Chapter 2

Secure Edge Intelligence in the 6G Era

Tanesh Kumar,[1*] Juha Partala,[2] Tri Nguyen,[3] Lalita Agrawal,[4] Ayan Mondal,[4] Abhishek Kumar,[3] Ijaz Ahmad,[5] Ella Peltonen,[6] Susanna Pirttikangas,[3] and Erkki Harjula[1]

[1] *Center for Wireless Communications, University of Oulu, 90570, Oulu, Finland*
[2] *Center for Machine Vision and Signal Analysis, University of Oulu, 90014, Oulu, PL 8000, Finland*
[3] *Center for Ubiquitous Computing, University of Oulu, 90014, Oulun yliopisto, Oulu, PL 8000, Finland*
[4] *Department of Computer Science and Engineering, Indian Institute of Technology Indore, 453552, Indore, India*
[5] *VTT Technical Research Centre of Finland, 02044, Espoo, Finland*
[6] *M3S research unit University of Oulu, Oulu, PL 8000, Finland*

*Corresponding Author: Tanesh Kumar; tanesh.kumar@oulu.fi

2.1. Introduction

Despite the ongoing commercial deployment of the 5G technology, the research community has already started to explore the potential of future mobile and wireless communication networks beyond 5G systems. Future 6G networks are expected to enable a smart, connected, and intelligent digital ecosystem where numerous stakeholders and network entities will require secure and trusted communication-computing continuum to ensure the ubiquitous availability of novel services to consumers in an efficient way. In order to ensure successful deployment and acceptance of 6G networks, it is highly important to consider and address various strict requirements, such as ultra-low latency, security and privacy, embedded trust, automated operations, network management, big data management, as well as intelligent data analysis and decision-making, among many others [Akyildiz et al., 2020].

To ensure the smooth development towards future 6G networks, strong support is required from various advanced and disruptive communication related technologies, such as virtualization, Artificial Intelligence (AI), softwarized/programmable networks, edge and fog computing, quantum computing, and Distributed Ledger Technologies (DLTs)/Blockchain [Akhtar et al., 2020]. Among these, Edge Intelligence (EI) is a centric enabler for various novel 6G-based applications, which combines the capabilities of edge computing and AI to provide crucial features, such as ultra-low latency, high reliability, high resource and energy-efficiency, and high level of security and privacy [Letaief et al., 2022]. The integration of EI with 6G networks will enable the efficient use of local computing, storage, and processing capabilities along with cloud data centers for optimal placement of data processing, analysis and decision-making. This is vital for various future 6G-enabled critical Internet of Things (IoT) applications in different verticals, such as real-time process control in Industry 5.0, virtual reality use cases in computer-aided surgery or remote vehicle operation, self-driving vehicles, etc., all requiring highly reliable, efficient, scalable and secure communication and computing infrastructure for their operations and processes [Bhat and Alqahtani, 2021], [Khan et al., 2022].

Along with all the above benefits, the integration of edge, AI and 6G networks brings wider than before threat landscape for adversaries to launch various security and privacy attacks. For example, during the dynamic computational task offloading in a multi-tier edge-cloud architecture, a malicious entity can fetch or alter the user's sensitive information that is transmitted among various computational nodes [Zhu et al., 2021]. Moreover, when AI algorithms are either fully or partially running on various distributed edge nodes, several security and privacy threats will rise. For example, poisoning attack is one of the most common attacks against Machine Learning (ML) algorithms to alter or change their training models [Mukherjee et al., 2020]. Furthermore, since 6G networks combine various other enabling technologies, such as DLT/Blockchain and quantum computing, there will be a high probability of existing and new security and privacy attacks [Siriwardhana et al., 2021]. Finally, since the 6G-EI ecosystem will comprise several entities (users, devices, service providers, applications, etc.), dynamic and embedded trust management mechanisms will be required.

To address these challenges and secure the EI for future 6G networks, the literature has recently pointed out some potential technologies that will enhance security and privacy [Adhikari et al., 2022]. For example, ML-based security and privacy algorithms will play a significant role in providing intelligent and real-time intrusion detection, prevention, and mitigation mechanisms [Sun et al., 2020]. Moreover, the addition of various security-enabling technologies such as DLTs/Blockchain and quantum-resilient cryptography will enhance the overall security and trust for future 6G network architecture.

The key objective of this research work is to analyze what is still missing in the current mobile generation in terms of security, privacy and trust challenges and what kind of novel and advanced technological developments are required to cope with the new and strict requirements of future massive-scale

IoT applications and critical infrastructures. This chapter mainly explores the potential security vulnerabilities in the context of the future EI and 6G networks. Section 2.2 provides background details about the fundamentals of edge computing, the evolution of edge intelligence, and the need for secure EI for 6G. Sections 2.3, 2.4, and 2.5 discuss various potential security, privacy, and trust threats for 6G EI-enabled systems, respectively. We briefly present the ongoing and future vision for the security standardization activities in 6G and Edge-AI in section 2.6 and conclude the chapter in section 2.7.

2.2. Background/Roadmap

2.2.1. Edge Computing and its importance

Cloud computing allows various users to access services or resources from a remote location via the Internet. Based on the provided level of software and hardware resources, the cloud services are categorized into three categories —Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [Botta et al., 2016], [Stergiou et al., 2018]. These cloud services allow users to create applications and use hardware, software, and operating system in a virtualized environment at a large scale.

IoT is one of the fastest-growing domains of ICT, and IoT devices generate rapidly growing amounts of data to be handled by the cloud. However, due to the long distance from IoT data sources and end-users to the cloud, there are many challenges related to transferring, processing and storing massive data in the cloud, such as high latency, high burden on networks and high energy consumption [Botta et al., 2016, Stergiou et al., 2018]. Edge computing is envisioned to overcome the aforementioned challenges of cloud computing for IoT applications by bringing cloud computation capacity closer to data sources and end-users, as shown in Figure 2.1.

