Advancing Security for 6G Smart Networks and Services

Madhusanka Liyanage*, Pawani Porambage† Engin Zeydan‡, Thulitha Senavirathne§,
Yushan Siriwardhana¶, Awaneesh Kumar Yadav‖, Bartlomiej Siniarski**
*§¶‖School of Computer Science, University College Dublin, Ireland, †VTT Technical Research Centre, Finland
‡Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain, ¶CWC, University of Oulu, Finland
Email: *madhusanka@ucd.ie, †pawani.porambage@vtt.fi, ‡engin.zeydan@cttc.cat,
§thulitha.senevirathna@ucdconnect.ie, ¶yushan.siriwardhana@oulu.fi, ‖**bartlomiej.siniarski@ucd.ie

***Abstract*—6G Smart Networks and Services are poised to shape civilization's development of 2030's world, supporting the convergence of digital and physical worlds. The arrival of 6G networks brings unprecedented challenges and opportunities, requiring robust security measures to safeguard against emerging threats. Thus, several complementary issues must be addressed to advance the security of 6G smart networks and services. This research paper explores a multi-faceted approach to 6G security, addressing key areas of security of 6G smart networks and services such as distributed trusted AI/ML, zero-touch holistic end-to-end (E2E) security, energy efficient security and privacy enablers, real-time resilience for timing-sensitive 6G software technologies and quantum-safe 6G communications. We comprehensively investigate the security and privacy challenges associated with integrating these technologies into 6G networks and their possible direction to mitigate them.**

I. Introduction

The evolution of communication technologies to 6G introduces new dimensions of connectivity and capabilities. However, with increased capabilities and advanced services comes the need for robust security measures. This research aims to propose a comprehensive security framework for 6G networks, addressing various challenges and leveraging advanced technologies.

6G networks, shaping civilization into the 2030s, will merge digital and physical worlds, enabling advanced applications like the metaverse and immersive communication. These networks will feature joint sensing, programmability, energy efficiency, trustworthiness, scalability, and affordability. However, their complexity requires a new approach to network management, and their advanced capabilities necessitate robust security against the expanding threat landscape. The strategic integration of AI/ML is pivotal for every layer of upcoming 6G networks, with applications in automated decision-making, enhancing network performance with intelligence decisions, ensuring zero-touch automation, and automated end-to-end security rely on AI integration in 6G. To enable such ubiquitous AI usage in 6G demands efficient data management solutions for collecting, processing, storing, and exposing information. Balancing the power of AI, laden with potentially private data, underscores the critical need for privacy and safety assurance. Quantifying the security and privacy impacts throughout the AI pipeline is a significant challenge. Thus, several complementary issues should be addressed to advance the security of 6G smart networks and services:

Exploitation of (distributed) trusted AI/ML for 6G infrastructures: 6G networks must secure the entire AI life cycle for predictable models and behaviours, addressing vulnerabilities during development and deployment, considering accountable AI measures, and implement protection mechanisms against potential misuse.

Zero-touch Integrated E2E Security Deployment for Adaptive Security: Securing 6G involves innovative approaches like Zero-touch and zero-trust frameworks while ensuring compliance with human-centric measures. These mechanisms should support E2E security by supporting a complete cycle of digital infrastructure resilience, i.e. threat identification, protection, detection, response, and recovery.

Innovative Enablers for Energy Efficient Security and Privacy : Enabling energy-efficient security and privacy in 6G could employ various techniques such as energy-efficient AI/ML architectures, multi-level security, spatial fragmentation, flexible profiling of resources and energy-efficient privacy-enhancing technologies. To promote green and sustainable AI methodologies by achieving energy efficiency in 6G network security mechanism design.

Real-Time Resilience using Adaptive Time Sensitive Software Technologies for 6G Service Provisions: 6G deployment involves timing-sensitive software and hardware for multi-stakeholder service provision. Designing adaptive security and privacy mechanisms for these Time-Sensitive Networks (TSNs) is important to support future 6G smart networks and services.

Quantum-Safe 6G Communications Securing 6G communications should be targeting on integrating Quantum key distribution and post-quantum cryptography for long-term network security, including challenges that could arise in a post-quantum era.

