Chapter 76
Security and Privacy Mechanisms for 6G Internet of Everything Networks in Banking

Ilgin Safak
https://orcid.org/0000-0002-2788-7276
Fibabanka R&D Center, Istanbul, Turkey

Fatih Alagöz
Boğaziçi University, Computer Engineering Department, Istanbul, Turkey

Emin Anarım
https://orcid.org/0000-0002-3305-7674
Boğaziçi University, Electrical and Electronics Engineering Department, Istanbul, Turkey

ABSTRACT

6G, as a platform for the internet of everything, supports high data rates and low latency and satisfies the requirements for services, massive data traffic, storage, and processing, thus providing new opportunities for accessing consumer goods and digital services. Due to its enhanced autonomy, accuracy, and predictive capabilities, artificial intelligence (AI) is anticipated to play a significant role in the evolution of 6G by enabling large-scale deployments of self-optimized and automated systems, and enhancing applications and services, including augmented/virtual/mixed reality, Industry 5.0, banking, and financial services. 6G and AI can potentially revolutionize the banking and financial industry despite cost, scalability, security, privacy, and adoption constraints. This chapter discusses security and privacy concerns in 6G and potential solutions, the relevance and impact of 6G technology to the banking and financial industry, solutions and recommendations for developing secure 6G banking and financial systems, and future research directions.

INTRODUCTION

6G wireless telecommunications technology, still under development, is expected to be operational in the early 2030s. In addition to SHF (3-30 GHz) and EHF (mm-waves) bands employed in 5G, EHF (30-300 GHz) and THz (300-3000 GHz) frequency bands are likely to be used in 6G (Akyildiz, C. Han, Nie, & Jornet, 2022). Much larger transmission bandwidths available in EHF and THz bands will improve the

DOI: 10.4018/978-1-6684-7366-5.ch076

capabilities of 6G. This leads to dramatically higher data rates in 6G, especially for indoor and short-range cellular links. However, free space, atmospheric and precipitation losses also increase rapidly with increasing frequencies. Therefore, outdoor communication links in 6G may need higher margins for reliable operation. Increased gains of transmit and receive antennas in these bands can compensate for these losses and allow operation at reasonable transmit power levels (Jiang, Han, Habibi, & Schotten, 2021).

Optical bands, an option for 6G, also offer high data rates, better resolution, robustness to interference, and inherent security. As in EHF and THz bands, optical waves cannot penetrate walls and suffer large atmospheric and precipitation losses. In addition to indoor-based systems, optical links may also be suitable for short-range outdoor communications such as vehicle-to-vehicle communications (Akhtar, et al., 2020). Since 6G systems must have line-of-sight (LOS) and short ranges, base stations are expected to be more densely located than 5G systems.

Utilization of artificial intelligence (AI), augmented/virtual reality (AR/VR), blockchain, robotics, THz band communications, molecular communication, vortex millimeter waves, and quantum communication can drastically improve the performance of 6G systems (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). Vortex millimeter waves, due to rapidly changing spins, enable transmission at extremely fast data rates. Due to dramatic improvements over 5G, 6G is expected to enable people to enjoy consumer goods and digital services equally. 6G is not just about increased data rates, but also about a major shift in networks driven by quantum technology advances. Architectural designs are being transformed by technological advances in quantum devices. Note that quantum computers are still in the early stages of development, hardware is limited and architecture is uncertain. However, as quantum computers become more powerful, quantum software is expected to play a more significant role (Tripathi, Sabu, Gupta, & Dhillon, 2021).

Parallelism inherent in quantum communication networks increases capacity and security (Chehimi & Saad, 2021). Transferring quantum bits is a key component of quantum computing and communications. In a quantum computing network, quantum bits, or qubits, are fundamental units of data transmission. Qubits differ from standard computing bits in that they can take multiple values, including 0 and 1, at the same time. Qubits are transferred over a channel using quantum entanglement. Multiple qubits are entangled together and can be linked over longer distances. Quantum memory preserves a photon's quantum state without destroying the quantum information it carries. Quantum memory releases a photon with the same quantum state as the stored photon after a predetermined period of time (Brennen, Giacobino, & Simon, 2015). This is critical in quantum communications.

In standard cryptographic practices, data transmitted over the Internet is secured by posing a difficult-to-solve mathematical problem or algorithm. An attacker can see all the protected information if it solves this problem. Quantum cryptography, on the other hand, operates differently. As a result of entanglement, any attempt to gain access to protected information alters the cryptographic formula. This can easily be detected by communicating peers. Therefore, quantum cryptography significantly increases data security compared to standard cryptography (Muheidat, Dajania, & Tawalbeh, 2022).

6G anticipates the realisation of the Internet of Everything (IoE), which entails the interconnectivity of people, processes, data, and things, a concept much broader than the traditional Internet of Things (IoT), to enhance efficiency, productivity, and decision-making. This creates a highly interconnected network in which virtually all elements of the digital and physical world can communicate, interact, and exchange information. Not only do these include devices and sensors, but also individuals, applications, and contextual data associated with objects. Customer data plays a critical role in the IoE, enabling personalized experiences, optimizing services, and enabling seamless interactions across intercon-

nected devices, people, and processes. Due to the increased threat surface of IoE, a heightened level of responsibility is required in terms of data privacy and security to ensure customers' trust. However, due to resource constraints, not all IoE devices can afford complex cryptography to maintain strong security, making them a primary target for attackers. In addition, the deployment of keys and the performance of management functions are more difficult in large networks. Compromise of these devices could allow cyber-attacks resulting in data location, and identity theft (V. -L. Nguyen, 2021).

A decentralized approach, using distributed ledger technology (DLT) such as blockchain, could eliminate single points of failure and enhance the security of 6G IoE networks, characterized by private and public sensors, devices, sub-networks, and hybrid cloud systems. DLT is an ideal solution for storing and exchanging trust information, as well as supporting dynamic roaming policies and contract updates through smart contracts. Smart contracts are software programs that run on a blockchain if a predetermined condition is met. Blockchain and smart contracts are proven technologies for decentralized resource management, workflow automation in massively large and distributed networks, spectrum sharing, and service management (Hakeem, Hussein, & Kim, 2022). DLT procedures enable a key maintenance lifecycle of update, expiration, and refresh. By leveraging the ubiquitous edge cloud as an extension of its computing, battery, and software capabilities, 6G will usher in an era of flexible devices and sensors that can better respond to application needs. Observed device behavior can be utilized to build and share trust information through DLT, as the network manager fingerprints and creates reports of registered device behavior that deviates from accepted policy. These reports, stored in the DLT, cannot be modified by malicious users. Based on past behavior reports securely recorded in the DLT, a network can establish a level of trust and access for a device. Edge cloud providers can then use this trust information to determine the privileges and resources provided to a device based on the trust information. However, limitations and challenges still exist in terms of dynamic management, latency, scalability, as well as for cooperative transmission among multiple access points and multi-hop data brokerage (Ziegler, et al., 2021).

However, blockchains and smart contracts also present security and privacy concerns, if transaction data and the logic behind smart contracts of publicly stored data are leaked. Additionally, the blockchain stability may be undermined by the so-called 51% attacks that imply that malicious users gain control over 51 percent of the blockchain nodes. Blockchain systems with majority voting are vulnerable to 51% attacks since attackers can modify the transaction history and prevent future official transactions confirmation. Sybil attacks, as a group of attackers attempt to capture a peer-to-peer blockchain network by establishing fake identifications, is expected to increase with 6G. Blockchain systems using restricted and automated member acceptance methods are more prone to these attacks. Blockchains and smart contracts are also prone to reentry attacks, which occur when a smart contract frequently contacts another smart contract that is vulnerable, and to double-spending attacks, which attempt to use a cryptographic token more than once (Hakeem, Hussein, & Kim, 2022).

AI, machine learning (ML) and big data analytics are valuable tools to make 6G systems more intelligent, and to enhance the security and privacy (Kommadi, 2023). Descriptive analytics is used to obtain perceptions of performance indicators, such as traffic profiles, channel states, and user viewpoints, based on historical data sets. Diagnostic analytics is employed to identify potential causes of network failures to improve future systems. Predictive analytics can be used in analyzing past cybersecurity threat intelligence data closely to predict future attacker behaviors and make predictions. Prescriptive analytics can be used to improve resource allocation, network virtualization, cache management, edge computing, and fog computing (V. -L. Nguyen, 2021).

Distributed and large-scale systems will use AI/ML techniques for a variety of use cases, including network management. This includes rapid control and analytics of the enormous volumes of generated data spatially pushed closer to the data source for lower latency while distributing ML functions across the network for improved performance through optimized models and ensemble decision-making (V. -L. Nguyen, 2021). However, IoT devices still have practical limitations, including computational limitations and intermittent connectivity. Distributed AI/ML may be effectively implemented in different phases of 6G's cybersecurity protection and defense to enable autonomy, accuracy, and predictive capabilities.

However, the alliance between 6G and AI may also be a double-edged sword in some cases, since AI can both protect and violate privacy and security. AI/ML systems may be compromised through poisoning attacks, data injection, data manipulation, logic corruption, model evasion, model inversion, model extraction, and membership inference attacks. AI/ML systems perform better against attacks when more data is collected. (Siriwardhana, Porambage, Liyanage, & Ylianttila, 2021).

