.

[4] Zeydan, E., Yanikomeroglu, H., & Oktug, S. (2025).Quantum technologies for beyond 5G and 6G networks. arXiv preprint, arXiv:2504.17133.

[5] Centre Tecnològic de Telecomunicacions de Catalunya (CTTC). (2025).Quantum key distribution for security in open and disaggregated 6G networks. Project report.

[6] International Telecommunication Union – Telecommunication Standardization Sector (ITU-T). (2020).Recommendation ITU-T Y.3800: Overview on networks supporting quantum key distribution.

[7] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., et al. (2019).Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236.DOI: https://doi.org/10.1364/AOP.361502(Originally circulated as arXiv:1906.01645)

[8] Al-Ghamdi, A., Al-Dhaifallah, M., & Al-Qahtani, S. (2020). On the security and confidentiality of quantum key distribution. Security and Privacy, 3(5), e111. https://doi.org/10.1002/spy2.111

[9] Bedington, R., Arrazola, J. M., & Ling, A. (2017).Progress in satellite quantum key distribution. npj Quantum Information, 3, 30. https://doi.org/10.1038/s41534-017-0031-5

[10] Kjwan, A. A. H. (2024).Adaptive covert communication framework for 6G networks. International Journal of Computational and Electronic Aspects in Engineering, 5(4), 203–213.

[11] Trinh, P. V., Nguyen, D. H., & Dang, T. K. (2023).The quantum internet. IET Quantum Communication. https://doi.org/10.1049/qtc2.12042

[12] Sun, S., Zhang, Y., & Wang, X. (2019).A blockchain-based framework for secure quantum key distribution communications in 6G networks. Future Networks, 12(1), 45–60.

[13] Primaatmaja, I. W., Curty, M., & Lim, C. C. W. (2022).Security of device-independent quantum key distribution protocols: A review. arXiv preprint, arXiv:2206.04960.

[14] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., et al. (2019).Advances in quantum cryptography. arXiv preprint, arXiv:1906.01645.

[15] Bedington, R., Arrazola, J. M., & Ling, A. (2017).Progress in satellite quantum key distribution. arXiv preprint, arXiv:1707.03613.

[16] [Wang, Y. (2025).Research on the design and application of 6G communication network architecture based on quantum key encryption. Applied and Computational Engineering, 119, 1–8.

[17] Centre Tecnològic de Telecomunicacions de Catalunya (CTTC). (2025).Quantum key distribution for security in open and disaggregated 6G networks. Technical Report.

[18] Kjwan, A. A. H. (2024).Adaptive covert communication framework for 6G networks integrating quantum cryptography and AI-augmented physical layer security. International Journal of Computational and Electronic Aspects in Engineering, 5(4), 203–213.

[19] Trinh, P. V., Nguyen, D. H., & Dang, T. K. (2023).The quantum internet: A synergy of quantum information technologies and 6G networks. IET Quantum Communication. https://doi.org/10.1049/qtc2.12042

[20] Nguyen, V.-L., Lin, X., & Nguyen, D.-T. (2021).Security and privacy for 6G: A survey on prospective technologies and challenges. arXiv preprint, arXiv:2108.11861.

[21] Bhatt, S., Mishra, D., & Verma, A. (2024).Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions. Future Generation Computer Systems, 160, 1–15. https://doi.org/10.1016/j.future.2023.12.015

[22] Yaacoub, E., & Alouini, M. S. (2019).A key 6G challenge and opportunity—Connecting the remaining 4 billions: A survey on rural connectivity. arXiv preprint, arXiv:1906.11541.

[23] Sun, Y., Zhang, L., Feng, G., Yang, B., Cao, B., & Imran, M. A. (2019).Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment. IEEE Internet of Things Journal, 6(5), 5791–5802. https://doi.org/10.1109/JIOT.2019.2916715

[24] Dorri, A., Kanhere, S. S., & Jurdak, R. (2016).Blockchain in Internet of Things: Challenges and solutions. arXiv preprint, arXiv:1608.05187.