In edge computing, the processing of data generated from different IoT devices occurs at the edge, i.e., between the cloud and the IoT devices. Edge computing platform is distributed in nature and provides networking, storage, and computation services for IoT applications and services, [Laroui et al., 2021, Dizdarevic et al., 2019, Pan and McElhannon, 2018, Tefera et al., 2021]. Edge computing platform addresses the following key issues faced by the cloud computing platform:

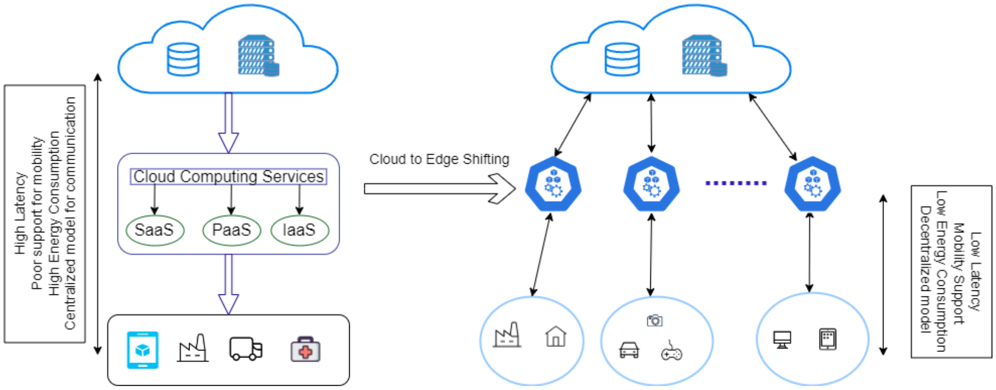

Figure 2.1: Cloud computing to edge computing shifting for IoT applications

1. **Performance (latency, throughput):** Edge nodes are available in the access or local network. Therefore, the distance between edge nodes and IoT devices is less than between the cloud servers and the IoT devices. Hence, edge computing serves the user requests with less delay, and the bandwidth is not limited by as many potential bottlenecks.
2. **Efficiency (resource, cost and energy-efficiency):** Edge computing

decentralizes the processing of data. Therefore, data coming from IoT devices can be processed closer to their sources, and consequently, not as much data needs to be sent over. This reduces energy consumption while also core network congestion is relieved.

3. **Dependability (reliability, security, privacy):** In addition to decentralized data processing, edge computing also decentralizes decision-making. This brings resilience against server/data center failures, network failures and congestion, as well as denial of service or other types of security attacks. Furthermore, edge computing helps limit the propagation of private data, reducing its probability to be exposed to potentially hostile parties.

2.2.2. Emergence of Edge Intelligence

To support the decentralized edge computing platform, AI technologies are envisioned to serve as a support system for fast data processing, i.e., analyzing and extracting meaningful information/patterns from a large amount of data near the source. AI-based optimization methods, such as Federated Learning (FL) and Reinforcement Learning, can help in enhancing the system efficiency at large. Additionally, the integration of AI to edge supports multiple heterogeneous applications in terms of data types, data handling, and offloading while ensuring a minimum latency. Hence, EI comes into existence by incorporating AI techniques and models to support the edge computing platform, [Deng et al., 2020, Zhang et al., 2019]. The edge nodes enabled with AI techniques and platforms are called intelligent edge nodes. Figure 2.2 represents a schematic diagram for EI. It is to be highlighted that EI is not only a simple integration of edge computing and AI. To understand EI, we need to find answers to the following fundamental questions.

1. How can AI techniques provide a solution for edge computing challenges?
2. How can edge computing optimize the operation of AI techniques?

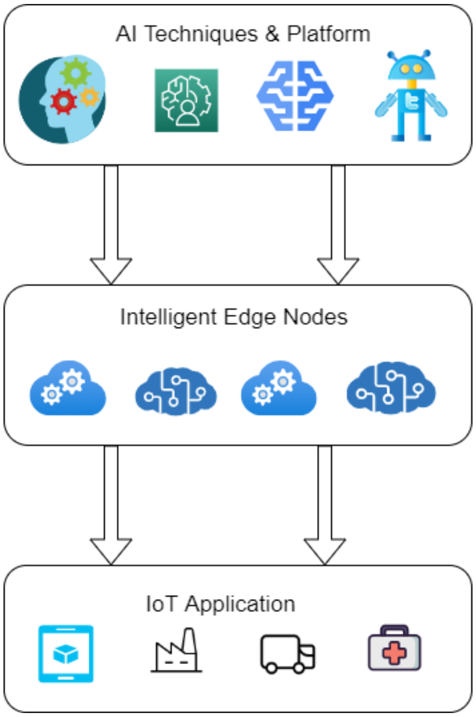

Figure 2.2: Schematic Diagram of Edge Intelligence

To answer these questions, researchers have presented multiple architectures, systems, and enabling technologies for EI [Deng et al., 2020, Zhang et al., 2019, Nain et al., 2022]. For example, [Deng et al., 2020] presented two aspects of EI, i.e., the first one is “AI for edge” that mainly concentrates on efficiently utilizing AI-based solutions and technologies to enhance the edge computing paradigms, e.g., a better, intelligent and more secure solution to data collection and computation offloading for mobile environments. The other aspect is "AI on edge," which deals with constructing AI models for integrating and executing AI techniques in the edge computing environment.

The edge computing platform enhances AI applications to work in heterogeneous and distributed networks, i.e., shift from cloud to edge network. Due to the physical limitations of the edge nodes, EI suffers from the following challenges.

- **Constrained resources:** Due to having limited computational and storage capacity, executing AI algorithms on edge nodes is challenging in a distributed edge computing architecture.
- **Inconsistency:** Cloud computing is capable of supporting multiple platforms for executing AI techniques. Edge nodes have limitations in provisioning these AI-compatible platforms.

To overcome the aforementioned issues, [Zhang et al., 2019] proposed a framework, named OpenEI. The authors constructed a model using lightweight packages of deep reinforcement learning algorithms. OpenEI framework aims to find appropriate AI techniques corresponding to edge environments to remove the inconsistency. In another work [Zhu et al., 2020] identified the importance of distributed learning, i.e., FL, for edge nodes. Using FL, the authors addressed several issues using the amalgamation of AI and edge computing.

2.2.3. Integration of Edge Intelligence and 6G

The future 6G network is expected to bring the next-generation revolution in the telecommunication sector. The 6G ecosystem will combine a plethora of various existing as well as novel enabling technologies along with advanced sensing and communication technologies that will empower future massive-scale IoT applications such as Industry 5.0, virtual reality use cases, and autonomous driving. To accomplish the 6G vision, the research community has already started to drive deep into the various requirements, e.g., ultra-low latency, reliability, massive connectivity, autonomous and self-adapting networks, peak data rate, optimal spectrum usage, and maturity in the relevant enabling technologies among others [Qadir et al., 2022], [Ray, 2021]. In addition, various open challenges require suitable solutions such as robust security and privacy solutions, energy efficient and sustainable solutions, optimized resource utilization, and implementing AI/ML solutions for future communication networks [Zhang and Zhu, 2020].