Current 5G standards do not address security issues associated with quantum computing. Instead, they rely on traditional cryptography such as Elliptic Curve Cryptography. As the 6G era marks the presence of quantum computing, security mechanisms such as digital signatures and blockchain technology, which rely on asymmetric cryptography, like RSA and Elliptic Curve Cryptography, will become vulnerable to quantum computer-based attacks. As a result, asymmetric key cryptography cannot ensure the post-quantum security of 5G communications (Bernstein & Lange, 2017). These algorithms will need to be replaced or extended by quantum-safe variants. The most likely candidates are 6G Authentication and Key Agreement, quantum-secure cryptographic schemes, and physical layer security (Hakeem, Hussein, & Kim, 2022).

As AI is incorporated into the network, 6G will be able to support large-scale deployments of automated systems and enhance applications and services. For example, it is possible to establish a feedback loop between the wireless network system and the decision process by utilizing current AI mechanisms such as reinforcement and deep reinforcement learning. 6G wireless networks are anticipated to be self-configuring, self-monitoring, self-healing, and self-optimizing with minimal human intervention. However, the dynamicity, complexity, density, and heterogeneity of these networks make existing optimization mechanisms incompatible with them. A massive 6G network also presents serious challenges for existing mathematical optimization techniques (Siriwardhana, Porambage, Liyanage, & Ylianttila, 2021).

Advanced AI/ML technologies could also help diagnose and correct anomalies, self-healing, automatic resource allocation, channel estimation, attack prevention, network fault detection and optimize wireless networks not only at the physical layer but also at higher layers (Akbar, Hussain, Sheng, & Mukhopadhyay, 2022). IoE devices could perform additional AI functions and report them to the network to facilitate resource management decisions. In order to scale AI, algorithms will need to be developed and trained at different network layers, including application, transport, network, and physical layers. The implementation of AI-native and data-driven network architectures may be necessary within the network and management domains, possibly requiring data from multiple sources using edge intelligence (EI). EI is the acquisition, storage, or processing of data at the network edge using AI/ML algorithms. In an EI network, data is aggregated by an edge server that combines data generated by multiple associated devices. Several edge servers exchange data for training models, which are later analyzed and predicted (V. -L. Nguyen, 2021). This allows devices to benefit from faster feedback, reduced latency, and lower costs while enhancing their performance.

Advanced AI algorithms could also be applied to the metaverse. The metaverse refers to a virtual world that combines various aspects of digital technologies, including video conferencing, games, cryptocur-

rencies, AR/VR/mixed reality (MR), social media, and live streaming (Akyildiz, Guo, Dai, & Gerstacker, 2023). In the metaverse, users' actions in the real world are projected into the virtual world. This allows them to fully control their avatars and interact with other objects. A user could receive contextual and personalized AR/VR/MR experiences by accessing edge-based on-demand holographic content tailored to their circumstances and/or interests, for example, by using holographic content provisioning (M. Glushakov, 2020). Furthermore, avatars can interact with many real-world modes, including expressions, emotions, body movements, and physical interactions, as well as speech recognition and sentiment analysis powered by AI. 6G, AI, blockchain and technologies such as AR/VR/MR could revolutionize the metaverse through the widespread deployment of interconnected sensor networks. These networks include cameras, photodiodes, inertial sensors, time-of-flight sensors, ambient sensors, and biometric sensors (Maksymyuk, et al., 2022).

The integration of enabling technologies such as 6G, IoE, big data analytics, and blockchain with AI-based cognitive skills and innovation can improve production and deliver customized products faster to customers. Industry 5.0 provides a production model that focuses on man-machine interaction, which facilitates smart product development. The new 6G network architecture is expected to include banking communications technologies, quantum computing, AI, intelligent reflective surfaces, quantum teleportation, quantum encrypted messaging, 6G holography, distributed ledger technology, and the metaverse (Sejan, et al., 2022). The metaverse could revolutionize how we bank. Traditional banks could use the metaverse to compete against challenger banks and catch up on embedded finance innovations. Financial institutions have to provide facilities to allow people to transact in the metaverse, like converting fiat currency into cryptocurrency or extending loans (Bhat, AlQahtani, & Nekovee, 2023). By facilitating identity management during community and social experiences, Non-Fungible Tokens (NFTs), which comprise digital data stored on blockchains, can serve as a bridge between users and the metaverse. Therefore, NFTs could be used in identifying ownership of virtual reality products in the metaverse (Renduchintala, Alfauri, Yang, Pietro, & Jain, 2022). As ownership can be transferred by the owner, NFTs can be sold and traded based on ownership records recorded in the blockchain. Banks could use NFTs as an asset class to manage wealth and launch mutual funds that invest in NFTs. Banks can offer immersive 24/7 banking in the metaverse for customers who still prefer branch banking. Customer service representatives in call centers may be replaced by their avatars in the metaverse. Thus, customers could access a 360-degree view without waiting in line at the bank or speaking on the phone with a customer relationship manager. The metaverse could allow customers to have personalized conversations with bank personnel. This could offer access to all bank services 24/7, at their own convenience. As required for all financial transactions, transactions in the metaverse also need to be secured. Blockchain and 6G could be used in paving the way for collaborative peer-to-peer lending, as well as direct transactions between parties using blockchain and cryptocurrency (Baliker, et al., 2023). Additionally, 6G systems are expected to boost open banking with their speed, low latency, and support for a wide range of connected devices. Individual customers can own their banking data through open banking. This provides fundamental support for the development of a new ecosystem of data marketplaces and financial services. It is expected that the finance sector will use federated learning to decentralize data ownership in open banking (Long, Tan, Jiang, & Zhang, 2020). As a result, FinTechs will be able to provide businesses and consumers with highly customized, efficient, and secure banking solutions such as decentralized identity management, distributed credit scoring for the unbanked, and privacy-preserving personalized financial management and peer-to-peer lending. 6G's enhanced security measures, including quantum-resistant encryption, will also instill increased trust in users.

BACKGROUND

6G security challenges are the vulnerabilities inherent in previous generations, and the vulnerabilities created by 6G's increased threat surface. In addition to having a better encryption and security architecture than 4G, 5G will also be used in a much broader array of applications, and with more connected devices. 6G is anticipated to provide even more elaborate use models, which will make it an even greater target for dynamic, software-based cyberattacks. Moreover, as the IoT expands, billions of connected devices across networks provide opportunities for attackers.

Security aspects of 6G can be divided into three categories: security, privacy, and trust (Ziegler, et al., 2021). Security technologies, such as automated software creation, automated closed-loop security operations, quantum-safe cryptography, physical layer security, and jamming protection, must be extended to achieve the ultimate goal of trustworthy 6G networks (Akbar, Hussain, Sheng, & Mukhopadhyay, 2022). Security is essential to protect privacy and enable trust. Besides protecting sensitive information from external attacks, security may also reduce the amount of information disclosed internally, i.e., to multiple stakeholders involved in communicating. As a result, enabling technologies that go beyond security are required, as well as trust-creating technologies embedded in hardware and the cloud, such as anchors of trust and distributed ledgers. The addition of specific technologies focusing on trust completes the picture of a resilient, privacy-preserving, and trustworthy 6G network.

This section examines the challenges in 6G for security, privacy, and trust (see Figure 1).

Security Threats and Mitigation Methods

This section discusses security, privacy and trust threats in 6G networks and their potential mitigation methods.

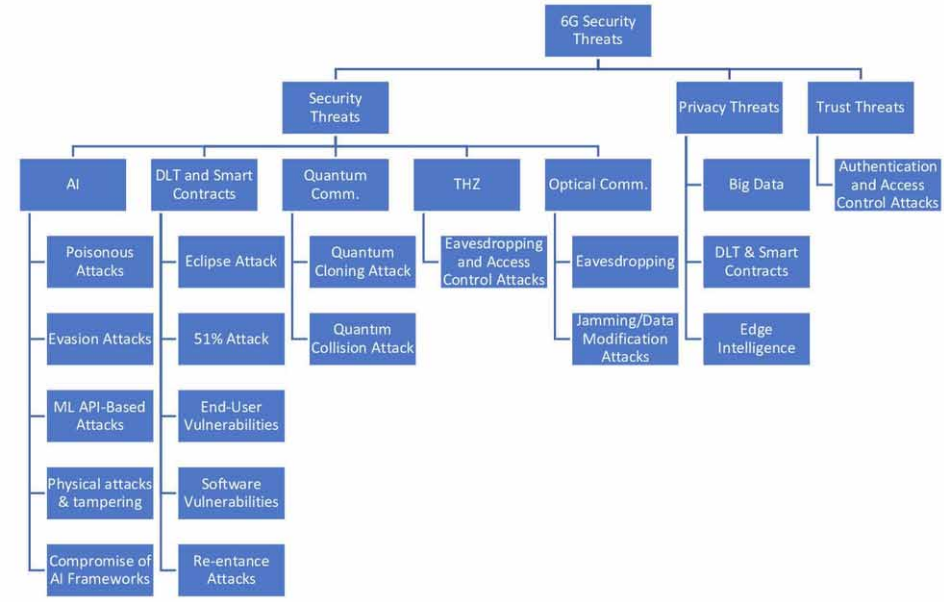
Security Threats and Mitigation Methods

Security threats related to AI, DLT, smart contracts, quantum communications, THz communications, and optical communications are summarized below:

Artificial Intelligence

- *Poisonous attacks* aim to influence learning outcomes and lead to misclassification and incorrect regression results by using malicious samples for training purposes, e.g., manipulating labeled data or using weak labels (Siriwardhana, Porambage, Liyanage, & Ylianttila, 2021), (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). Automated *security operations, such as automated,* distributed, cognitive, closed-loop security operations and analytics may mitigate these attacks (Ziegler, et al., 2021). Cyber-resilience entails persistent connections, data, and resources with context awareness. Privilege restrictions in network activities and the "least privilege" principle are required. To ensure cyber resilience, distributed monitoring and auditing agents will be required. In addition, redundancy in architecture, integrity checks, segmentation, partitioning, or dynamic isolation. Nested Intelligent Security Orchestration allows for automation and response closed-loops across a horizontally distributed heterogeneous cloud topology, and distributed and federated security orchestration across management stacks. In accordance with the vision of the

Figure 1. Security threats in 6G



6G data and information architecture, network functions, data and information layers, applications, services, and solutions are performed by autonomous AI and ML decision-making execution units at all abstraction levels. Efforts should be made to minimize latency between event generation and inference. Moreover, it is possible to leverage data and information layers to connect disconnected units while providing consistent capabilities across endpoints and in the cloud.