[25] National Institute of Standards and Technology (NIST). (2017). Post-quantum cryptography. NISTIR 8105.

[26] Bernardo, L., Malta, S., & Magalhães, J. P. (2025).An evaluation framework for cybersecurity maturity aligned with the NIST cybersecurity framework. Electronics, 14(7), 1364. https://doi.org/10.3390/electronics14071364

[27] European Telecommunications Standards Institute (ETSI). (2017). ETSI GR QSC 006 V1.1.1: Quantum-safe cryptography; Limits to quantum computing applied to symmetric key sizes.

[28] McNeely, D. (2024).Transitioning to quantum-safe encryption. Delinea White Paper.

[29] Open Quantum Safe. (2024).Software for the transition to quantum-resistant cryptography.

[30] Clancy, T. C., et al. (2019).Post-quantum cryptography and 5G security: Tutorial. Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks. https://doi.org/10.1145/3317549.3319721

[31] Toshiba Europe. (2025).Secure 'quantum messages' sent over telecoms network in breakthrough. Financial Times.

[32] Liao, S.-K., et al. (2017).Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. Nature Photonics, 11(8), 509–513. https://doi.org/10.1038/nphoton.2017.116

[33] Wang, J.-Y., et al. (2013).Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. Nature Photonics, 7(5), 387–393. https://doi.org/10.1038/nphoton.2013.89

[34] Bouchard, F., et al. (2018).Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. Quantum, 2, 111. https://doi.org/10.22331/q-2018-11-05-111

[35] Heim, B., et al. (2014).Atmospheric continuous-variable quantum communication. New Journal of Physics, 16(11), 113018. https://doi.org/10.1088/1367-2630/16/11/113018

[36] Guo, H., et al. (2021).A survey on space-air-ground-sea integrated network security in 6G. IEEE Communications Surveys & Tutorials, 24(1), 53–87. https://doi.org/10.1109/COMST.2021.3123396

[37] Inoue, K. (2006).Quantum key distribution technologies. IEEE Journal of Selected Topics in Quantum Electronics, 12(4), 888–896. https://doi.org/10.1109/JSTQE.2006.877173

[38] Tarantino, S., et al. (2018).Feasibility of quantum communications in aquatic scenario. IEEE Photonics Conference Proceedings, 1–2. https://doi.org/10.1109/IPCon.2018.8527214

[39] Zhang, Y. H., et al. (2019).Robust and universal seamless handover authentication in 5G HetNets. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2019.2921875

[40] Fernández-Caramés, T. M. (2019).From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet of Things Journal, 7(7), 6457–6480. https://doi.org/10.1109/JIOT.2019.2958788

[41] Mao, Q., et al. (2018). Deep learning for intelligent wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 20(4), 2595–2621. https://doi.org/10.1109/COMST.2018.2846401

[42] Ye, N., et al. (2019).Deep learning aided grant-free NOMA toward reliable low-latency access in tactile Internet of Things. IEEE Transactions on Industrial Informatics, 15(5), 2995–3005. https://doi.org/10.1109/TII.2018.2883279

[43] Kim, W., et al. (2020). Deep neural network-based active user detection for grant-free NOMA systems. IEEE Transactions on Communications, 68(4), 2143–2155. https://doi.org/10.1109/TCOMM.2019.2963311

[44] Liu, Y.-J., et al. (2020). Device association for RAN slicing based on hybrid federated deep reinforcement learning. IEEE Transactions on Vehicular Technology, 69(12), 15731–15745. https://doi.org/10.1109/TVT.2020.3034179

[45] Gundu, S. R., et al. (2022).Sixth-generation (6G) mobile cloud security and privacy risks for AI systems using high-performance computing. Wireless Communications and Mobile Computing, 2022, 4397610. https://doi.org/10.1155/2022/4397610

[46] 3GPP. (2024).TS 33.210 V18.1.0: Network Domain Security (NDS); IP Network Layer Security (Release 18).