The integration of EI and 6G will enable ubiquitous intelligence at scale, i.e. convergence of communications, sensing, and localization with decentralized learning and inference at the edge over an end-to-end environment. The integration is likely to lead to a cognitive network architecture capable of accommodating the requirements of the 6G verticals. It will further facilitate the design and deployment of the verticals capable of utilizing resources for learning and inference in the programmable world in real time. EI will enable support for autonomous computing features, such as self-healing, self-configuration, and self-optimization in 6G verticals, thus making 6G resilient to unforeseen and unintended incidents.

2.2.4. The need for secure Edge Intelligence

The 6G ecosystem will be a collective, collaborative platform ecosystem with a plethora of advanced enabling technologies and multiple stakeholders, such as network operators and service providers, that may utilize integrated computation and communication platforms for various services.

The integration of EI with the future 6G will enable massive IoT applications by offering distributed intelligence, reliable connectivity, and faster data analysis/decision-making. To make this vision a reality, novel security solutions are required to protect entire EI-enabled 6G ecosystems for various applications. Some of the security solutions for such smart ecosystems may also utilize different existing security technologies and approaches proposed for 5G systems. For example, Blockchain-based/integrated/empowered security mechanisms and frameworks have been widely proposed and developed for the 5G networks.

2.3. Security Challenges in 6G EI

2.3.1. Computational offloading

In an untrusted IoT computing environment where several sensor nodes/devices are connected to a cloud server through edge nodes-devices, the outsourcing of resources/computations or sensitive data from end devices to potentially untrusted edge nodes or devices can create challenges regarding the confidentiality and integrity of the computation. Dishonest serving nodes can modify both the input data and the actual computation and return plausible but false results. The untrustworthiness of the computing party is also a problem if the input data contains sensitive information. This type of environment, where we cannot assume inherent trust within a network and its entities, should be dealt with a Zero-trust approach, Syed et al. [2022], requiring strict identity verification and continuous authentication for all users, devices, and applications.

To ensure confidantiality, homomorphic encryption (HE) can be applied to compute on encrypted data [Rivest et al., 1978, Gentry, 2009]. Fully homomorphic encryption enables computations to be performed on encrypted information and those computations translate to the unencrypted domain. However, fully homomorphic encryption is computationally demanding and may be too costly for edge devices even if advances are made in the development of these schemes. Flexible mechanisms are needed to determine whether certain data can be transmitted for outsourced computation.

Verifiable computing is seen as one of the potential solution candidates to the integrity problems. In verifiable computing, the computing party generates proof that the required computation was performed correctly [Babai et al., 1991, Gennaro, 2017]. The proof is significantly easier to check than to repeat the actual computation. Thus, computation can be outsourced even to an untrusted party with its integrity guaranteed. The generation of such proofs is, however, computationally expensive and can be prohibitively for edge devices.

2.3.2. Security of Machine Learning

It is evident that ML plays an integral part in 6G EI. Therefore, the trustworthiness of the applied models is essential in the correct operation of the network. However, there are multiple challenges regarding the security of ML. In particular, we have to ensure that 1) the training data is correct and not disclosed to unauthorized parties, 2) the model training is executed correctly and no false data is inserted into the training set, and 3) the applied models do not enable malicious parties to infer information about the training data from

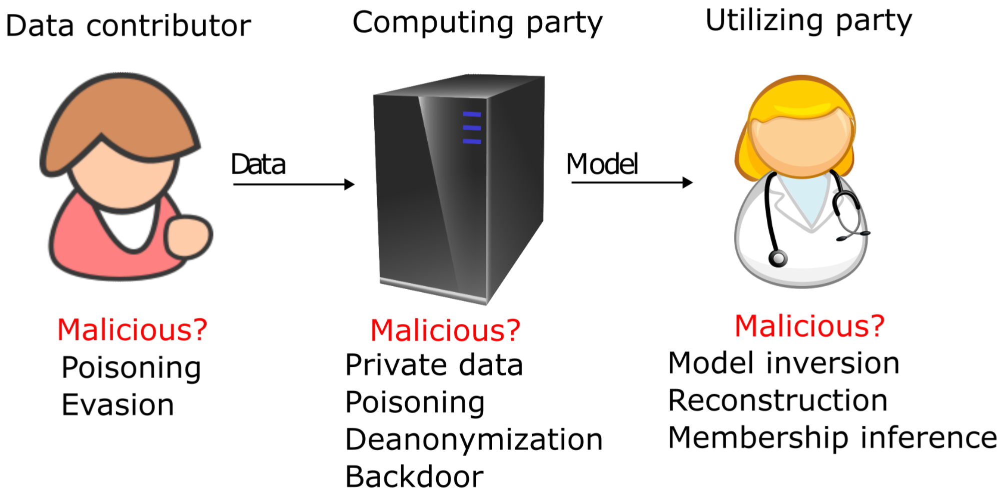

Figure 2.3: Challenges related to the security of machine learning.

them or to exploit the model, for example, through evasion attacks [Biggio et al., 2014]. These challenges have been discussed in detail below and have been depicted in Fig. 2.3.

EI can function correctly only if the applied models are correct. Regarding AI and ML, a correct model requires correct training data. Poisoning attacks insert malicious data into the training set in order to skew the trained model. As a result, the model may exhibit poor generalization and behave incorrectly. In order to have trustworthy models, poisoning attacks need to be detected, and the false data need to be removed from the training set. In general, protecting against poisoning is hard [Pitropakis et al., 2019], and there is not a generic method that works for any use case. Additional research is needed to have satisfactory protection mechanisms for the EI use case. When using the FL proposed in Zhu et al. [2020], there are risks of potential poisoning attacks to occur [Tolpegin et al., 2020].

While the integrity of training data is important, the same applies to the integrity of the trained model. For EI, the training is performed on the edge, potentially by an untrusted entity. Such delegation of computing can raise serious questions of trust. The training party has complete authority over the training process and can potentially insert its own data into the training set or create a backdoor into the model. Such a backdoor can have incorrect and unexpected behaviour on certain inputs specified by the malicious party. Furthermore, such a backdoor can be *provably undetectable* even if the user tries to validate the model's accuracy and robustness [Goldwasser et al., 2022].

As discussed in section 2.3.1, one of the potential solutions to the integrity issues is Verifiable computing, which generates computational proofs and verifies the correctness of the outsourced information. However, the generation of proof for the correctness of training can be prohibitively expensive.