- *Evasion attacks* bypass the learned model during the test phase by introducing disorders to the test instances (Siriwardhana, Porambage, Liyanage, & Ylianttila, 2021), (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). This can be mitigated by automated *software creation*. Quantum AI/ML-driven software creation enhances software quality and customer readiness, and provides insights into code characteristics during continuous development and integration. Use cases include automated code generation and testing, detection of static and dynamic bugs, code optimization to avoid duplication and deviation from coding guidelines. Software creation in the 6G era will increasingly adopt concepts of chaos and performance engineering to build confidence in the system's capability to withstand unforeseen circumstances. Resilience can be proven proactively using techniques such as experimental and potentially destructive fault injection testing. These could include, for example, subjecting the component to a series of what-if scenarios in a virtual reality (VR) or mixed-reality (MR) system constructed using digital twins of interacting hardware and software elements (Ziegler, et al., 2021).
- *ML API-based attacks attempt to obtain predictions about input feature vectors using malicious party queries and attacks on the application programming interface (API) of an ML model.* A model inversion attack attempts to recover training data, extract model architecture, and infer memberships. This exploits the model output to predict training data and ML models (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). These attacks could be mitigated using automated software creation and automated security operations.

- *Infrastructure physical attacks & communication tampering* aim to cause a slowdown in data processing and decision-making, or the malfunction of the entire AI system by causing intentional outages and degradation of communications and computing infrastructure (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). These attacks could be mitigated by using automated security operations and *jamming protection.* In Industry 5.0, the availability and cyber-resilience of critical network infrastructure may be seriously compromised by jamming, which can affect the production environment and result in economic losses (Ziegler, et al., 2021). For example, a simple increase in latency can halt banking and financial services. Therefore, research into the security design options of the 6G physical layer presents the opportunity to think of novel ways to mitigate the risk of jamming and other denial of service (DoS) attacks. Anomaly detection and user and/or device authentication using AI/ML techniques may be useful in detecting jamming and preventing node compromise attacks. Additionally, *self-healing* could be used in addressing physical layer problems associated with existing wireless systems, including receiver noise, channel and hardware impairments, quadrature imbalance, path loss, atmospheric and rain attenuation, interference, and fading. The use of AI can provide an optimal method for communicating between different hardware types. Sensor-based 6G networks are expected to benefit from AI-based self-improvement mechanisms in the future. A critical step towards achieving this goal is the ongoing specification efforts to integrate AI/ML as native elements of future networks, including the ETSI Zero Touch Network and Service Management (ZSM) architecture that entails closed-loop operation and AI/ML techniques that automate a wide variety of network management operations, including security (Chen, Feng, Ge, & Zhang, 2022).
- *Compromise of AI frameworks* implies disabling AI/ML functions by exploiting software, firmware, and hardware vulnerabilities in existing AI/ML framework artifacts or traditional attack vectors, especially in cloud-centric operations (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). *Automated security operations* and *tamper-resistant hardware could serve* as mitigation techniques. The tamper-resistant secure hardware component will act as a root of trust for ensuring data and code security when deployed over untrusted platforms, e.g., for remote attestation and key/data encryption. This includes enhanced and hybrid processing units, hardware acceleration, and an abstraction layer relating to hardware acceleration for data-intensive computation for demanding 6G use cases such as AR, VR, and MR. Currently, attestation is performed per server, however, the challenge is expanding it to include virtual images and containers across the hybrid cloud (Ziegler, et al., 2021). Additionally, *quantum-safe security* could be used for, e.g., access control, data protection, system protection from viruses, quantum computer-based attacks, and other types of network intrusions. Quantum-safe security may be enhanced by adapting parameters such as key size to symmetric encryption algorithms such as Advanced Encryption Standard. However, quantum algorithms such as Quantum Key Distribution may provide an effective approach to securing 6G networks and protocols (Muheidat, Dajania, & Tawalbeh, 2022).

DLT and Smart Contracts

- *Eclipse attack:* Blockchain nodes may be forced to accept false information when their communications are disrupted or disseminated, resulting in the confirmation of fraudulent transactions (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). These attacks could be mitigated using

automated security operations based on AI-based predictive analytics in predicting these attacks before they occur.

- *Centralization of miners (51% Attack):* The blockchain can be manipulated by cybercriminals if they gain control over at least 51% of the mining power of public blockchain applications (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). These attacks could be mitigated using automated security operations.
- *End-user vulnerabilities:* The loss or misplacement of private keys can compromise the assets stored on the blockchain, e.g., identity theft, malware, and phishing attacks (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). These attacks could be mitigated using quantum-safe cryptographic algorithms. For example, messages could be first transmitted using a quantum layer, followed by a second layer that uses Toeplitz hashing to preserve private keys created on the first layer. This includes lattice-based, code-based, multivariate, and isogeny-based cryptographic schemes (Ziegler, et al., 2021).
- *Software Vulnerabilities:* Cyber risks can be devastating and long-lasting if DLT implementations deploy unproven codes on live blockchains (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). Automated software creation could be used as a mitigation method.
- *Re-entrance attacks:* Occurs when a smart contract contacts another smart contract that is vulnerable. These attacks could be mitigated using automated security operations.

Quantum Communications

- *Quantum cloning attack:* It refers to making an exact copy of information based on a random quantum state without altering its original form (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). These attacks could be mitigated using tamper-resistant secure hardware and quantum-safe security.
- *Quantum collision attack:* These attacks, which occur when two inputs of a hash function give the same output, can be mitigated using a quantum collision-resistant hashing algorithm (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021), (Cherckesova, Safaryan, Lyashenko, & Korochentsev, 2022).

THz Communications

- *Eavesdropping and access control attacks:* A malicious party may intercept communications, breach access controls, steal data or user credentials in order to access unauthorized resources, or make changes to the system parameters of a 6G system. The narrow beamwidths, the inability to penetrate walls and reduced ranges of THz signals force unauthorized users to remain close to legitimate users, thereby offering stronger security at the physical layer. However, an eavesdropper might still intercept signals scattered by objects close to the LOS path. High data rates involved in 6G makes repeat-back-jamming attacks more difficult since the processing time of the eavesdropped signals may not be sufficiently short so as to outsmart the user receiver. Nevertheless, one must carefully consider the vulnerabilities of mm-wave and THz signals to such attacks (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). EHF and THz communications may also be susceptible to access control attacks, malicious behavior, and the exposure of data transmissions. As a result, new physical layer solutions may be needed for link security. Electromagnetic

signatures of materials and devices in the THz band may be used as authentication methods at the physical layer for preventing eavesdropping and access control attacks.

Optical Communications

- *Eavesdropping:* In comparison to RF systems, optical links can potentially provide a higher level of security since optical radiation is much more focused and cannot penetrate walls. However, they may still be susceptible to jamming and eavesdropping from unauthorized nodes located close to the LOS (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). Physical layer security techniques can provide effective solutions to the security of optical links. Beamforming techniques based on reinforcement learning provide optimal beamforming policies against eavesdropper attacks (Sejan, et al., 2022).
- *Jamming or data modification attacks:* Malicious transmitters may pass undetected in optical or hybrid optical-RF systems (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). The probability of a successful attack increases with highly directed transmitters, or with optical beamforming. On the other side, a combination of accurate localization capabilities of optical waves and ML techniques can also be used for detection of anomalies and jamming. Additionally, AI-based authentication and authorization systems can prevent node compromise attacks (Ziegler, et al., 2021).

Privacy Threats and Mitigation Methods

In the envisioned era of 6G, in addition to the security threat mitigation, privacy protection is also a fundamental performance requirement and poses the following challenges. In this section, privacy threats related to big data, DLT, smart contracts, edge intelligence, and accuracy are provided, and potential mitigation techniques are provided:

- *Big Data:* As it becomes easier to access and collect data, high 6G data traffic may threaten user privacy. D*ata synthesis* can be utilized as a mitigation technique. The purpose is to extend the coverage of data to simplify or convert a model. This is when no real data exists, or only spare real data is available. Data synthesis refers to the process of using synthetic data to perform the same downstream tasks as real data. This includes analysis, test-case generation, virtual reality modeling, behavior prediction, and queries. By replacing real data points, it also removes privacy-sensitive data set features, making it a data privacy-preserving technology. Privacy can be protected by omitting information from real data sets that is irrelevant to the analysis objective. This includes information on the owners or locations of users, sensors, or sub-networks (Ziegler, et al., 2021).
- *DLT & Smart Contracts:* DLTs and smart contracts are prone to privacy concerns, including transaction data leakage, smart contract logic leakage, user privacy leakage, and privacy leakage during smart contract execution (Ziegler, et al., 2021). As a mitigation technique, personal data could be offloaded to a server instead of storing it on the ledger, where reference or synthetic data could be used in smart contracts instead.
- *Edge Intelligence:* EI is highly vulnerable to security attacks because it collects data from multiple sources, and AI/ML algorithms are highly data-dependent. This dependency can be exploited by attackers to launch different attacks, including data poisoning, data evasion, and privacy attacks that undermine AI/ML benefits. Edge validation could be used as a mitigation method. This

method validates the data integrity of IoE sensors through an automated method before it is shared with other applications, e.g., using a DLT network-based solution. Data from specific sensors is restricted by the network to only pre-configured applications in the cloud that process the data according to user preferences. In this way, private information will not be sent intentionally or unnecessarily. Upon validation by the application, the data may either be forwarded to the appropriate far-end application or returned to the user for use with other applications. Such an approach is particularly relevant when the endpoint itself is unable to clean the data, due to a lack of computational power or inability to configure such policies. Thus, this approach may be an effective way of achieving differential privacy. This involves sharing and processing information related to sensors, devices, and subnetworks. Validation of data can be done by analyzing and describing the properties and patterns within the edge cloud datasets. This is done by withholding information about the owner or context of the dataset, such as the particular sensor or network location of the dataset (Ziegler, et al., 2021). Intelligence migration to the network edge will require more sophisticated applications running on mobile devices. This in turn will increase attack threat. On the other hand, it may not be easy to integrate privacy-protection mechanisms into devices with limited resources. A zero-trust architecture (ZTA) could be used as a mitigation method (Chen, Feng, Ge, & Zhang, 2022). In a classical cybersecurity model, an authentication process establishes trust by allowing a user or device access to data, assets, applications, or services. In a ZTA, however, successful authentication does not necessarily imply trust; authentication is only a prerequisite for access. ZTA consists of relationships between network entities, protocol processes, and access control rules (Ramezanpour & Jagannath, 2022). ZTA could be used for monitoring users, IoE devices, network traffic and analytics in real-time and performing risk assessment and trust evaluation for accessing data/applications. It could also be used for generating dynamic policies and automating decision-making processes for granting access to data/applications and for data orchestration purposes.

- *Accuracy:* Many smart applications require location information and identities. However, it is important to strike a balance between maintaining high-accuracy services and protecting the privacy of users (Ziegler, et al., 2021). Consequently, data access rights and ownership, supervision, and privacy regulations must be carefully considered. *Edge-based ML models* may be used for the dynamic detection of privacy-preserving routes, the ranking of these routes, and the use of privacy-preserving routes based on the ranking. *Federated learning*, which allows for flexible training of ML models by having copies of the model sent to the location where data is stored, could be used in performing functionalities, including training, at the edge. Compared to cloud-based centralized learning, federated learning maintains data at the user's fingertips, which enhances data privacy and location privacy. This will require novel multi-stage federated learning protocols, as well as learning model updates, possibly utilizing DLTs (Ziegler, et al., 2021). AI at the subnetwork level in 6G allows for the preservation of privacy within the subnetwork while sharing no more than the learned intelligence outside to minimize the risk of identity theft. In-body networks can benefit from the confinement of data within the network. Due to the large number of applications available in 6G and the massive amount of data collected for the purpose of feeding intelligent models, users may have different privacy preferences for different applications. In order to support fully automated 6G networks while maintaining privacy, AI-based policy updates may offer a potential solution.

- *AI/ML:* There are two ways in which AI/ML may impact privacy. Privacy can be protected in 6G if AI/ML is applied correctly. On the other hand, privacy may be violated by AI/ML attacks during both the training and testing phases, e.g., reverse attacks, membership interference, and adversarial (V. -L. Nguyen, 2021). *Homomorphic cryptography* could be used for performing computations directly on encrypted data, and to build ML models from a large sample set containing sensitive data. Once the data has been decrypted, the result of the computation matches the result of the computation performed on clear text data (Ziegler, et al., 2021).

Trust in 6G Systems

Trust threats related to authentication and access control are discussed below.

Traditional network security models assume that unauthorized access to a network can be prevented by protecting the network perimeter. After appropriate authentication and authorization, any subject operating within the trust zone is considered trustworthy. Users can act maliciously after authentication. Due to the agile radio environment, mobility, and heterogeneity of next-generation tactical networks, identifying the perimeter of the network is challenging, if not impossible (Porambage, Gur, Osorio, Liyanage, & Ylianttila, 2021). Furthermore, such models permit lateral movement of subjects in the trust zone following authentication. Therefore, it is necessary to reform authentication architecture in light of 6G network design changes towards cloud-based and programmable networking platforms.

6G system security architecture is based on openness. In 6G, the line between inside and outside the network will become increasingly blurred as it is expected to be a more open network than 5G. Current network security measures, such as IPsec and firewalls, will not prevent outside intruders from entering the network. This issue can be alleviated by incorporating the zero-trust (ZT) concept into the 6G security architecture (Chen, Feng, Ge, & Zhang, 2022). ZT considers system resources as the most significant aspect of security. ZT assumes that an attacker may reside within a network and that the network architecture is accessible to or unreliable from outside the network. Internal asset loss risk must be regularly assessed, and actions must be taken to minimize it.

Unlike present centralized cloud-based AI systems, 6G will rely heavily on EI. Due to its distributed nature, edge-based federated learning can be applied to network security in an environment where there are a large number of devices and data ensuring high levels of communication efficiency. AI is incorporated into several levels of the network hierarchy in the 6G architecture. At the cellular level, AI can help prevent DoS attacks on cloud servers. Multi-connectivity in a mesh network enables several base stations to utilize AI algorithms to identify a device's behavior and determine its authenticity by using weighted average schemes. As small cells and multiple access technologies result in frequent handovers, behavior-based approaches reduce overhead caused by frequent key exchanges (Hakeem, Hussein, & Kim, 2022). It is possible to establish different levels of authorization at the sub-network level and at the wide area network level with federated learning. Sub-network trust scores may only be shared outside the network when external communication is necessary.

SOLUTIONS AND RECOMMENDATIONS

Banking of the future promises customers a secure, seamless, reliable, and trustworthy digital experience. Shareholders and other stakeholders are similarly concerned that security incidents will not result

in bank equity loss. It is a significant challenge to determine how to be efficient while considering that the legacy environment has an adequate security layer by which security can be embedded into customer experiences and digital transformation supporting technologies.

6G banking security has two dimensions. First, there is 6G security. In this regard, the bank may be transparent. However, it will be responsible for ensuring the security of the 6G infrastructure and capabilities delivered to the bank. To ensure 6G security, all network participants, including banks, need to implement enhanced security, testing, and training standards. De-risking 6G development and operation across the ecosystem will be achieved through robust standards, network security, testing, and visibility solutions.

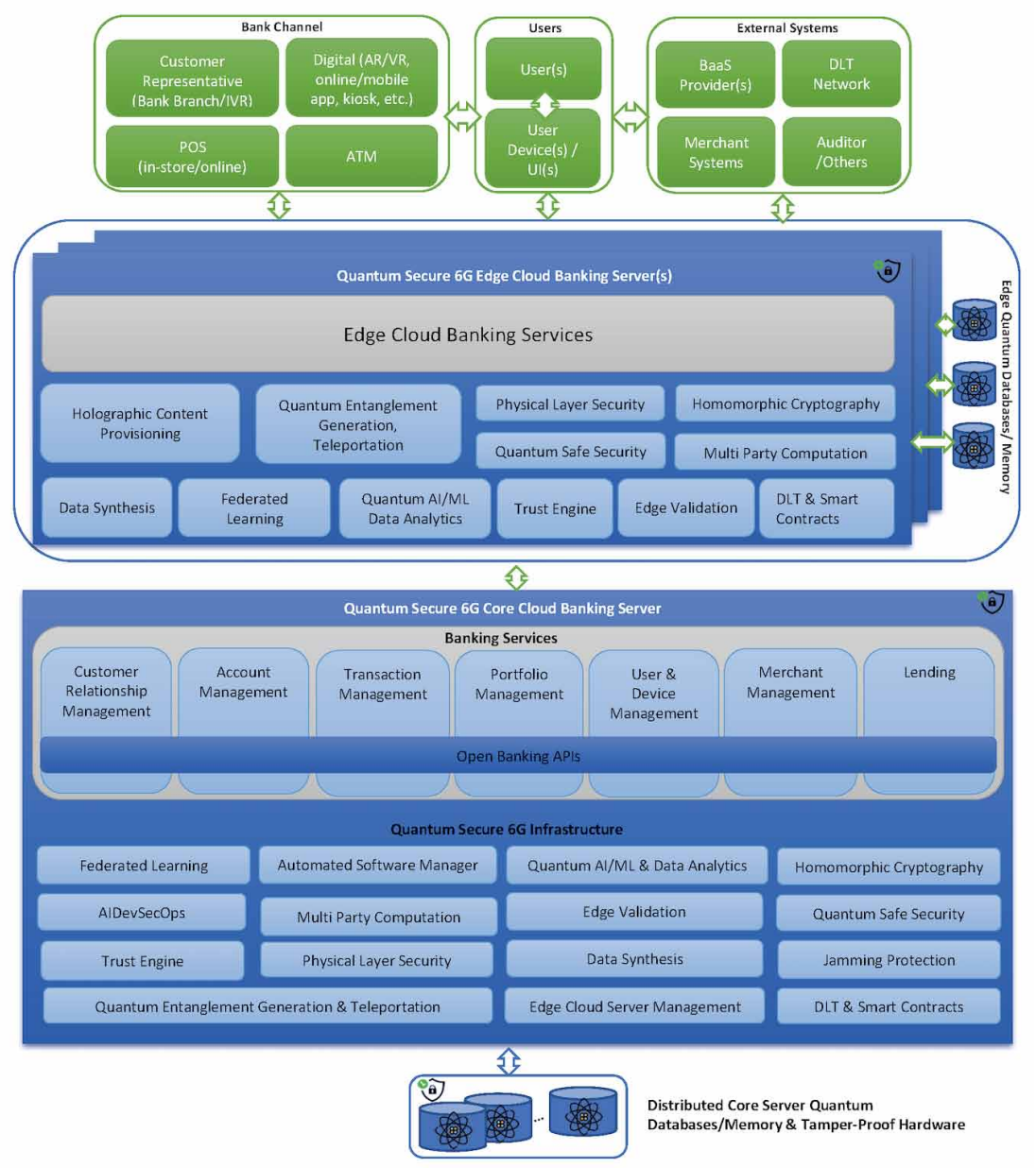
Second, there is the security of banking in 6G environments. Security controls are vital to supporting the banking business model of the future and its ecosystem, which includes people, processes, and technology. Banks can maximize value for their customers and return on investment for the business through predictive analytics combined with the vast amount of customer data in the connected ecosystem. Every aspect of customer engagement relies on speed. Future banking security at 6G speeds, therefore, entails defining and implementing security templates through automation. In addition, it entails supporting the technology and processes that enable the business. Predefined templates for detecting and resolving vulnerabilities, image signing processes, credential vault parameters, etc., can be employed using AI for Development and Security Operations (AIDevSecOps). This is similar to the hardening of various platforms using technical specification templates, which can be automated as a whole.