In the remaining sections, this paper discusses the above-mentioned prioritizing trusted AI, zero-touch security, energy-efficient measures, quantum-safe communications, and real-time resilience, which are vital for robust 6G network security.

II. Distributed and Trusted AI/ML for 6G

The use of AI and machine learning in 6G networks is pivotal but raises concerns about security. This section focuses on developing frameworks that ensure the security of the entire AI lifecycle. This involves addressing vulnerabilities in AI

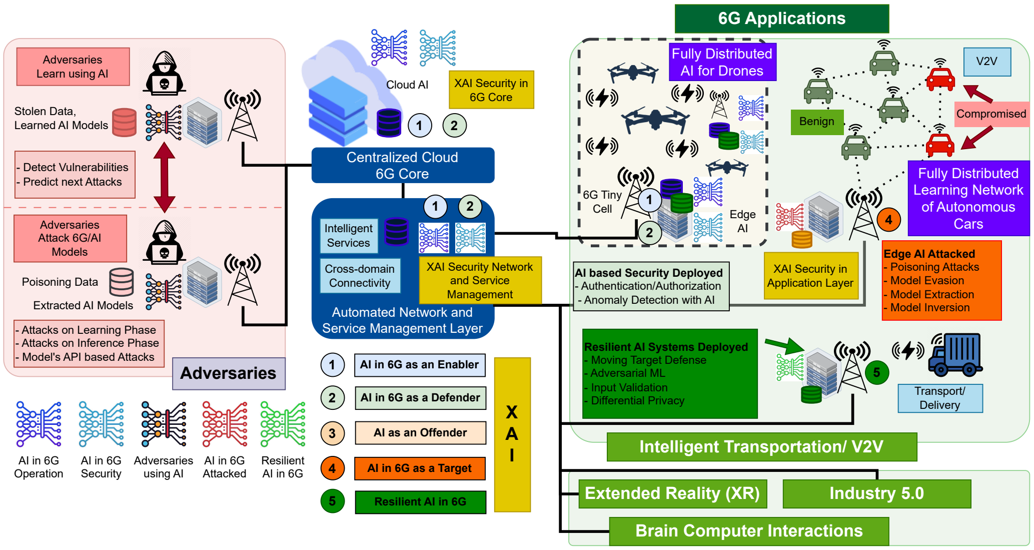


Fig. 1: Different roles of AI in 6G smart networks.

models, quantifying model vulnerability, and implementing protective measures against AI misuse.

A. AI's role as an Enabler, Defender, Offender, and a Target in 6G Smart Networks and Services

Fig. 1 depicts the application of distributed AI techniques in 6G networks and applications while highlighting the various roles AI plays in 6G service provisioning. The network-wide distributed deployment of AI techniques is integral to 6G, rather than confining it to server environments. In the 6G era, networks and applications utilize AI as an enabler for efficient service provision due to AI's ability to learn in complex environments and make accurate predictions. AI plays a vital role in 6G network security provision as a defender. The interconnection of complex networks in 6G that support applications with diverse requirements makes the security provision challenging. Proactive approaches, where the network can predict an attack based on the traffic behavior are required instead of conventional reactive approaches. AI's ability to uncover anomalies within large volumes of data can prevent the network and applications from zero-day attacks.

B. Federated AI/ML

Not only the network and application designers, but adversaries also gain access to AI. This defines the AI's role as an offender to the network where adversaries utilize AI as a tool to learn about the network and launch intelligent and adaptive attacks towards the 6G system. The adversaries can collect data about the network vulnerabilities using AI models and predict the most suitable points to attack for maximum impact. The distributed AI models deployed in 6G can also be a target for adversaries. In this case, the adversaries aim to attack the AI models and modify the output produced by the models to suit an attacker's objective. Data and model poisoning attacks, inference attacks, model inversion, and model evasion are some of the well-known attacks against AI systems [1]. Hence the AI systems should be designed with enhanced robustness and resilience against such attacks, ensuring that the true potential of AI benefits 6G service provision.

Adapting the distributed paradigm of AI/ML in the realm of 6G shifts the sole accountability away from centralized servers and disseminates it across several devices. Previously, centralized servers solely controlled the learning process, but now, multiple members have a say in the final model.