2.3.3. Post-quantum cryptography

Quantum computing has taken large steps towards practicality during the last decade. It is widely known that certain problems are easier to solve on a quantum computer than on a traditional one. Some of those problems underlay the contemporary public-key encryption algorithms. Therefore, a lot of research has recently concentrated on the security of cryptographic algorithms in the quantum computing model.

Since quantum computing will have a significant role in the context of 6G and EI, the employed security mechanisms should be designed in a way that it should guarantee and fulfil the desired security requirements for the quantum computing models. Cryptographic primitives that are secure both in the standard computational model and the quantum model are called *post-quantum* *secure.* There are recent efforts to standardize post-quantum primitives by various institutions, such as the National Institute of Standards and Technology (NIST) in the United States. However, post-quantum security requires a trade-off in terms of performance and efficiency.

In general, cryptography comes in two flavours: symmetric and asymmetric (or public-key cryptography). Quantum computing affects both, but mostly public-key primitives. Starting from 5G, public-key protocols have become an integral part of the core of wireless networks. Contemporary asymmetric cryptography is based on mathematical problems such as integer factorization and the discrete logarithm problem that can be solved quickly on a quantum computer. These methods need to be replaced for post-quantum secure versions.

Symmetric cryptography involves primitives, such as encryption and message authentication. Fortunately, contemporary primitives are only lightly affected by quantum algorithms. However, some modifications are needed in order to preserve the current security level. Due to Grover's algorithm [Grover, 1996], the key length needs to be doubled in the quantum model (i.e. 128-bit encryption to 256-bit encryption). In practice, such an increase incurs a modest performance penalty. Otherwise, the same symmetric cryptographic primitives can be applied.

Asymmetric cryptography involves primitives such as key exchange, public-key encryption and digital signatures. Contemporary primitives are typically based on elliptic curves and the elliptic curve Diffie-Hellman problem (ECDH), which is relatively efficient and has compact public and private keys. These methods are not secure in the quantum computing model and need to be replaced with less efficient ones. Currently, there are different alternatives with their own pros and cons.

With regard to public-key cryptography in 6G EI, choices need to be made between methods that provide efficient key generation, relatively compact keys or signatures or efficient operations (encryption, signing, etc.), but not all at the same time. Their efficient use in post-quantum secure wireless networks remains a future challenge.

2.4. Privacy Challenges in 6G EI

The protection of privacy on the edge can be challenging. Devices collect huge amounts of personally identifiable information (PII), which can potentially be used to monitor every action of an individual. Thus, end-to-end encryption should be applied to protect the users from those that seek to enact harm, and computation should be performed only by trusted entities. Privacy laws, such as GDPR, also require that PII needs to be protected. The GDPR also mandates that the system has to adopt a *privacy-by-design* approach; the whole system has to be designed from the ground up to protect the privacy of its users.

For ML models that are trained exclusively on sensitive information, the protection should not refer only to the samples used for training or to the input to a classifier. In many situations, the machine learning model itself needs to be protected since PII can be inferred directly from the model using, e.g., model inversion or extraction, where information about the training data is deduced from the model [Fredrikson et al., 2014, 2015] or membership inference, where the owner of a specific training data point is deduced [Shokri et al., 2017]. In the contemporary setting, the training data is typically seen by the training party.

Privacy-preserving ML attempts to enable model training without the disclosure of the private training set. In general, there are two approaches to the protection of PII: its removal using anonymization techniques and protection using cryptographic protocols. Anonymization techniques [Samarati and Sweeney, 1998, Machanavajjhala et al., 2007, Li et al., 2007] remove any PII from the training data by grouping individuals so that it is impossible to identify a single individual from the group. However, for certain use cases, such a grouping may render classification tasks impossible or limit its accuracy.

The most widely used anonymization approach to prevent the leakage of PII is differential privacy [Dwork et al., 2006]. In general, differential privacy inserts noise into the training data in order to prevent the extraction of PII. It is an efficient method of preventing PII leakage but can lead to performance issues regarding training [Wei et al., 2020], as well as poor performance of the final model. In addition, differential privacy cannot be applied in all use cases; it has strict limitations for certain types of data [Liu et al., 2021] and can be totally inapplicable if the model is trained on data from a single individual.

Another widely adopted method for limiting access to the training data is to apply FL. In FL, training data is not transferred to a centralized server. Instead, a local model is trained close to the data collection. Then, multiple local models are transferred to the server, and a final global model is computed using the local models. Since the training data does not leave the collection site, FL offers better privacy guarantees than the centralized training approach. However, it should be noted that FL does not offer perfect privacy guarantees: the local models can be abused to infer information about the training data using, e.g. model inversion and membership inference attacks [Shokri et al., 2017]. FL is also highly susceptible to poisoning attacks.

On the other hand, cryptographic schemes can also be applied to protect sensitive training data. For certain models, homomorphic encryption (HE) [Rivest et al., 1978, Gentry, 2009] can be applied to perform the training on encrypted data. Thus, the confidentiality of both the training data and the final model is preserved. The deployment of the fully homomorphic encryption requires significant computational capabilities, but, in some use cases, its limited or lightweight version may be efficient and effective [Liu et al., 2016, Phong et al., 2018, Gilad-Bachrach et al., 2016].

Functional encryption (FE) [Boneh et al., 2011] is similar to HE, but the output of the computation is not hidden. It is also significantly more efficient than HE, but there are limitations: currently, it is not known how to enable efficient FE for other than linear or quadratic functions.

Secure multiparty computing (MPC) is another approach that can protect the confidentiality of the training data. In MPC, multiple parties jointly compute a function on hidden data and learn only the output of the computation. Thus, the training data can remain confidential while the model training is performed by running MPC. The drawback of MPC is the large amount of communication required while running the protocol. If the number of parties is limited, the computation is relatively efficient - especially compared to HE - but does not scale well with the number of participants due to the communication costs. Contrary to HE and FE, secure MPC is an interactive protocol; it requires the computing parties to be online and is a feasible choice only if interactivity between the data contributors is possible.