A reference quantum secure 6G banking system architecture is presented in Figure 2.

A description of the system components is provided below.

- **AIDevSecOps:** Enables operations, including security, and the runtime of the Quantum Secure 6G Banking System. A secure 6G banking system is shaped by cyber-resilience principles as well as AI/ML, automation, and analytics methodologies across the dimensions of customer relationship management, service management, and resource management. Cyber-resilience entails persistent connections, data, and resources with context awareness. Privilege restrictions, e.g., role-based access, are necessary in network activities. As a result of shared data and Quantum AI/ML, operations data could be ingested and analyzed scalable. This could make it possible to analyze and monitor the behavior of microservice-based system calls and thread-level interactions at a microservice level with per microservice granularity at the medium access control (MAC) layer. AIDevSecOps could work with the Quantum AI/ML Module for anomaly detection, self-healing, and root cause analysis of system failures and errors.
- **Automated Software Creation:** Quantum AI/ML-driven automated code generation, as well as automated testing, could be used for the detection of static and dynamic bugs, and perform code optimization to avoid duplication and deviation from coding guidelines. This enhances the system's overall performance, software quality, and reliability.
- **Automated Teller Machine (ATM):** Provides customers with the option to perform financial transactions, including withdrawing cash, making deposits, transferring funds, and checking their balances and accounts, without interacting directly with a bank representative. Includes DLT-based transactions, e.g., cryptocurrency transactions. Communications between the ATM and Quantum Secure 6G Banking Server and the user device could be performed using quantum communications.

Figure 2. Quantum secure 6G banking system architecture



- **Customer Relationship Management (CRM)** has long been recognized as a crucial aspect of a successful business. CRM enables businesses to engage meaningfully with their customers, thereby improving the quality of service, customer satisfaction, profitability, and reducing costs.
- **Data synthesis:** Synthetic data could be used in performing tasks including data analysis, test-case generation, AR/VR/MR user experience modeling, behavior prediction, and queries, where usage of real data is not possible, e.g., in processing data externally of bank systems or due to regulatory restrictions.

- **Device Management module:** The module that manages all IoE devices that access the Quantum Secure 6G Banking System.
- **Digital Banking:** Digital banking refers to services offered by a bank or a financial institution that allows its customers to carry out financial operations remotely, e.g., crypto transactions, person-to-person (P2P) or cross-border payments, applying for loans, etc., via e.g., an AR/VR/MR device, mobile device and/or a mobile/web application offered by the bank or financial institution. It includes all 6G digital banking channels, such as the metaverse, mobile banking, online banking, digital kiosks, etc., used in accessing banking and financial services.
- **DLT & Smart Contracts:** This module performs DLT and smart contracts related activities and acts as an interface between the DLT network and the Quantum Secure 6G Banking Server. It could be used for storing and exchanging trust information, enabling key maintenance lifecycles, as well as supporting dynamic roaming policies and contract updates through smart contracts. Observed device behavior could be utilized to build and share trust information through the DLT network. Since reports stored in the DLT cannot be modified by malicious individuals, DLTs can be used by the bank's IoE network to establish device reputation. This will enable edge cloud providers to establish a level of trust and access granted to a device.
- **Edge Cloud Banking and Financial Services:** It refers to banking and financial services provided by the Quantum Secure 6G Banking Server.
- **Edge Cloud Server Management:** Manages all edge cloud servers in the Quantum Secure 6G banking system. It includes data provisioning, synchronization, disaster recovery, configuration and policy management, audit, compliance, and trust scoring. Quantum Secure 6G Edge Cloud Banking Servers that are detected performing fraudulent or malicious activities can be removed from the network by the Quantum Secure 6G Core Banking Server.
- **Edge Validation:** Validates the data integrity of IoE devices in the bank's IoE network through an automated method before sharing with others, e.g., using a DLT network-based solution. Data from specific IoE devices is restricted by the network to only pre-configured banking and financial applications that process the data according to user preferences. Upon validation, the data may either be forwarded to the appropriate banking application or returned to the user, ensuring data privacy. Validation of data can be done by analyzing and describing the properties and patterns within the datasets in the Quantum Secure 6G Edge Cloud Banking Server.
- **External systems:** It refers to all other external systems that connect with the Quantum Secure 6G Banking System, e.g., Banking as a Service (BaaS) Providers, DLT network, external auditors, etc.
- **Federated learning:** To ensure privacy preservation, it performs functionalities, including training, on the Quantum Secure 6G Edge Cloud Banking Server. This enables distributed customer data ownership in open banking. It could work in conjunction with the DLT network and the Open Banking APIs.
- **Holographic Content Provisioning:** Provides context-aware and personalized AR/VR/MR experiences by on-demand provisioning of holographic content to the user device. Takes into account user conditions, device type, application type, battery level, etc. Utilized by the Quantum Secure 6G Edge Cloud Banking Server.
- **Homomorphic Cryptography:** Could be used in ensuring data privacy between third-party providers and banking systems and to build ML models from a large sample set containing sensitive data.

- **Jamming Protection:** Mitigates jamming and other DoS attacks. Anomaly detection, and user and/or device authentication using AI/ML techniques may be useful in detecting jamming and preventing node compromise attacks. Therefore, this module would work together with the Quantum AI/ML Module.
- **Lending module:** A lending module performs all loan operations within the bank.
- **Merchant Module:** This module performs merchant related activities by the Quantum Secure 6G Banking Server and provides customer support to merchants for online payments, billing, and POS integrations in accepting payments, including crypto transactions, in store or online.
- **Merchant Systems:** Merchant systems are used in providing merchant services for accepting and processing payments, or merchant processing. Merchant systems are usually integrated with banks for reconciliation, and POS terminals for accepting online and in-store payments. Merchant systems may be integrated with the blockchain-based banking application server using the integration supported by the Merchant Module.
- **Multi-Party Computation:** Multiple parties can perform computation at the same time and receive the results without revealing the inputs of the other party. Data is processed across the device-cloud-edge continuum by leveraging the computational capabilities across devices, subnetworks, edge clouds, and central clouds (Ziegler, et al., 2021).
- **Open Banking APIs:** Open banking involves providing third-party banking service providers with access to consumer banking, transaction data, and other monetary information from banks and other financial institutions through APIs. With open banking, consumers, financial institutions, and third parties can connect accounts and data across institutions. Data generated by the Federated Learning module could be shared across different bank servers and FinTechs to achieve decentralized customer data ownership with these APIs.
- **Physical Layer Security (PLS):** Despite many PLS schemes already implemented, PLS is still of importance for IoE networks. Existing radio communications concepts can be employed for dual purposes, for example, to verify transmission validity at the physical layer. Specifically, two peers can use radio channel characteristics known and only available to them to verify the origin of messages, without relying on encryption or message authentication. Furthermore, channel characteristics may be used to determine or refresh a shared key between two communicating peers. PLS methods complement encryption techniques, and provide security demonstrated using information theory. In contrast, cryptographic methods assume that encryptions are unbreakable (Ziegler, et al., 2021).
- **POS:** Refers to a merchant device or software where a customer makes a payment for goods or services in-store or online. POS systems could be integrated with the Quantum Secure 6G Banking Server using Merchant Module-supported integrations.
- **Quantum AI/Data Analytics:** This module performs all data analytics activities in the bank using quantum ML/AI algorithms. This includes running quantum ML/AI algorithms to perform banking, security, and fraud-related activities such as quantum cyber-attack intrusion detection, prevention, trust scoring, risk-based authentication, and anomaly detection.
- **Quantum Database(s)/Memory:** Stores and manages data used in 6G banking. Unlike a conventional database, a quantum database allows resource transactions only when forced by observation. The assignment of system resources to consumers in such environments will be more successful if they are deferred until all constraints are available to the system. Quantum databases can

enable collaborative applications with constraint satisfaction directly within the database system through the entanglement of queries and transactions (Hamouda, Bahaa-Eldin, & Said, 2016).