Federated AI/ML in 6G can span across several layers of the 6G architecture such as the edge layer, user equipment (UE) layer, and application layers. Edge computing provides the necessary infrastructure for decentralized AI/ML applications in 6G. This architecture, known as Edge AI, aims to improve bandwidth efficiency and reduce communication latency in the high-demand era of 6G. On the other hand, current AI/ML methods in 5G require large data storage spaces and computational resources to cater to the services of largely evolving heterogeneous UEs. Apart from the advantage of optimal usage of computing power, federated AI can also provide a layer of privacy to the users. Even with secure transmissions and regulatory requirements, the third-party AI/ML service providers could still be subjected to privacy leakages either from third-party attackers or the service providers themselves. Pertaining to proprietary rights, certain organizations are not too interested in sharing their data with cloud service providers. Also, sending data to cloud platforms for processing is an added cost to the organizations making edge/UEs viable in the business perspective.

C. Trust and accountability

In federated AI/ML, regardless of architectural differences, trust is crucial, particularly in applications like automated vehicle networking [2] and edge communication [3]. While FL enhances privacy, its expanded threat landscape due to device connectivity necessitates transparent decision-making for trustworthiness. Explainable Artificial Intelligence (XAI) is vital for security in Beyond 5G networks and is integral to FL applications' trust. XAI methods, including correlation analysis and data visualization, provide essential insights into training data, influencing AI/ML model development. This is particularly relevant for FL's diverse data types and structures.

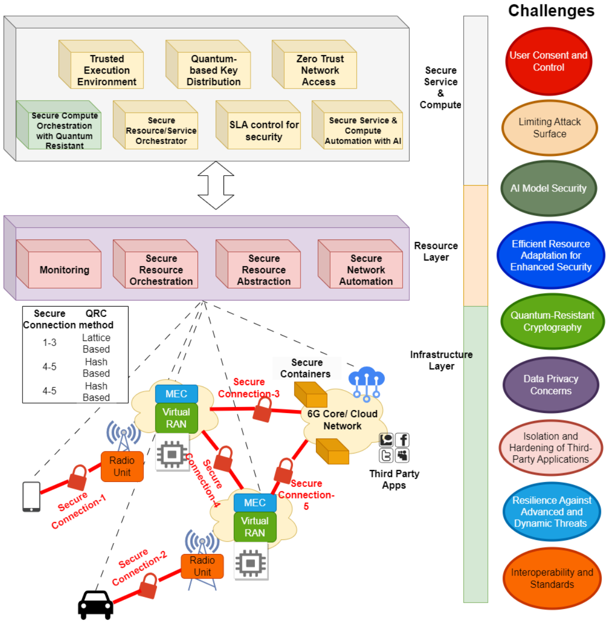
Aggregation in federated learning (FL) usually occurs in cloud or edge environments, with security depending on whether it's a Trusted Execution Environment. In trusted environments, the aggregator is generally secure, but in untrusted ones, FL faces risks from client-originated attacks like data poisoning. Detecting and isolating malicious elements in FL is feasible through XAI methods, such as identifying poisoned data in health devices or spotting abnormal data points. Continuous monitoring of the aggregator using XAI, especially in untrusted environments, is crucial. Techniques like SHAP are effective for detecting shifts in ML models, helping to counter evasion attacks [4], a significant threat in the Beyond 5G era.

III. Zero-touch Integrated E2E Security Deployment for Adaptive Security

The integration of AI, quantum technologies, and end-to-end security solutions provides a coherent framework for establishing an adaptable zero-touch security implementation that meets the unique challenges of highly distributed 6G environments [5]. As illustrated in Fig. 2, there are many challenges in the context of highly distributed and virtualized 6G environments such as quantum-resistant cryptography, privacy concerns, user consent and control, resilience to advanced threats, AI model security, interoperability and standards. The design and implementation of adaptive ciphers, post-quantum cryptographic algorithms, robust model validation and testing protocols, data anonymization and encryption techniques, and mechanisms to isolate and secure third-party applications or attack surface limitations can play a crucial role in the zero-trust integration of adaptive E2E security.