The benefit of the cryptographic approach compared to anonymization is that no noise is added to the training data, resulting in better accuracy. However, it should be noted that the discussed methods are costly in terms of computation and communication, and further studies are needed in order to

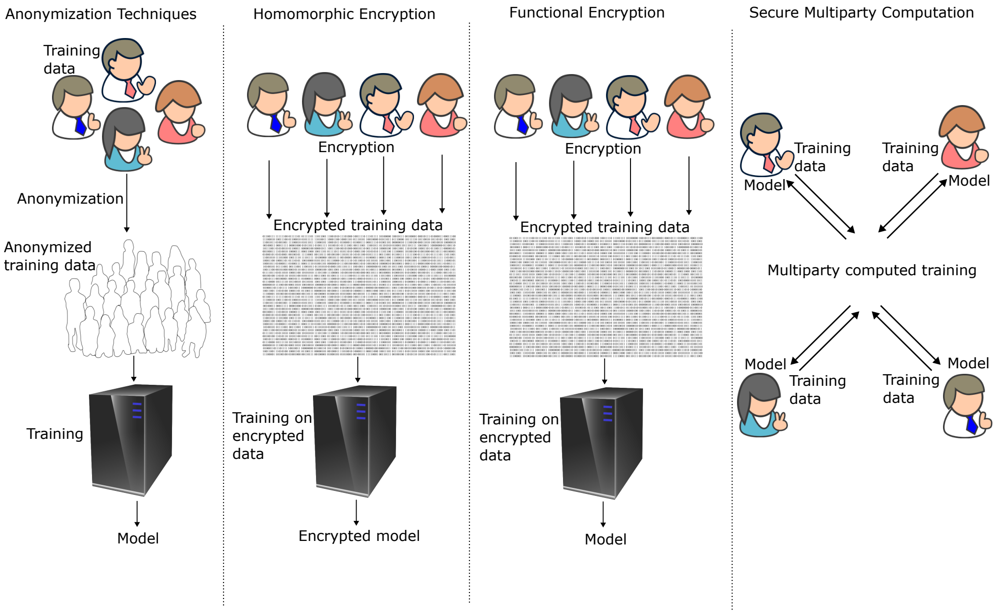

Figure 2.4: Methods for privacy-preserving machine learning.

assess their feasibility in EI. Privacy-protection methods presented in this section have been collectively depicted in Fig. 2.4.

2.5. Trust Challenges in 6G EI

Trust raises challenges for integration via the usage of EI in the 6G era. For example, 6G is expected to provide an interconnected computing platform where several network elements and service providers will require frequent collaboration and communication; it is highly vital to establish an embedded trust management mechanism among them. Also, EI systems demand communication and exchange of data and local models, which raise trust challenges in collecting, storing, and processing. Notably, trust formation is done via advanced technologies, ensuring security.

Trust is critical in the 6G era, especially when EI is in use. Applying EI cannot guarantee trust in a cloud-based system when the system needs communication from a set of different devices and resources. Also, with the next generation of IoT systems, the requirements for collaboration [Ziegler et al., 2021] raise the trust in communication, data generation, and computation. Hence, if a suitable trust management mechanism is placed, it will minimise the need for intermediaries and eventually help in the overall cost reduction of the heterogeneous massive-scale IoT application. Notably, the swift growth and the numerous demands of FL in EI raise trust challenges to deploy the technology in the 6G era. Therefore, the 6G white paper [Ylianttila et al., 2020] mentions the importance of trust in increasing security in 6G via defining trust modelling, policies, and mechanisms. Also, [Porambage et al., 2021b,a] points out the need for trust network topologies for forming EI services, including authentication, access control, data integrity, and mutual platform verification. The 6G architecture proposed by [Ziegler et al., 2020] follows the heterogeneous cloud (het-cloud) computing environment, which will be comprised of various subnetworks, edge clouds, private clouds, central cloud, and public cloud. In such an environment, trustworthiness challenges arise due to the heterogeneous and distributed het-cloud architecture components connected from different locations and operated/managed by diverse stakeholders. Besides, the huge scale of millions of subnetworks and billions of data sources (sensors) raises further trust challenges. Zero-trust approach (ZTA), Syed et al. [2022], emphasizes trust management in every component of a communication system by requiring continuous verification and validation of the identity and security posture of users, devices, and applications at every interaction, ensuring that trust is never assumed and security is maintained throughout the communication process. Therefore, the creation of multivendor trust domains via the cloud stack and topologies that connect untrusted domains as subnetworks of data generation is required. In particular, the data generation side, including sensors, devices, and human-machine interfaces, is the origin of threats in trust data collection. From the network side, trust is a question for subnetworks that require secure definitions, such as authentication and identity.

The trust related to EI is from data and models via procedures, including collection, storage, and process. Due to the vulnerabilities of the sensor networks in attacks, the guarantee of trust in collected data is a huge question, especially when applying EI [Zhang et al., 2021]. For example, due to the diversity of sensor networks, it may become hard to protect all the devices, and thus, the possibility of adversary attacks also increases. Besides that, bad environmental conditions can also cause hurdles in ensuring the correctness of collected data. Therefore, to maintain the required trust in collected data, it is highly critical to detect and recognize the sensor failures, which will help eliminate the noise data and improve the overall system performance. In addition, maintaining data storage raises security issues concerning the integrity and therefore requires suitable solutions, e.g., since the storage of collected data in centralized locations leads to security concerns due to data integrity or single-point failure of storage, a distrusted storage mechanism can be useful to increase the data/resources availability and can improve the performance by performing dynamic load balancing. Interestingly, leveraging EI in heterogeneous networks leads to issues related to trust in exchange for training models. For example, when deploying FL, the most significant challenges affecting the trust are single-point failure of aggregator, malicious clients or false data and lack of incentives [Bagdasaryan et al., 2020].

The formation of trust is frequently based on reputation; however, with the growth of advanced technologies, trust can be shaped by novel technologies. In particular, the trust in current works is mainly based on logs revealing the history of operations. Blockchain technology [Ylianttila et al., 2020, Porambage et al., 2021b, Nguyen et al., 2021b] can be a promising solution for trust formation in the 6G era, especially applying EI. Particularly, the collaboration of service providers requires trust that can be enabled by leveraging blockchain technology [Nguyen et al., 2022, 2019]. Moreover, due to the immutability and transparency, blockchain supports audits by keeping track of records to build trust in communication and verification. Also, via the integration between blockchain and FL [Kim et al., 2020, Lu et al., 2020, Nguyen et al., 2021a], the trust of EI in 6G is an example case for the promise of this technology to address trust challenges for 6G EI. In the concern of trust-based hardware, Trusted Execution Environments (TEE) is another notable trusted solution for confidentiality and integrity in specific network environments [Ziegler et al., 2021]. Like this consideration, [Ylianttila et al., 2020] mentions pre-defined liabilities as the trusted party to handle various liability-related challenges, e.g., safety and work health.