- **Quantum Entanglement Generation & Teleportation:** Manages quantum communications and performs necessary transformations required for data processing. Works together with the Quantum Database/Memory.
- **Quantum Secure 6G Banking System:** Includes all software and hardware components used by a bank for its 6G secure operation. Hardware components include quantum servers, databases, memory, Hardware Security Modules (HSMs), ATMs, edge cloud servers, etc. Banking system software is used to manage, monitor, and record transactions at banks and other financial institutions. The software is used to assist in managing front-office functions such as customer engagement, portfolio management, and sales of core banking products. Also supported are back-office functions such as credit approvals, auditing, financial accounting, background checks, and system integrations.
- **Quantum Secure 6G Core Banking Server:** Differs from standard, centralized banking servers in that it utilizes quantum computing. Quantum communications are performed via its Quantum Entanglement Generation and Transport system. Data is stored in quantum secure memory/databases. Quantum communications is used between the Quantum Secure 6G Core Banking Server and external system components, including edge servers, user devices, ATMs, POS, etc. The Quantum Secure 6G Banking Server functions as both a DLT and a quantum node in the network. DLT-related activities are carried out on a decentralized blockchain network. Data is stored on the DLT and Quantum Databases/Memory, and smart contracts drive the logic of DLT-related activities.
- **Quantum Secure 6G Edge Cloud Banking Server:** Performs Edge Validation of IoE devices at a subnetwork location and shares the information with the Quantum Secure 6G Banking Core Server. Utilizes Tamper-Proof Hardware.
- **Quantum Safe Security:** Security software used to secure and protect bank systems, including its application servers, its network, and any IoE device connected to it. It provides access control, data protection, protects the system from viruses, quantum computing-based attacks and other network-related intrusions, and evades other system-level security risks.
- **Tamper-Resistant Secure Hardware:** Could be used as a root of trust for ensuring the security of data and code when deployed over third-party platforms, e.g., a BaaS provider.
- **Transaction Management:** Performs processing of a bank's financial transactions, including bank cash management, credit/debit/prepaid card transaction processing, money order management, national and international transactions, check management, as well as preparing files for reporting of end-of-day processes.
- **Trust Engine:** Monitors users, IoE devices, network traffic and analytics in real-time. In addition, it performs risk assessment and trust evaluation for accessing data/applications. It also generates dynamic policies and automates decision-making processes for granting access to data/applications and data orchestration. The trust engine works in conjunction with the Quantum AI/ML system for detecting anomalies.
- **User:** The end user that accesses banking and financial services. It should be noted that the user group is heterogeneous since they use a variety of applications and perform a variety of tasks. In order to meet the requirements of each application, a specific minimum entanglement generation rate and fidelity level must be guaranteed.

- **User Devices:** Any IoE device accessing the Quantum Secure 6G banking system, including customer and employee devices.
- **User Interface (UI):** The interface between a user and an IoE device used in accessing the bank services, including touch screens, keyboards, AR/VR/MR enabled devices, a mobile banking application or website. Holographic user experience is provisioned by the Quantum Secure 6G Edge Cloud Banking Servers.
- **User Management:** Software that is used in onboarding and managing bank customers. Bank's administrators and customers can access banking services through this software module.

The advantages of the presented architecture are summarized below.

- *AIDevSecOps:* Potentially allows operations data to be ingested and analyzed at a scalable rate. This enhances the banking system's observability in a data-centric manner and with adjustable granularity. Can help enhance the cybersecurity of a 6G banking system using AI/ML, automation, and analytics by enabling self-healing, ensuring the persistence of connections, data, and resources with the appropriate level of context awareness.
- *Automated Software Creation:* Benefits include software quality enhancement, increased resilience, fault tolerance, and agility.
- *Data synthesis:* Can help preserve data privacy in banking systems by replacing real data with synthetic data that are irrelevant for its processing, such as information on the owners or user locations, sensors, or sub-networks.
- *DLT & Smart Contracts:* DLT will help increase banking system cybersecurity by preventing attacks including majority, double-spending, re-entry, Sybil, and privacy attacks. Additionally, a network can establish a level of trust for a device based on previous behavioral data. Smart contracts could further enhance banking system security by automatically executing, controlling, or documenting legal events and actions according to the terms of a contract. This could be used for crypto asset trading, crypto-backed loans, or digital insurance applications.
- *Edge Validation:* This approach may be an effective way of achieving privacy of banking systems by restricting the transmission of private data and its processing only to its intended user.
- *Federated learning:* Could ensure the privacy of 6G banking systems by optimizing resources and performing functionalities, including ML training, at the edge.
- *Homomorphic Cryptography:* Enhances privacy and data security by allowing computations to be performed directly on encrypted data.
- *Jamming Protection:* Mitigates jamming and other DoS attacks using anomaly detection and user and/or device authentication using AI/ML techniques. This increases up-time, improves customer experience, and reduces economic losses.
- *Multi-Party Computation:* Supports multiple parties performing computations at the same time and receiving the results without revealing data of the other party.
- *PLS:* Could complement quantum cryptography in enhancing the overall cybersecurity of the 6G banking system by verifying data integrity at the physical layer.
- *Quantum AI/Data Analytics:* Could enhance a 6G banking system's security and value-added services via quantum ML/AI algorithms for banking, security and fraud related activities, including quantum cyber-attack intrusion detection, prevention, trust scoring, risk-based authentication and anomaly detection.

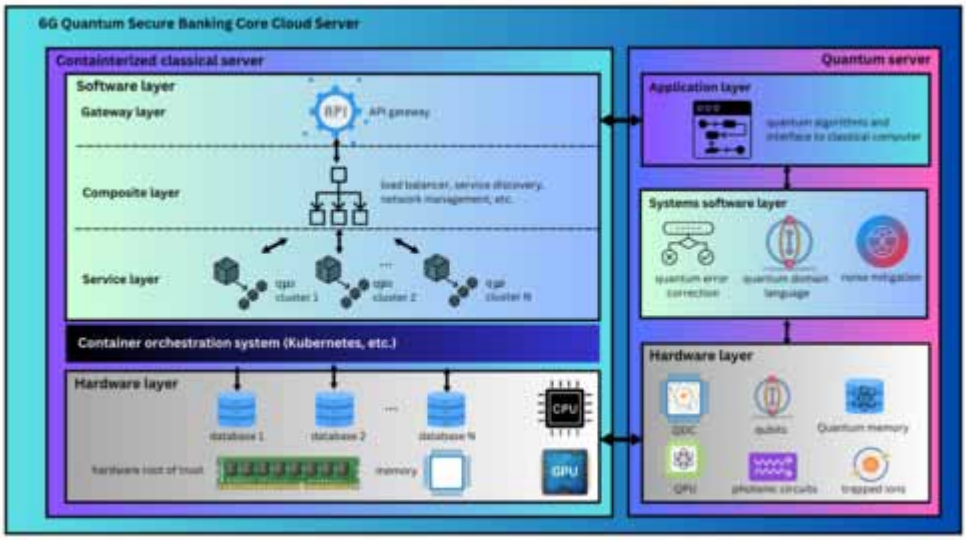
- *Quantum Database(s)/Memory:* Through the entanglement of queries and transactions, collaborative applications with constraint satisfaction can be enabled directly within the database system.
- *Quantum Safe Security:* Could help enhance bank systems' cybersecurity, privacy, and trust, including its application servers, IoE network, DLT and other financial networks. This is done using Quantum Cryptography and Quantum Key Distribution.
- *Quantum Entanglement Generation & Teleportation:* Supports quantum communications and performs necessary transformations required for data processing.
- *Tamper-Resistant Secure Hardware:* Enhances the security of data and code in a banking system when deployed over untrusted platforms by acting as a root of trust.
- *Trust Engine:* Enhances banking system cybersecurity by removing the assumption that authenticated users are trustworthy. This is achieved by automating risk assessment and trust evaluation for access control internally and externally with dynamic policy generation and automatic decision making.

A reference layered architecture of the Quantum Secure 6G Core Cloud Banking Server is depicted in Figure 3. The server has a hybrid quantum computer master-slave architecture based on (Klusch, 2023). The classical machine (CM) is assumed to have a microservices software architecture that is deployed on a containerized server. Using a microservices architecture in banking allows for a more flexible, resilient, and responsive infrastructure, which is well suited to the dynamic nature of the financial industry (Newman, 2021). The classical machine (CM) is assumed to have a microservices software architecture deployed on a containerized server. The microservices in the system, referred to as quantum microservices, accelerate highly complex computations using the quantum machine (QM), including fraud detection, quantum cyber-attack intrusion detection and prevention, risk-based authentication, and quantum artificial intelligence algorithms. Not all quantum microservices necessarily access the quantum computer all the time; they may only access it when necessary for scaling purposes or when there are many requests.

The architectural layers of the containerized classical machine (CM) are described below.

- **Software layer:** The software layer comprises the software backend application of the Quantum Secure 6G Core Cloud Banking Server, with the functionalities provided in Figure 2. The software application has a microservices architecture, with the following software layers:
  - **Gateway layer:** Provides simple gateway routing capability, such as versioning, to handle devices with differing platforms. This typically involves API management through an API gateway. This approach integrates different application domains with each other and routes traffic to the appropriate version of services.
  - **Composite layer:** An essential middle tier that manages the composition of multiple quantum microservices. By triggering events or simply passing the split/aggregated result to other quantum microservices, they perform more complex routing from the processing of content data and aggregate/split data. In this layer, the complexity of quantum microservices is hidden from the clients.
  - **Service layer:** Comprises quantum microservices. Performs data retrieval and business logic processing.

