Privacy-Preserving Data-Driven Learning Models for Emerging Communication Networks: A Comprehensive Survey

Mostafa M. Fouda, *Senior Member, IEEE,* Zubair Md Fadlullah, *Senior Member, IEEE,* Mohamed I. Ibrahem, *Senior Member, IEEE,* and Nei Kato, *Fellow, IEEE.*

***Abstract*—With the proliferation of Beyond 5G (B5G) communication systems and heterogeneous networks, mobile broadband users are generating massive volumes of data that undergo fast processing and computing to obtain actionable insights. While analyzing this huge amount of data typically involves machine and deep learning-based data-driven Artificial Intelligence (AI) models, a key challenge arises in terms of providing privacy assurances for user-generated data. Even though data-driven techniques have been widely utilized for network traffic analysis and other network management tasks, researchers have also identified that applying AI techniques may often lead to severe privacy concerns. Therefore, the concept of privacy-preserving data-driven learning models has recently emerged as a hot area of research to facilitate model training on large-scale datasets while guaranteeing privacy along with the security of the data. In this paper, we first demonstrate the research gap in this domain, followed by a tutorial-oriented review of data-driven models, which can be potentially mapped to privacy-preserving techniques. Then, we provide preliminaries of a number of privacy-preserving techniques (e.g., differential privacy, functional encryption, Homomorphic encryption, secure multi-party computation, and federated learning) that can be potentially adopted for emerging communication networks. The provided preliminaries enable us to showcase the subset of data-driven privacy-preserving models, which are gaining traction in emerging communication network systems. We provide a number of relevant networking use cases, ranging from the B5G core and Radio Access Networks (RANs) to semantic communications, adopting privacy-preserving data-driven models. Based on the lessons learned from the pertinent use cases, we also identify several open research challenges and hint toward possible solutions.**

***Index Terms*—Privacy preservation, machine learning, deep learning, data-driven models, communication networks, federated learning.**

This work was supported in part by the National Science Foundation of the USA under Award 2210252; in part by the National Institute of Information and Communications Technology, Japan, under Grant 22403; and in part by the Natural Sciences and Engineering Research Council of Canada under Award RGPIN-2020-06260. (Corresponding author: Mostafa M. Fouda.)

Mostafa M. Fouda is with the Department of Electrical and Computer Engineering, College of Science and Engineering, Idaho State University, Pocatello, ID 83209, USA (email: mfouda@ieee.org).

Zubair Md Fadlullah is with the Department of Computer Science, Western University, London, Ontario N6G 2V4, Canada (email: zfadlullah@ieee.org).

Mohamed I. Ibrahem is with the School of Computer and Cyber Sciences, Augusta University, Augusta, GA 30912, USA (email: mibrahem@augusta.edu).

Nei Kato is with the Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan (e-mail: kato@it.is.tohoku.ac.jp).

I. Introduction

The field of privacy-preserving data-driven learning models (data-driven models in short) for emerging communication networks is a new area of research that focuses on creating machine learning (ML) models that can learn from sensitive data without compromising the privacy of the individuals in the data. This observation is particularly applicable to emerging communication networks, e.g., cell-free networks [1], space-air-ground integrated networks [2], and Internet of Things (IoT) systems [3], where the data flow across multiple users and devices, and the data sharing may not be possible or even appropriate because of security, privacy or regulatory policies. To effectively deal with this challenge, privacy-preserving technologies (e.g., differential privacy (DP) [4], Homomorphic encryption (HE) [5], secure multi-party computation (SMPC) [6], and federated learning (FL) [7]) are being increasingly adopted in learning models exploiting large-scale, decentralized datasets. For instance, DP is capable of controlled insertion of noise into data so as to protect user privacy while permitting data mining and statistical analysis along with developing ML models [4]. On the other hand, HE and SMPC, which are based on cryptographic techniques, allow secure computations and learning on encrypted data [6]. Particularly in the case of SMPC, a number of parties can compute a function over their private inputs in tandem without having to share their respective input data with others [6]. Such techniques can be regarded as highly useful in emerging communication networks due to their ability to facilitate both the secrecy and data privacy of participating users. On the other hand, FL, a decentralized learning framework, has recently garnered much research attention in both academia and industry since it allows users to train local models based on their private data and share only the model parameters with a centralized server that aggregates model weights to converge to a global model [7]. Variants of FL have emerged based on the varied needs of different communication network scenarios, which range from Beyond 5G (B5G) cellular networks to Unmanned Aerial Vehicles (UAVs) or drones-assisted networks [8]–[11]. Furthermore, there is a growing focus on exploiting semantic communication system models with data-driven models, such as task-oriented semantic communication network (TOSCN) [12], DeepSC-ST (Deep Learning Enabled Semantic Communications with Speech Recognition and Synthesis) [13], and DeepJSCC-V (Deep Learning (DL)-based