2.6. Security Standardization for EI and 6G

Security-related standardization for EI and 6G is still in its infancy. However, for data privacy and security in general, various standards, such as ISO/IEC TS 27570 [ISO/IEC, 2022a] and ISO/IEC DIS 27400 [ISO/IEC, 2022b] have been developed by, e.g., the International Organization for Standardization (IOS) and the International Electrotechnical Commission (IEC). The former provides guidelines and recommendations for the management of privacy and the usage of standards, while the latter provides guidance for principles and controls to provide private and secure IoT systems, services and solutions [ISO/IEC, 2022b]. Furthermore, the European Telecommunications Standards Institute (ETSI) has recently unveiled ETSI EN 303 645 [ETSI, 2020] to provide cybersecurity standards and a baseline for IoT consumer products and certification schemes. While these guidelines do not specifically refer to Edge AI for 6G, they are applicable for developing private and secure edge AI models and algorithms to provide trustworthy products and services.

ETSI Industry Specification Group (ISG) Multi-Access Edge Computing (MEC) group recently published a white paper on MEC security [ETSI, 2022] highlighting the status of the ongoing standardization activities, as well as potential future trends for MEC security. Along with the evolution of the next-generation 6G networks, the report presented insight into the security standardization needed for edge computing-related technologies. For example, the privacy-preserving AI/ML algorithms at the edge network are vital for securing the users' critical information. Therefore, standardization efforts are needed to develop trustworthy AI/ML models for edge networks. Moreover, DLTs are an important security enabler for 6G and edge intelligence-enabled systems, e.g., by providing decentralized trust. To maximize the benefits of DLTs, efforts are required for standardizing various security-related processes, e.g., for smart contracts-based mechanisms.

NIST has been at the forefront towards working on various standards for post-quantum cryptography (PQC) solutions, e.g., standards for PQC algorithms that are acceptable for both quantum and classical systems [Alagic et al., 2020]. Related to the 6G security standards, ITU recently published a technical paper on the roadmap of 5G security standardization where the emphasis was also given to analyzing and identifying potential gaps in 5G security standards [ITU, 2022]. 5G IA released a white paper presenting the European vision and recommendation on future 6G ecosystems for policymakers and businesses that cover various dimensions of 6G networks, including the need for network and service security and trustworthiness for next-generation 6G networks [The 5G Infrastructure Association, 2021]. Furthermore, various research projects worldwide, such as 6G Flagship, HEXA-X, and MSIT 6G, among others, are aiming to contribute towards various security standardization activities in the coming future [Katz et al., 2018, Uusitalo et al., 2021, Castro, 2020].

2.7. Conclusion

The incorporation of EI with future 6G networks is vital from the perspective of enabling massive-scale smart and connected IoT applications with the key requirements of ultra-low latency, reliability, faster data analytics, and intelligent distributed decision-making. Such smart and hyperconnected digital environments are assumed to be highly complex and, therefore, vulnerable to various threats. For this, it is crucial to design and implement sufficient security mechanisms for securing intelligent 6G-enabled applications and communication architectures. In this chapter, we have provided an overview of the potential security, privacy and trust issues for 6G EI systems, such as threats related to computational offloading and distributed service provisioning on the edge, vulnerabilities due to the complex integration of various enabling technologies, and trust issues when multiple devices and stakeholders providers share information and resources using a common platform. In addition to the identified security, privacy and trust issues, the work also briefly presents some of the potential solutions to these issues. Moreover, a brief discussion about ongoing security-related standardization activities for edge intelligence and 6G systems is provided.

Bibliography

Mainak Adhikari, Ambigavathi Munusamy, Abhishek Hazra, Varun G Menon, Vijay Anavangot, and Deepak Puthal. Security in edge-centric intelligent internet of vehicles: Issues and remedies. *IEEE Consumer Electronics Magazine*, 11(6):24–31, 2022. doi: 10.1109/MCE.2021.3116415.

Muhammad Waseem Akhtar, Syed Ali Hassan, Rizwan Ghaffar, Haejoon Jung, Sahil Garg, and M Shamim Hossain. The shift to 6g communications: vision and requirements. *Human-centric Computing and Information Sciences*, 10 (1):1–27, 2020.

Ian F. Akyildiz, Ahan Kak, and Shuai Nie. 6g and beyond: The future of wireless communications systems. *IEEE Access*, 8:133995–134030, 2020. doi: 10.1109/ACCESS.2020.3010896.

Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the nist post-quantum cryptography standardization process. *US Department of Commerce, NIST*, 2020.

László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, STOC '91, page 21–32, New York, NY, USA, 1991. Association for Computing Machinery. ISBN 0897913973. doi: 10.1145/103418.103428. URL https://doi.org/10.1145/103418.103428.

Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. How to backdoor federated learning. In Silvia Chiappa and Roberto Calandra, editors, *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics*, volume 108 of *Proceedings of Machine Learning Research*, pages 2938–2948. PMLR, 26–28 Aug 2020.

Jagadeesha R. Bhat and Salman A. Alqahtani. 6g ecosystem: Current status and future perspective. *IEEE Access*, 9:43134–43167, 2021. doi: 10.1109/ACCESS.2021.3054833.

Battista Biggio, Giorgio Fumera, and Fabio Roli. Security evaluation of pattern classifiers under attack. *IEEE Transactions on Knowledge and Data Engineering*, 26(4):984–996, 2014. doi: 10.1109/TKDE.2013.57.

Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *Theory of Cryptography*, pages 253–273, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. ISBN 978-3-642-19571-6.

Alessio Botta, Walter de Donato, Valerio Persico, and Antonio Pescapé. Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, 56:684–700, 2016.

C. Castro. Korea lays out plan to become the first country to launch 6g, 2020. https://www.6gworld.com/exclusives/korea-lays-out-plan-to-become-the-first-country-tolaunch-6g/ [Accessed: (25.05.2023)].

Shuiguang Deng, Hailiang Zhao, Weijia Fang, Jianwei Yin, Schahram Dustdar, and Albert Y. Zomaya. Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. *IEEE Internet of Things Journal*, 7, 2020.

Jasenka Dizdarevic, Francisco Carpio, Admela Jukan, and Xavi Masip-Bruin. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. *ACM Computing Survey*, 51:1–29, 2019. doi: https://doi.org/10.1145/3292674.

Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, pages 265–284, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. ISBN 978-3-540-32732-5.

ETSI. CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements . *ETSI EN 303 645 V2.1.1 (2020-06)*, 2020.

ETSI. MEC security; Status of standards support and future evolutions. *ETSI White Paper No. 46*, 2022.

Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 1322–1333, New York, NY, USA,

2015. Association for Computing Machinery. ISBN 9781450338325. doi: 10.1145/2810103.2813677. URL https://doi.org/10.1145/2810103.2813677.

Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart. Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 17–32, San Diego, CA, August 2014. USENIX Association. ISBN 978-1-931971-15-7.

Rosario Gennaro. Verifiable outsourced computation: A survey. In *Proceedings of the ACM Symposium on Principles of Distributed Computing*, PODC '17, page 313, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349925. doi: 10.1145/3087801.3087872. URL https://doi.org/10.1145/3087801.3087872.

Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery. ISBN 9781605585062. doi: 10.1145/1536414.1536440.

Ran Gilad-Bachrach, Nathan Dowlin, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In Maria Florina Balcan and Kilian Q. Weinberger, editors, *Proceedings of The 33rd International Conference on Machine Learning*, volume 48 of *Proceedings of Machine Learning Research*, pages 201–210, New York, New York, USA, 2016. PMLR. URL https://proceedings.mlr.press/v48/gilad-bachrach16.html.

Shafi Goldwasser, Michael P. Kim, Vinod Vaikuntanathan, and Or Zamir.

Planting undetectable backdoors in machine learning models, 2022. URL https://arxiv.org/abs/2204.06974.

Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery. ISBN 0897917855. doi: 10.1145/237814.237866. URL https://doi.org/10.1145/237814.237866.

ISO/IEC. ISO/IEC TS 27570:2021 Privacy protection — Privacy guidelines for smart cities. *Guidelines*, 2022a.

ISO/IEC. ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines. *Guidelines*, 2022b.

ITU. XSTP-5GsecRM 5G security standardization roadmap. *ITU-T, Technical Paper*, 2022.

Marcos Katz, Marja Matinmikko-Blue, and Matti Latva-Aho. 6genesis flagship program: Building the bridges towards 6g-enabled wireless smart society and ecosystem. In *2018 IEEE 10th Latin-American Conference on Communications (LATINCOM)*, pages 1–9, 2018. doi: 10.1109/LATINCOM.2018.8613209.

Latif U. Khan, Walid Saad, Dusit Niyato, Zhu Han, and Choong Seon Hong. Digital-twin-enabled 6g: Vision, architectural trends, and future directions. *IEEE Communications Magazine*, 60(1):74–80, 2022. doi: 10.1109/MCOM.001.21143.

H. Kim, J. Park, M. Bennis, and S. Kim. Blockchained on-device federated learning. *IEEE Communications Letters*, 24(6):1279–1283, 2020. doi: 10.1109/LCOMM.2019.2921755.

Mohammed Laroui, Boubakr Nour, Hassine Moungla, Moussa A. Cherif, Hossam Afifi, and Mohsen Guizani. Edge and fog computing for IoT: A survey on current research activities future directions. *Computer Communications*, 180:210–231, 2021. doi: https://doi.org/10.1016/j.comcom.2021.09.003.

Khaled B. Letaief, Yuanming Shi, Jianmin Lu, and Jianhua Lu. Edge artificial intelligence for 6g: Vision, enabling technologies, and applications. *IEEE Journal on Selected Areas in Communications*, 40(1):5–36, 2022. doi: 10.1109/JSAC.2021.3126076.

Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering*, pages 106–115, 2007. doi: 10.1109/ICDE.2007.367856.

Bo Liu, Ming Ding, Sina Shaham, Wenny Rahayu, Farhad Farokhi, and Zihuai Lin. When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys*, 54(2), 2021. ISSN 0360-0300. doi: 10.1145/3436755. URL https://doi.org/10.1145/3436755.

Ximeng Liu, Rongxing Lu, Jianfeng Ma, Le Chen, and Baodong Qin. Privacy-preserving patient-centric clinical decision support system on naïve bayesian classification. *IEEE Journal of Biomedical and Health Informatics*, 20(2):655–668, 2016. doi: 10.1109/JBHI.2015.2407157.

Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. Blockchain and federated learning for privacy-preserved data sharing in industrial iot. *IEEE Transactions on Industrial Informatics*, 16(6):4177–4186, 2020. doi: 10.1109/TII.2019.2942190.

Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data*, 1(1):3–es, 2007. ISSN 1556-4681. doi: 10.1145/1217299.1217302. URL https://doi.org/10.1145/1217299.1217302.

Mithun Mukherjee, Rakesh Matam, Constandinos X. Mavromoustakis, Hao Jiang, George Mastorakis, and Mian Guo. Intelligent edge computing: Security and privacy challenges. *IEEE Communications Magazine*, 58(9):26–31, 2020. doi: 10.1109/MCOM.001.2000297.

Garima Nain, K.K. Pattanaik, and G.K. Sharma. Towards edge computing in intelligent manufacturing: Past, present and future. *Journal of Manufacturing Systems*, 62:588–611, 2022.

Dinh C. Nguyen, Ming Ding, Quoc-Viet Pham, Pubudu N. Pathirana, Long Bao Le, Aruna Seneviratne, Jun Li, Dusit Niyato, and H. Vincent Poor. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, 8(16):12806–12825, 2021a. doi: 10.1109/JIOT.2021.3072611.

Huong Nguyen, Tri Nguyen, Teemu Leppänen, Juha Partala, and Susanna Pirttikangas. Situation awareness for autonomous vehicles using blockchain-based service cooperation. In Xavier Franch, Geert Poels, Frederik Gailly, and Monique Snoeck, editors, *Advanced Information Systems Engineering*, pages 501–516, Cham, 2022. Springer International Publishing. ISBN 978-3-031-07472-1.

Tri Nguyen, Lauri Lovén, Juha Partala, and Susanna Pirttikangas. *The Intersection of Blockchain and 6G Technologies*, pages 393–417. Springer International Publishing, Cham, 2021b. ISBN 978-3-030-72777-2. doi: 10.1007/978-3-030-72777-2_18. URL https://doi.org/10.1007/978-3-030-72777-2_18.

Tri Hong Nguyen, Juha Partala, and Susanna Pirttikangas. Blockchain-based mobility-as-a-service. In *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–6, 2019. doi: 10.1109/ICCCN.2019.8847027.

Jianli Pan and James McElhannon. Future Edge Cloud and Edge Computing for Internet of Things Applications. *IEEE Internet of Things Journal*, 5, 2018.

Le Trieu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shiho Moriai. Privacy-preserving deep learning via additively homomorphic encryption. *IEEE Transactions on Information Forensics and Security*, 13(5): 1333–1345, 2018. doi: 10.1109/TIFS.2017.2787987.