A. Enhanced Security Mechanisms in 6G Environments

The distributed and virtualized nature of 6G environments introduces new challenges in securing the network. Strategies such as network segmentation, microsegmentation, and dynamic network policies are essential in minimizing the attack surface for network orchestration. AI-driven anomaly detection plays a crucial role in continuously monitoring network activity to identify and isolate potential threats. The integration of quantum-resistant security protocols into zero-touch security orchestrators is vital for reducing vulnerabilities by strengthening communication channels against quantum-based attacks [6]–[8]. Additionally, with the increasing reliance on third-party applications in 6G ecosystems, implementing robust mechanisms to isolate and secure these applications is imperative. Quantum-safe algorithms are crucial in protecting against quantum threats. Technologies like containerization (e.g., Docker, Kubernetes), hardware-based isolation mechanisms (e.g., Intel SGX, AMD SEV), and Trusted Execution Environments (e.g., Intel SGX, ARM TrustZone) create secure execution environments. These are complemented by dynamic sandboxing and AI-powered behavioral analytics for granular control over applications, and blockchain-based application isolation with a Zero Trust Network Access approach for managing permissions and continuously verifying identities.



Challenges
Trusted Execution Environment
Quantum-based Key Distribution
Zero Trust Network Access
Secure Compute Orchestration with Quantum Resistant
Secure Resource/Service Orchestrator
SLA control for security
Secure Service & Compute Automation with AI
Secure Service & Compute
Monitoring
Secure Resource Orchestration
Secure Resource Abstraction
Secure Network Automation
Resource Layer
Infrastructure Layer
Secure Connection QRC method
1-3 Lattice Based
4-5 Hash Based
4-5 Hash Based
MEC
Virtual RAN
Radio Unit
Secure Connection-1
Secure Connection-2
Secure Connection-3
Secure Connection-4
Secure Connection-5
Secure Containers
6G Core/ Cloud Network
Third Party Apps
User Consent and Control
Limiting Attack Surface
AI Model Security
Efficient Resource Adaptation for Enhanced Security
Quantum-Resistant Cryptography
Data Privacy Concerns
Isolation and Hardening of Third-Party Applications
Resilience Against Advanced and Dynamic Threats
Interoperability and Standards

Fig. 2: The orchestration approach based on Zero Trust integrated into a mobile network infrastructure and corresponding security and privacy challenges.

B. Adaptive Security and Resource Optimization in 6G

An essential aspect of securing 6G networks involves the development and implementation of adaptive ciphers [9]. These ciphers dynamically adapt encryption algorithms and key management protocols in response to the evolving threat landscape. Utilizing AI algorithms, adaptive ciphers continuously evaluate network conditions, traffic patterns, and potential vulnerabilities to optimize encryption strategies in real-time. This proactive approach is critical for maintaining a robust defense against sophisticated cyberattacks. Furthermore, AI algorithms are central in the dynamic allocation of security resources, ensuring optimal protection without compromising network performance. Quantum-based key distribution mechanisms [10] contribute to resource efficiency by providing secure communication channels with reduced computational overhead. Efficient orchestrator design is key to balancing security measures with available resources, optimizing the trade-off between security and operational efficiency in 6G networks.

IV. Real-Time Resilience using Adaptive Time Sensitive Software Technologies for 6G

Time synchronization is crucial for the efficient operation of deterministic communication systems, ensuring seamless integration between the physical and digital worlds. For example, autonomous vehicles rely on exact time alignment to operate safely and efficiently. This necessity extends to all network notes, which require access to a shared time reference to support various time-sensitive applications. Firstly, it's essential for network nodes to synchronize with one another with high accuracy and precision. This synchronization enables the execution of time-triggered operations in line with a globally coordinated schedule. Secondly, applications at the endpoints must also be time-aware, undertaking specific actions at predetermined moments. In the context of 6G networks, the importance of time synchronization is amplified due to the expected increase in network speed and capacity.