Figure 3. Quantum secure 6G banking server layered architecture



- **Hardware layer:** Comprises all hardware components, including databases, memory, hardware root of trust, central processing units (CPUs), graphics processing units (GPUs), and data processing units (DPUs) of the Quantum Secure 6G Core Cloud Banking Server. CPUs handle general-purpose single-threaded workloads, GPUs handle parallel processing workloads, and DPUs manage processing and low-latency data movement to keep CPUs and GPUs well-supplied with data. CPUs might be used to run databases, while GPUs might be used for artificial intelligence and video processing. DPUs deliver data on time, efficiently, and securely. QM components are controlled and scheduled by a CPU or GPU in a classical containerized server. The memory is accessed by classical and quantum addressing schemes. The time and sequence of quantum operations in the QM are controlled by classical signals and CM processing.

The architectural layers of the QM are as follows:

- **Application layer:** Includes an interface to the CM and quantum algorithms. Quantum algorithms are used in performing computations that are impossible or difficult for classical computers.
- **Systems software layer:** Comprises quantum error correction (QEC), noise mitigation and quantum domain language. QEC protects qubits and ensures reliable communication in quantum channels by increasing communication reliability through error correction. QPL programs consist of high-level primitives for logical quantum operations interleaved with classical workflow statements. The QPL primitives are compiled by the CPU into low-level instructions for qubit operators which are then passed to the QDC for translation into physical qubit operations (registers) which are executed by the QPU. Using a universal set of quantum gates, the QPU performs quantum measurements and basic qubit operations with error correction. This minimizes quantum decoherence caused by imperfect quantum operations control, measurement errors, the number of entangled qubits, and quantum systems limitations. Quantum measurements are only returned

to the CM by the QM. Several quantum programming languages (QPLs) are available for hybrid quantum computers, including procedural QCL, QL, and functional QPL (Klusch, 2023).

- **Hardware layer:** Consists of physical devices and systems that are used to implement quantum computation, including topological qubits, physical qubits, superconducting qubits, logical qubits, trapped ions, photonic circuits, quantum memory, quantum processing units (QPUs), quantum buses, and quantum devices controllers (QDCs) with interfaces to classical machines.

The combination of hybrid quantum computing architecture with microservices software architecture allows banks to perform tasks such as running quantum AI algorithms and key generation and encryption with unprecedented computational capability, which significantly enhances their competitive advantage and cybersecurity. Quantum computing's ability to perform complex calculations complements microservices' agility, scalability, and fault isolation. As a result, banks can quickly react to cybersecurity threats, adapt to market conditions and regulatory requirements. Microservices are in perfect alignment with the hybrid quantum architecture, enabling independent scaling and maintenance. By combining these two innovative technologies, banks are equipped with the computational power and flexibility they need to drive innovation. This will strengthen security measures, and offer sophisticated financial services to their customers.

FUTURE RESEARCH DIRECTIONS

Designing cybersecurity into software architecture and development lifecycles should help identify vulnerabilities and restore networks quickly in the event of a breach. Note that the classical world lends itself better to human intuition than the quantum world. Therefore, it might be more likely to commit errors in designing and implementing complex quantum-based banking systems, since this is a relatively new area of expertise. Therefore, quantum-based banking will present an even greater challenge in terms of accuracy, safety, and reliability than traditional banking practices.

Future research directions of the Quantum Secure 6G Banking System architecture presented in the previous section are provided below.

- *Automated Software Creation:* Software vulnerabilities are a major cause of security issues in today's networks and information technology (IT) systems. The increased attack surface due to the increasing software complexity and heterogeneity in 6G systems will pose a significant challenge. This challenge can be met through AI/ML implementation in the software development process. Despite the ongoing research efforts, existing approaches are still immature and isolated. It remains a challenge to fully utilize AI and ML for highly automated and secure software.
- *AIDevSecOps:* In order to achieve quantum security in 6G banking, an AI/ML-enabled security architecture is necessary both during software development and during network operations. In order to mitigate adversarial attacks, an effective AIDevSecOps system is required rather than large-scale continuous logging. This will include adversarial training to improve robustness, ML algorithms to classify data, and omnipresent checks of the models' integrity and consistency. Security issues due to unsecure network configuration and operation may be overcome by increasing automation through AI/ML. The challenge here is to advance existing approaches to highly automated, intelligent, self-adapting, and holistic orchestration and management systems. Despite

AI/ML's high potential for enhancing network security, the system itself may suffer attacks targeting AI/ML. For 6G networks to remain safe, it is essential to follow closely new developments in this area.

- *DLT:* DLTs provide an effective framework for simplifying trust establishment in heterogeneous operator domains. In addition, they enhance 6G use cases and cumulative trust building based on verified device behavior. However, practical deployments would face challenges regarding scalability, energy efficiency, and latency. Further research is expected to focus on improving DLT consensus algorithms' scalability, making them quantum-safe, and reducing latency and energy costs.
- *Hardware-Based Embedded Security:* 6G systems require hardware-based trust anchors and embedded security. Although server-based attestation has proven effective in today's networks, the challenge is to extend 6G to virtualization and container technologies and make it compatible with highly flexible and dynamic network deployment in the cloud.
- *Jamming Protection and Physical Layer Security:* The physical layer requires an additional security protection and integrity for the 6G radio interface without compromising throughput, latency, and energy efficiency. In addition to cryptographic methods, physical layer security mechanisms also provide additional security measures. Actual implementations should support the demanding requirements of 6G use cases, and must remain safe in the presence of sophisticated and resourceful adversaries. As part of the physical layer, jamming protection is another major challenge. It is not easy to achieve high spectral efficiencies while simultaneously making the radio interface highly resilient to jamming. Therefore, continued and increased research efforts are necessary especially for critical 6G services against novel jamming attacks. The design and implementation of the PLS may prove to be equally challenging as the implementation of cryptographical methods.
- *Privacy Preserving Technologies:* It may be necessary to collect data from diverse sources across different architectural domains to create precise models using AI/ML methods. High-precision location and network sensing will generate an unprecedented amount of sensitive information. Therefore, it is difficult to ensure the confidentiality and privacy of such data not only against external attackers but also to minimize the amount of sensitive information the various stakeholders need to share to provide 6G services. In light of the large amount of data continuously generated in 6G networks, a framework of improved privacy-preserving data processing technologies and inherent principles is necessary. By leveraging distributed 6G hybrid cloud and edge processing capabilities, such a framework controls and monitors data flows. It is also designed to enforce flexible data security and privacy policies. Concepts such as these enable *federated learning*. Increasing data privacy includes challenges and performance issues. In particular, they can be seen in secure multiparty computation, homomorphic cryptography, and hardware acceleration. Further, data privacy models require a comprehensive theoretical foundation that allows for verified model transformations and privacy labeling of data such as "free of privacy-sensitive data". A federated learning model and data synthesis would benefit from this.
- *Quantum Safe Security:* Security challenges have been identified in intelligence network management systems deployment. The first concern is that closed-loop network automation may introduce security threats, such as a DoS, a man-in-the-middle attack (MITM) or a deception attack. To increase virtual machines (VMs) capacity, fake heavy loads can be gradually added to virtual network functions (VNFs). MITM attacks trigger fraudulent fault events and intercept domain control messages to redirect traffic. Data can be tampered with to deceive. As a second concern,

6G networks may use Intent-Based Interfaces similar to ZSM, which could expose information, cause undesirable configurations, or cause abnormal behavior. In addition to compromising system security objectives (e.g., confidentiality, privacy), intercepting data can also result in other subsequent attacks. It is possible to compromise the security of the entire management system by implementing undesirable configuration in intent-based interfaces. Similar effects may also result from malformed intent. A number of promising algorithm candidates have been developed in the area of quantum-safe cryptographic schemes. However, there is still work to be done to bring these schemes to maturity. Consensus must be achieved in an open standardization process on adapting existing security protocols to such new algorithms.

- *Trust:* ZTA applications to delay-sensitive services may be limited by its trust evaluation process. Processing speed can be increased by utilizing methods such as behavior analysis that focus solely on analyzing incremental data correlation. Additionally, ZTA in 6G poses two major challenges to trust evaluation methods. Parameter determination usually involves determining the weights of trust elements from different sources when calculating the trust score. This is based on the trust level of the community and the user device. In addition, balancing generalization and accuracy is often difficult when determining trust thresholds. There is no objective or quantitative method for parameter selection. The development of data-driven trust evaluation methods based on federated learning techniques might be a potential solution. The accuracy of learning models for the same user device vary considerably across banks and financial institutions. This is because it can be difficult to collect sufficient behavioral data to train the models based on a customer data available to a single bank or financial institution. Open banking can tackle this issue.

CONCLUSION

Wireless communications have radically improved our ability to communicate. This is because people no longer need a cabled connection to communicate. In addition, 6G is expected to revolutionize the way consumers, networks, and devices connect with each other. This is done by supporting massive data traffic, storage, and processing for billions of heterogeneous IoE devices. 6G offers new banking possibilities, since it enables high data rates and low latency. It is expected to bring augmented reality, virtual reality, and mixed reality with real-time or non-real-time human-machine interaction where THz communications can play a pivotal role given its extremely wide bandwidth.