Joint Source-Cchannel Coding with Variable code length) [14], with a primary focus on attaining improved network sum rate. Some researchers further assessed the need and conceptualized techniques for incorporating privacy via FL frameworks for semantic communication-enabled networks [15].

While the aforementioned techniques are associated with unique advantages to enforce privacy preservation in data-driven learning models, they are not without shortcomings. For instance, data leakage is a key challenge in these privacy-preserving algorithms that train ML/deep learning (DL) models whereby unauthorized disclosure of sensitive information may take place. Data leakage may be observed when the parameters of a model, which is trained on sensitive data, are exposed to adversaries or unintended parties that were not supposed to. Another common issue of ML/DL techniques, referred to as model overfitting, also appears as a performance bottleneck for privacy-preserving learning algorithms. In such cases, the trained model memorizes the training data in such a manner that it fails to perform when it confronts unseen data. On the other hand, model stealing, i.e., unauthorized access or replication of the model, is another issue with privacy-preserving learning models whereby the models are shared/deployed in a public setting.

In this paper, we address the aforementioned challenges of privacy-preserving data-driven models in the context of emerging communication networks and investigate their unique requirements and characteristics. The roadmap of our work is illustrated in Fig. 1. For interested readers, we first provide the two enabling technologies, i.e., data-driven models and privacy-preserving technologies pertinent to communication networks. This tutorial-oriented approach sets the stage for the core survey to connect the enabling technologies in various network scenarios.

The key contributions of our paper are outlined below.

- We identify the actual research gap in terms of existing privacy-preserving data-driven models and their use in communication networks to protect the data. To the best of our knowledge, there is no joint treatment of these two domains, whereas there have been a number of research works addressing each domain in a separate manner [16]–[38].
- We provide detailed discussions on the different types of data that are typically carried by these networks and the privacy challenges that are associated with them. Overall, this paper provides a comprehensive survey of the research area of privacy-preserving data-driven learning models for emerging communication networks and aims to serve as a useful resource for researchers, practitioners, and policymakers working in this field.
- We also provide state-of-the-art privacy-preserving data-driven learning models for emerging communication networks, highlighting the main challenges and open problems and providing some insights into future research directions in this area. We delineate the various communication network scenarios, including cyber-physical systems, IoT, and semantic communications [15], that have recently started to derive the benefit of applying data-driven and privacy-preserving techniques in tandem.

The structure of the paper is shown in Fig. 3. The remainder of this paper is structured as follows. We present a background on this research topic and delineate the exact research gap in the existing literature in Section II. Then, in Section III, we provide the preliminaries of data-driven models in communication networks. Next, Section IV contains a brief overview of privacy-preserving methods. These preliminaries enable us to offer Section V, which presents privacy-preserving data-driven models for various communication network scenarios along with the lessons learned in the respective network settings. Section VI discusses open research issues followed by potential research directions. Finally, Section VII concludes the paper.