A. Challenges and Solutions for Time-Synchronization in 6G

With 6G's potential to support more complex and time-critical applications, such as advanced autonomous systems and IoT devices, maintaining precise time alignment becomes even more critical. 6G technology is expected to facilitate ultra-low-latency interactions crucial for critical applications, notably in industrial automation. This advancement necessitates the implementation of highly accurate and swift time synchronization mechanisms. Essential to this process is the incorporation of end-to-end (E2E) security measures, which rely on precise monitoring and rapid response capabilities to effectively implement countermeasures against potential threats. A challenge in this setup is that network monitoring, while essential for security, tends to introduce additional latency. It is crucial that this added latency remains minimal to ensure it does not compromise the stringent timing guarantees required for effective communication in these applications. The future of E2E deterministic networks is likely to continue leveraging standards like TSN or Deterministic Networking (DetNet), traditionally used in secure, controlled environments to mitigate exposure to external threats. Due to the strict timing requirements of TSN/DetNet, potential vulnerability points will be introduced in an integrated 6G-TSN network. For instance, the need for accurate time synchronization in a TSN network makes DoS attacks very effective, e.g., a time-critical flow can be disrupted by a long PTP outage, slowDoS-type attacks can be sufficient to disrupt sensitive applications [11]. These attacks are difficult to be detected with traditional signature-based intrusion detection approaches, even more when the HTTP traffic is encrypted. However, the landscape for 6G systems is significantly different, characterized by open and heterogeneous networking technologies spanning various sectors. This openness increases the vulnerability to external attacks, such as jamming, device impersonation, and the introduction of compromised or fake nodes. Such threats can have immediate and significant impacts on time synchronization, determinism, packet delivery, and overall network consistency.

B. Future landscape and security enablers

To effectively address these challenges, a comprehensive 'security by design' strategy is essential. This strategy includes implementing Zero-touch network and Service Management (ZSM) for an automated, end-to-end security management process. Through the integration of ZSM, 6G networks are positioned to significantly improve their resilience and adaptability. This integration is crucial for meeting the high standards of performance and reliability expected of these networks, while also upholding robust security protocols in a complex and vulnerable digital environment. This approach is critical in meeting the requirements of Cyber-Physical Systems (CPS) applications and support dynamic network changes.

Furthermore, 6G systems are set to adopt even greater adaptability in terms of application operation modes. This means applications will have the capacity to adjust their operational modes dynamically, aligning with real-time network conditions and specific application needs. Such flexibility is key to promptly adapting to fluctuating scenarios, thereby ensuring consistent and robust support for a range of CPS applications. This paradigm shift towards enabling deterministic communications within 6G systems hinges on a variety of technological advancements across different sectors of the communications and computing infrastructure.

Next-generation networks are addressing security challenges in time-sensitive communication with a multi-faceted approach. Machine learning algorithms will analyze system behavior for vulnerability prediction and network performance optimization. Digital twinning, creating virtual replicas of network components, allows for controlled behavior simulation. The integration of TSN and DetNet with wireless technology enhances reliability and flexibility for mobile applications in 6G networks. Emphasizing 'Security by Design', security features are integrated at the initial stages of network development, making security a fundamental part of the network architecture, essential for addressing sophisticated challenges in future networks.

Standards such as IEEE 802.1Q [12] (foundational TSN elements), 802.1Qbv [13] (TSN traffic scheduling), 802.1Qci [14] (filtering and plicing), 802.1CB [15] (reliability improvements) collectively form a comprehensive framework for implementing and managing TSN in various network environments, including the upcoming 6G networks, where the demand for low-latency and high-reliability communication is expected to increase significantly.

V. Innovative Enablers for Energy Efficient Security and Privacy

The focus on energy efficiency implies a concerted effort to minimize energy consumption or optimize resource usage within the 6G network infrastructure. This is crucial for sustainability and reducing the environmental impact of network operations. This is particularly important as networks become increasingly complex and resource-intensive and more emphasis is placed on the development of sustainable and eco-friendly communication and network technologies [16]. As summarized in Figure 3, this section explores technologies such as multi-level security, security segregation, and privacy quantization. It also shows how to enable efficient security and privacy measures, including multi-stakeholder moving target defense developments and rapid proactive security recovery techniques.