The relevance and impact of 6G technology on the banking and financial industry, architectural considerations for developing AI/ML-enabled quantum secure 6G banking systems, as well as its advantages and challenges are discussed in this chapter. Future banking promises to offer customers a secure, seamless, reliable, and trustworthy digital experience. However, the migration and digital transformation of a legacy banking environment to a 6G banking system is expected to be arduous, especially in terms of end-to-end security. This will require ensuring the security of the 6G infrastructure and the capabilities utilized by the bank. In addition, it will require hardening the banking system's security in the 6G environment. To ensure 6G banking and financial systems security, all network participants, including banks, need to implement enhanced security, testing, and training standards. De-risking 6G development and operation across the ecosystem will be achieved through robust standards, network security, and test and visibility solutions. However, since the quantum world is less intuitive than the classical world, the design and implementation of complex quantum banking systems will present an even greater challenge

in terms of accuracy, safety, and reliability than present systems. Therefore, the security of future banking at 6G depends on automation and supporting the technology and processes that enable the business. This can be accomplished by automating security operations, and software creation, implementing jamming protection and physical layer security, utilizing DLTs for distributed threat detection, federated learning, using tamper-proof hardware, quantum computers, edge validation, quantum-safe security, homomorphic cryptography, and quantum cryptography. Additionally, cross-collaboration and data sharing between banks and financial institutions using open banking, federated learning and 6G technology could solve many of the existing pain points related to cybersecurity and privacy in traditional banking systems.

REFERENCES

Akbar, M. S., Hussain, Z., Sheng, Q. Z., & Mukhopadhyay, S. (2022). 6G Survey on Challenges, Requirements, Applications, Key Enabling Technologies, Use Cases, AI integration issues and Security aspects. *arXiv*.

Akhtar, M. W., Hassan, S. A., Ghaffar, R., Jung, H., Garg, S., & Hossain, M. S. (2020). The shift to 6G communications: vision and requirements. *Human Centric Computing Information Sciences*, 10-53.

Akyildiz, I. C., Han, Z. H., Nie, S., & Jornet, J. (2022). Terahertz band communication: An old problem revisited and research directions for the next decade. *IEEE Transactions on Communications*, *70*(6), 4250–4285. doi:10.1109/TCOMM.2022.3171800

Akyildiz, I. F., Guo, H., Dai, R., & Gerstacker, W. (2023). Mulsemedia communication research challenges for metaverse in 6G wireless systems. *arXiv, 2306.16359*.

Baliker, C., Baza, M., Alourani, A., Alshehri, A., Alshahrani, H., & Choo, K.-K. (2023). On the Applications of Blockchain in FinTech: Advancements and Opportunities. *IEEE Transactions on Engineering Management*, 1–18.

Bernstein, D., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188–194. doi:10.1038/nature23461 PMID:28905891

Bhat, J. R., AlQahtani, S. A., & Nekovee, M. (2023). FinTech enablers, use cases, and role of future internet of things. *Journal of King Saud University. Computer and Information Sciences*, *35*(1), 87–101. doi:10.1016/j.jksuci.2022.08.033

Brennen, G., Giacobino, E., & Simon, C. (2015). Focus on Quantum Memory. *New Journal of Physics*, *17*(5), 050201. doi:10.1088/1367-2630/17/5/050201

Chehimi, M., & Saad, W. (2021). Entanglement Rate Optimization in Heterogeneous Quantum Communication Networks. *arXiv*.

Chen, X., Feng, W., Ge, N., & Zhang, Y. (2022). Zero Trust Architecture for 6G Security. *arXiv*.

Cherckesova, L. V., Safaryan, O. A., Lyashenko, N. G., & Korochentsev, D. A. (2022). Developing a New Collision-Resistant Hashing Algorithm. *Mathematics*, *10*(15), 2769. doi:10.3390/math10152769

Glushakov, M. Y. Z. (2020). Edge-based Provisioning of Holographic Content for Contextual and Personalized Augmented Reality. In *IEEE Workshop on Smart Edge Computing and Networking.* Austin, TX: IEEE. 10.1109/PerComWorkshops48775.2020.9156256

Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security Requirements and Challenges of 6G Technologies and Applications. *Sensors*.

Hamouda, I., Bahaa-Eldin, A. M., & Said, H. (2016). Quantum databases: Trends and challenges. In *2016 11th International Conference on Computer Engineering & Systems (ICCES)* (pp. 275-280). IEEE.

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. doi:10.1109/OJCOMS.2021.3057679

Klusch, M. (2023). Toward Quantum Computational Agents. *Lecture Notes in Computer Science*.

Kommadi, B. (2023). *AI and ML Applications: 5G and 6G*. IntechOpen.

Long, G., Tan, Y., Jiang, J., & Zhang, C. (2020). Federated Learning for Open Banking. In Federated Learning, Lecture Notes in Computer Science book series (LNAI) (Vol. 12500, pp. 240–254). Springer. doi:10.1007/978-3-030-63076-8_17

Maksymyuk, T., Gazda, J., Bugár, G., Gazda, V., Liyanage, M., & Dohler, M. (2022). Blockchain-Empowered Service Management for the Decentralized Metaverse of Things. *IEEE Access : Practical Innovations, Open Solutions*, *10*, 99025–99037. doi:10.1109/ACCESS.2022.3205739

Muheidat, F., Dajania, K., & Tawalbeh, L. A. (2022). Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication. In *The 17th International Conference on Future Networks and Communications (FNC)* (pp. 32–40). Procedia Computer Science.

Newman, S. (2021). *Building Microservices* (2nd ed.). O'Reilly Media, Inc.

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 and Tutorials*, *23*(4), 2384–2428. doi:10.1109/COMST.2021.3108618

Porambage, P., Gur, G., Osorio, D. P., Liyanage, M., & Ylianttila, M. (2021). 6G Security Challenges and Potential Solutions. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 622-627). IEEE. 10.1109/EuCNC/6GSummit51104.2021.9482609

Ramezanpour, K., & Jagannath, J. (2022). Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN. *Computer Networks*, *217*, 217. doi:10.1016/j.comnet.2022.109358

Renduchintala, T., Alfauri, H., Yang, Z., Pietro, R., & Jain, R. (2022). A Survey of Blockchain Applications in the FinTech Sector. *Journal of Open Innovation*, *8*(4), 185. doi:10.3390/joitmc8040185

Sejan, M., Rahman, M., Shin, B.-S., Oh, J.-H., You, Y.-H., & Song, H.-K. (2022). Machine Learning for Intelligent-Reflecting-Surface-Based Wireless Communication towards 6G: A Review. *Sensors (Basel)*, *22*(14), 5405. doi:10.3390/s22145405 PMID:35891085

Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). AI and 6G Security: Opportunities and Challenges. *2021 Joint European Conference on Networks and Communications (EuCNC) & 6G Summit.* 10.1109/EuCNC/6GSummit51104.2021.9482503

Tripathi, S., Sabu, N. V., Gupta, A. K., & Dhillon, H. S. (2021). Millimeter-wave and Terahertz Spectrum for 6G Wireless. *arXiv*.

Ziegler, V., Schneider, P., Viswanathan, H., Montag, M., Kanugovi, S., & Rezaki, A. (2021). Security and Trust in the 6G Era. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 142314–142327. doi:10.1109/ACCESS.2021.3120143

ADDITIONAL READINGS

Bertin, E., Crespi, N., & Magedanz, T. (2021). *Shaping Future 6G Networks: Needs, Impacts, and Technologies*. John Wiley & Sons. doi:10.1002/9781119765554

Božanić, M., & Sinha, S. (2021). *Mobile Communication Networks: 5G and a Vision of 6G*. Springer. doi:10.1007/978-3-030-69273-5

Henrique, P. S., & Prasad, R. (2021). *6G The Road to the Future Wireless Technologies 2030*. River Publishers.

Jiang, W., & Luo, F.-L. (2022). *6g Key Technologies: A Comprehensive Guide*. Wiley-IEEE Press. doi:10.1002/9781119847502

Maier, M., & Ebrahimzadeh, A. (2021). *Toward 6G: A New Era of Convergence*. Wiley-IEEE Press.

Sabry, F. (2022). *6G Network: Connecting together the cyber and the physical worlds*. One Billion Knowledgeable.

Wu, Y., Singh, S., Taleb, T., Roy, A., Dhillon, H. S., Kanagarathinam, M. R., & De, A. (2021). *6G Mobile Wireless Networks*. Springer. doi:10.1007/978-3-030-72777-2

Xie, X., Rong, B., & Kadoch, M. (2021). *6G Wireless Communications and Mobile Networking*. Bentham Books. doi:10.2174/9781681087962121010

KEY TERMS AND DEFINITIONS

Artificial Intelligence (AI): Refers to any machine or system that displays human-like behavior. It constructs models of human behavior by analyzing a body of data derived from past examples of similar behavior. An AI-enabled program can analyze and contextualize data for the purpose of providing information or triggering actions automatically without any human assistance.

Banking: Banking is the business of protecting and managing money on behalf of individuals, businesses, and other entities. Banks are financial institutions that provide financial services, e.g., lending

money. Banks assist people in saving, managing, and investing their funds. Banks generate interest, which generates profits for both themselves and their clients.

Cyber-Security: The process of protecting an organization's computer systems and its data against cyber threats, e.g., denial of service, phishing, malware, man-in-the-middle, and ransomware attacks.

Machine Learning (ML): A subcategory of AI where algorithms are used to automatically recognize patterns in data and apply this learning to make increasingly more accurate decisions through experience and data.

Privacy: Assurance that certain information about an entity is confidential and that access to that information is restricted. Data privacy refers to the way that consumers understand their rights regarding the collection, use, storage, and sharing of their personal information.

Sixth Generation (6G): The sixth-generation mobile system standard under development for wireless communications technologies supporting cellular data networks.

Trust: In information technology, trust is the assumption that a user, device, application, or service is who or what it claims to be, is allowed access to the resources it requests, is configured in a way that is expected of it, is free from compromise, and is able to carry out the actions being carried out.

Wireless Communications: Refers to the transfer of information between two or more points without the use of an electrical conductor, optical fiber, or other continuous guided medium. Radio waves are the most commonly used wireless technology.