Nikolaos Pitropakis, Emmanouil Panaousis, Thanassis Giannetsos, Eleftherios Anastasiadis, and George Loukas. A taxonomy and survey of attacks against machine learning. *Computer Science Review*, 34:100199, 2019. ISSN 1574-0137. doi: https://doi.org/10.1016/j.cosrev.2019.100199. URL https://www.sciencedirect.com/science/article/pii/S1574013718303289.

Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Livanage, and Mika Ylianttila. 6g security challenges and potential solutions. In *2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, pages 622–627, 2021a. doi: 10.1109/EuCNC/6GSummit51104.2021.9482609.

Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila. The roadmap to 6g security and privacy. *IEEE Open Journal of the Communications Society*, 2:1094–1122, 2021b. doi: 10.1109/OJCOMS.2021.3078081.

Zakria Qadir, Khoa N Le, Nasir Saeed, and Hafiz Suliman Munawar. Towards 6g internet of things: Recent advances, use cases, and open challenges. *ICT Express*, 2022.

Partha Pratim Ray. A perspective on 6g: Requirement, technology, enablers, challenges and future road map. *Journal of Systems Architecture*, 118: 102180, 2021.

Ronald L Rivest, Len Adleman, Michael L Dertouzos, et al. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

Pierangela Samarati and Latanya Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression, 1998.

Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 3–18, 2017. doi: 10.1109/SP.2017.41.

Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylianttila. Ai and 6g security: Opportunities and challenges. In *2021 Joint European Conference on Networks and Communications 6G Sum-*

mit (EuCNC/6G Summit), pages 616–621, 2021. doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*, 78:964–975, 2018.

Yuanyuan Sun, Jiajia Liu, Jiadai Wang, Yurui Cao, and Nei Kato. When machine learning meets privacy in 6g: A survey. *IEEE Communications Surveys Tutorials*, 22(4):2694–2724, 2020. doi: 10.1109/COMST.2020.3011561.

Naeem Firdous Syed, Syed W. Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, and Robin Doss. Zero trust architecture (zta): A comprehensive survey. *IEEE Access*, 10:57143–57179, 2022. doi: 10.1109/ACCESS.2022.3174679.

Getenet Tefera, Kun She, Maya Shelke, and Awais Ahmed. Decentralized adaptive resource-aware computation offloading caching for multi-access edge computing networks. *Sustainable Computing: Informatics and Systems*, 30, 2021.

The 5G Infrastructure Association. European Vision for the 6G Network Ecosystem. *White Paper*, 2021.

Vale Tolpegin, Stacey Truex, Mehmet Emre Gursoy, and Ling Liu. Data poisoning attacks against federated learning systems. In Liqun Chen, Ninghui Li, Kaitai Liang, and Steve Schneider, editors, *Computer Security – ESORICS 2020*, pages 480–501, Cham, 2020. Springer International Publishing. ISBN 978-3-030-58951-6.

Mikko A. Uusitalo, Mårten Ericson, Björn Richerzhagen, Elif Ustundag Soykan, Patrik Rugeland, Gerhard Fettweis, Dario Sabella, Gustav Wikström, Mauro Boldi, Marie-Helene Hamon, Hans D. Schotten, Volker Ziegler, Emilio Calvanese Strinati, Matti Latva-aho, Pablo Serrano, Yaning Zou, Gino Carrozzo, Josep Martrat, Giovanni Stea, Panagiotis Demestichas, Aarno Pärssinen, and Tommy Svensson. Hexa-x the european 6g flagship project. In *2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, pages 580–585, 2021. doi: 10.1109/EuCNC/6GSummit51104.2021.9482430.

Kang Wei, Jun Li, Ming Ding, Chuan Ma, Howard H. Yang, Farhad Farokhi, Shi Jin, Tony Q. S. Quek, and H. Vincent Poor. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Transactions on Information Forensics and Security*, 15:3454–3469, 2020. doi: 10.1109/TIFS.2020.2988575.

Mika Ylianttila, Raimo Kantola, Andrei Gurtov, Lozenzo Mucchi, Ian Oppermann, Zheng Yan, Tri Hong Nguyen, Fei Liu, Tharaka Hewa, Madhusanka Liyanage, Ahmad Ijaz, Juha Partala, Robert Abbas, Artur Hecker, Sara Jayousi, Alessio Martinelli, Stefano Caputo, Jonathan Bechtold, Ivan Morales, Andrei Stoica, Giuseppe Abreu, Shahriar Shahabuddin, Erdal Panayirci, Harald Haas, Tanesh Kumar, Basak Ozan Ozparlak, and Juha Röning. 6g white paper: Research challenges for trust, security and privacy, 2020. URL https://arxiv.org/abs/2004.11665.

Guangxue Zhang, Tian Wang, Guojun Wang, Anfeng Liu, and Weijia Jia. Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system. *Concurrency and Computation: Practice and Experience*, 33(7):e5109, 2021. doi: https://doi.org/10.1002/cpe.5109. e5109 cpe.5109.

Shunliang Zhang and Dali Zhu. Towards artificial intelligence enabled 6g: State of the art, challenges, and opportunities. *Computer Networks*, 183:107556, 2020.

Xingzhou Zhang, Yifan Wang, Sidi Lu, Liangkai Liu, Lanyu Xu, and Weisong Shi. OpenEI: An Open Framework for Edge Intelligence. *IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019.

Guangxu Zhu, Dongzhu Liu, Yuqing Du, Changsheng You, Jun Zhang, and Kaibin Huang. Towards an Intelligent Edge: Wireless Communication Meets Machine Learning. *IEEE Communications Magazine*, 58, 2020.

Pengcheng Zhu, Jun Xu, Jiamin Li, Dongming Wang, and Xiaohu You. Learning-empowered privacy preservation in beyond 5g edge intelligence networks. *IEEE Wireless Communications*, 28(2):12–18, 2021. doi: 10.1109/MWC.001.2000331.

Volker Ziegler, Harish Viswanathan, Hannu Flinck, Marco Hoffmann, Vilho Räisänen, and Kimmo Hätönen. 6g architecture to connect the worlds. *IEEE Access*, 8:173508–173520, 2020. doi: 10.1109/ACCESS.2020.3025032.

Volker Ziegler, Peter Schneider, Harish Viswanathan, Michael Montag, Satish Kanugovi, and Ali Rezaki. Security and trust in the 6g era. *IEEE Access*, 9:142314–142327, 2021. doi: 10.1109/ACCESS.2021.3120143.