Multi-level security in a telecommunications network refers to the implementation of security measures at different levels

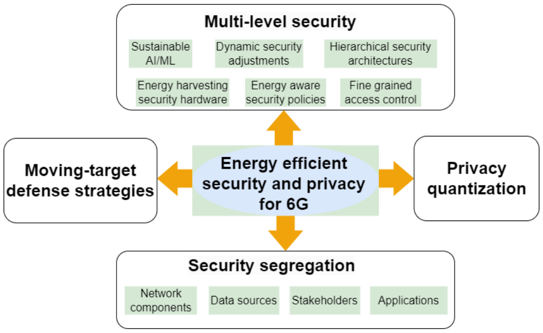

Multi-level security
Sustainable AI/ML
Dynamic security adjustments
Hierarchical security architectures
Energy harvesting security hardware
Energy aware security policies
Fine grained access control
Moving-target defense strategies
Energy efficient security and privacy for 6G
Privacy quantization
Security segregation
Network components
Data sources
Stakeholders
Applications

Fig. 3: Energy efficient security and privacy for 6G.

within the network infrastructure to protect against different types and levels of security threats. The concept is particularly relevant in environments such as 6G networks, where sensitive information, critical services and different stakeholders coexist. Implementing multi-level security with a focus on energy efficiency involves combining security measures at different levels of the network architecture while optimizing energy consumption [17]. Key aspects of multi-level security in 6G networks may include various security measures with adaptive authentication and authorization and also selective data encryption techniques; the use of sustainable AI/ML algorithms for security operations; the adoption of energy-aware security policies; and compliance with industry regulations; distributed security measures with dynamic security adjustments; energy-efficient security devices or energy harvesting for security devices; zero-trust security models with fine-grained access control; hierarchical security architectures and security levels that have a network of networks with edge-level security.

In the context of 6G networks, security segregation refers to the practice of dividing and isolating different components, data sources, applications, stakeholders, functions or entities within the network architecture to enhance security. The aim is to increase security by creating boundaries and controlling interactions between different entities within the 6G echo system. Energy-efficient security segregation in 6G networks involves implementing measures to separate and protect different levels of network resources and data while optimizing energy consumption. This approach aims to improve security without compromising the overall energy efficiency of the network, e.g. through dynamic and context-aware segmentation and resource-aware security policies. Novel techniques such as privacy quantization have also attracted a lot of attention in the 6G research community to improve privacy while increasing energy efficiency. In the application of differential privacy in federated learning, for example, the use of quantization proves to be a key technique for reducing the information encoded over the original input. An interesting question is to explore whether the introduction of randomization in quantization schemes can effectively optimize the trade-off between privacy preservation and model accuracy in the context of differentially private federated learning [18].

The focus of the above-mentioned aspects of energy efficiency lies in enabling effective security and privacy measures in the 6G context. In some ways, they can be specifically addressed with the implementation of multi-stakeholder moving target defense evolutions, which are dynamic security approaches that adapt to evolving threats by frequently changing the attack surface [19]. In addition, work can be extended to the deployment of rapid, proactive security recovery techniques aimed at quickly detecting and addressing security incidents. Incorporating these strategies should improve the overall resilience and responsiveness of security mechanisms in the 6G network environment and ensure energy efficiency.

VI. Quantum-Safe 6G Communications

The proliferation of Internet of Things (IoT) devices is expected to increase significantly due to the services offered by 6G. The security and privacy of the 6G core network will be closely linked to the security of IoT devices and their protection mechanisms [20]. In the current landscape, researchers predominantly use either symmetric or asymmetric encryption approaches to secure communications. The security of asymmetric encryption is based on the assumption of the hardness of factorization and discrete logarithm problems. However, Shor [21] has shown that post-quantum computers have the ability to solve these problems efficiently. Consequently, existing security mechanisms based on factorization and discrete logarithm problems, such as RSA and ECC, may be insufficient for ensuring communication security. Furthermore, Grove's findings indicate that small key sizes in existing symmetric algorithms such as SNOW 3G, AES and ZUC are also vulnerable to quantum attacks [22]. In the 5G specification, symmetric algorithms such as SNOW 3G, AES and ZUC use 128-bit keys for both encryption and message integrity. In the post-quantum world, however, these key lengths are considered insufficient due to the Grover algorithm, which requires doubling the key lengths of symmetric primitives. Therefore, symmetric cryptography with at least 256-bit keys must be implemented for future 6G networks in order to maintain the current level of security against quantum attacks. Fortunately, block ciphers such as AES remain secure and applicable in this context. The same applies to modern cryptographic hash functions such as SHA-2 and SHA-3. This revelation is a crucial signal for security researchers to start exploring alternative cryptographic solutions, considering the potential impact of quantum computing on the security landscape for 6G communications [23].

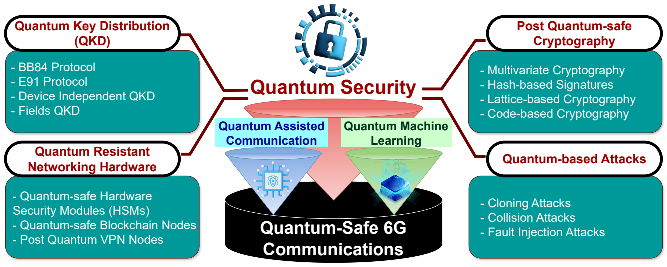

Quantum Key Distribution (QKD)
- BB84 Protocol
- E91 Protocol
- Device Independent QKD
- Fields QKD
Quantum Resistant Networking Hardware
- Quantum-safe Hardware Security Modules (HSMs)
- Quantum-safe Blockchain Nodes
- Post Quantum VPN Nodes
Quantum Security
Quantum Assisted Communication
Quantum Machine Learning
Quantum-Safe 6G Communications
Post Quantum-safe Cryptography
- Multivariate Cryptography
- Hash-based Signatures
- Lattice-based Cryptography
- Code-based Cryptography
Quantum-based Attacks
- Cloning Attacks
- Collision Attacks
- Fault Injection Attacks

Fig. 4: Quantum-Safe 6G Communications.

Different types of post-quantum cryptography algorithms and approaches have so far been developed to counter the threat posed by quantum computers to classical encryption methods. These post-quantum cryptographic methods can be categorized into different families based on their mathematical foundations and techniques. Here are some of the major types of post-quantum cryptography such as lattice-based cryptography, code-based cryptography, multivariate cryptography, and hash-based cryptography. Figure. 4 discusses the components of quantum-safe 6G communications. On the other hand, there are currently no secure post-quantum cryptographic algorithms that can provide both very small keys and compact ciphertexts/signatures while ensuring efficient key generation, encryption and decryption or signing and verification processes. In the transition from today's asymmetric primitives to safe post-quantum alternatives, trade-offs are unavoidable. Such replacements inevitably involve costs that affect either the communication or the operational efficiency of the network. It is imperative to conduct further research to determine the optimal application of secure post-quantum cryptography and to ensure compliance with the envisioned performance and functionality of the 6G architecture. Striking the right balance between security and operational efficiency will be critical when it comes to adapting cryptographic solutions to the evolving landscape posed by the challenges of quantum computing for 6G communications.

VII. Conclusion

In conclusion, this research paper proposes a comprehensive framework for 6G security that considers various dimensions, including AI/ML for intelligent threat detection and mitigation, E2E security to address vulnerabilities across the entire communication network, efficient enablers to optimize resource allocation and usage, zero-touch deployment for seamless and secure network setup, quantum technologies for advanced encryption methods, time-sensitive software to ensure real-time responsiveness, and privacy considerations to safeguard user data. The detailed integration of these elements aims to create not just a robust but also a resilient and provable security foundation for the next generation of communication networks. By exploring these key areas and addressing the intricate interplay between them, we pave the way for a secure and resilient foundation for the future of 6G networks.

Acknowledgement

This work is supported by following projects: Robust-6G funded by Eropean Union (Grant ID. 101139068); Science Foundation Ireland under CONNECT phase 2 (Grant no. 13/RC/2077_P2); XcARet funded by Research Council of Finland, "ERDF A way of making Europe" project funded by MCIN/AEI/ 10.13039/501100011033 under Grant PID2021-126431OB-I00 and Spanish MINECO - Program UNICO I+D (grants TSI-063000-2021-54 and -55).

References

[1] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, pp. 616–621.

[2] A. Renda, P. Ducange, F. Marcelloni, D. Sabella, M. C. Filippou, G. Nardini, G. Stea, A. Virdis, D. Micheli, D. Rapone *et al.*, "Federated learning of explainable ai models in 6g systems: Towards secure and automated vehicle networking," *Information*, vol. 13, no. 8, p. 395, 2022.

[3] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[4] G. Fidel, R. Bitton, and A. Shabtai, "When explainability meets adversarial learning: Detecting adversarial examples using shap signatures," in *2020 international joint conference on neural networks (IJCNN)*. IEEE, 2020, pp. 1–8.

[5] A. Hummelholm, T. Hämäläinen, and R. Savola, "Ai-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks," in *Proceedings of the European Conference on Cyber Warfare and Security*. Academic Conferences International, 2023.

[6] E. Zeydan, J. Baranda, and J. Mangues-Bafalluy, "Post-quantum blockchain-based secure service orchestration in multi-cloud networks," *IEEE Access*, vol. 10, pp. 129 520–129 530, 2022.

[7] L. Malina, P. Dobias, J. Hajny, and K.-K. R. Choo, "On deploying quantum-resistant cybersecurity in intelligent infrastructures," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–10.

[8] E. Zeydan, Y. Turk, B. Aksoy, and Y. Y. Tasbag, "Post-quantum era in v2x security: Convergence of orchestration and parallel computation," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 76–82, 2022.

[9] S.-C. Lin, K.-C. Chen, and A. Karimoddini, "Sdvec: Software-defined vehicular edge computing with ultra-low latency," *IEEE Communications Magazine*, vol. 59, no. 12, pp. 66–72, 2021.

[10] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher *et al.*, "Quantum key distribution: a networking perspective," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.

[11] N. Garcia, T. Alcaniz, A. González-Vidal, J. B. Bernabe, D. Rivera, and A. Skarmeta, "Distributed real-time slowdos attacks detection over encrypted traffic using artificial intelligence," *Journal of Network and Computer Applications*, vol. 173, p. 102871, 2021.

[12] "Ieee standard for local and metropolitan area networks–bridges and bridged networks," *IEEE Std 802.1Q-2022 (Revision of IEEE Std 802.1Q-2018)*, 2022.

[13] "Ieee standard for local and metropolitan area networks – bridges and bridged networks - amendment 25: Enhancements for scheduled traffic," *IEEE Std 802.1Qbv-2015*, pp. 1–57, 2016.

[14] "Ieee standard for local and metropolitan area networks–bridges and bridged networks–amendment 28: Per-stream filtering and policing," *IEEE Std 802.1Qci-2017*, pp. 1–65, 2017.

[15] "Ieee standard for local and metropolitan area networks–frame replication and elimination for reliability," *IEEE Std 802.1CB-2017*, 2017.

[16] P. Porambage and M. Liyanage, *Security and Privacy Vision in 6G: A Comprehensive Guide*. John Wiley & Sons, 2023.

[17] P. Porambage, J. Pinola, Y. Rumesh, C. Tao, and J. Huusko, "Xcaret: Xai based green security architecture for resilient open radio access networks in 6g," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2023.

[18] N. Lang, E. Sofer, T. Shaked, and N. Shlezinger, "Joint privacy enhancement and quantization in federated learning," *IEEE Transactions on Signal Processing*, vol. 71, pp. 295–310, 2023.

[19] T. Zhang, C. Xu, P. Zou, H. Tian, X. Kuang, S. Yang, L. Zhong, and D. Niyato, "How to mitigate ddos intelligently in sd-iov: a moving target defense approach," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1097–1106, 2022.

[20] J. Partala, "Post-quantum cryptography in 6g," *6G Mobile Wireless Networks*, pp. 431–448, 2021.

[21] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[22] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[23] G. G. Rozenman, N. K. Kundu, R. Liu, L. Zhang, A. Maslennikov, Y. Reches, and H. Y. Youm, "The quantum internet: A synergy of quantum information technologies and 6g networks," *IET Quantum Communication*, vol. 4, no. 4, pp. 147–166, 2023.