II. Background and Research Gap

Intelligent network functions are regarded as a desired feature in next-generation communication systems and networks. Network intelligence appears as a critical requirement that is anticipated to be seamlessly integrated into B5G and 6G network systems across various levels, ranging from the physical to application layers. In particular, data-driven learning emerged as a revolutionary solution for addressing complex computational problems in emerging networks. While for traditional networks, the network management tasks could be computed locally in network nodes, the growing size of both wired and wireless networks and the exponentially growing traffic volume, coupled with diverse traffic types and ultra-high user mobility, contributed to much higher network dynamism. Conventional optimization and decision-making algorithms often demonstrate that it is difficult to obtain a high-quality solution within a short period of time. In such scenarios, data-driven learning techniques, particularly ML and DL models, emerged as alternative solutions that provide reasonable solutions with regard to standard benchmarks. The underlying algorithms of these models depend on finding specific patterns with non-linear relationships within the data. However, a key issue remains in this conventional ML/DL paradigm, which is the plain-text nature of the input data. In other words, both raw and pre-processed data used to train these learning models are traditionally non-encrypted. When they are encrypted with state-of-the-art cryptography, the patterns contained within the data are not the same, and the data-driven models can no longer be effectively trained. While there has been a number of research works among the ML community to devise an effective solution to encrypt the data to preserve the privacy of data and still be able to train AI models, network practitioners are yet to systematically address this issue in various types of communication networks. There are some scattered research works in the literature that aim to protect the privacy of the input data of the data-driven models [25]–[37]. However, they are not systematically surveyed. To the best of our knowledge, there is no comprehensive survey in the existing literature that identifies this prevalent research gap as demonstrated in Table I. In this paper, we address this research gap of privacy-preserving data-driven learning models for emerging communication networks as demonstrated in Fig. 4. The figure outlines the desired properties of emerging communication network systems, focusing on

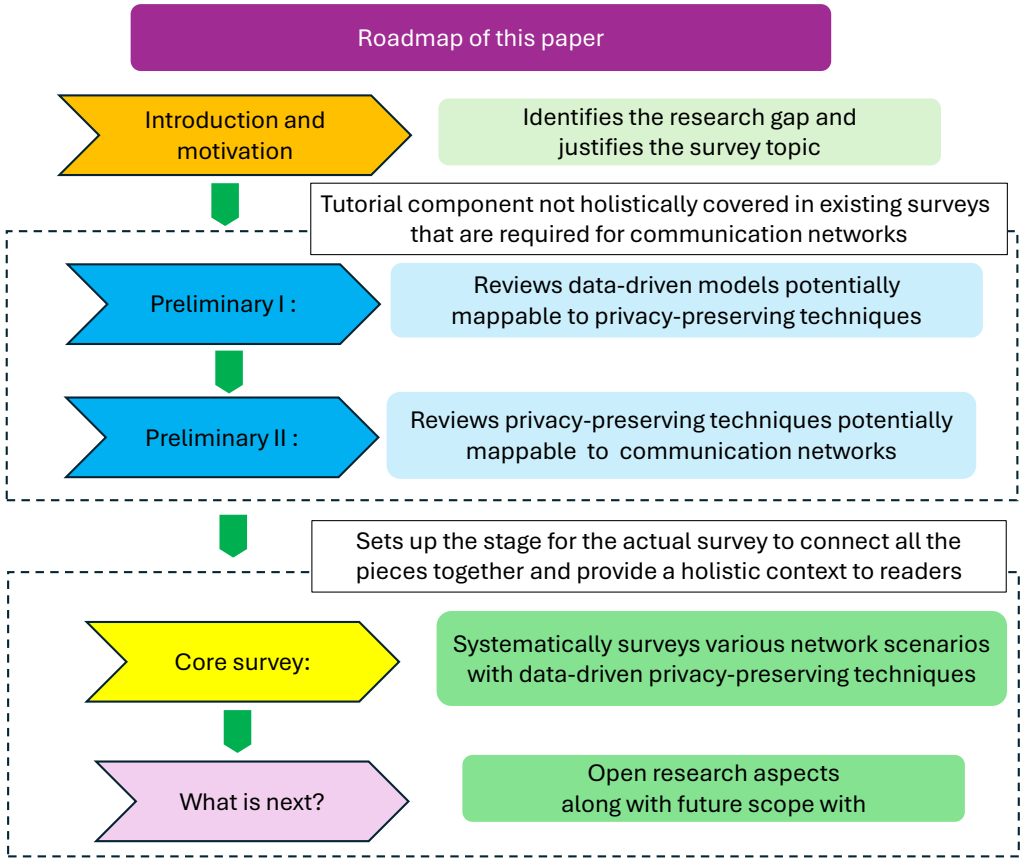


Fig. 1. The road map in this paper is composed of a balanced tutorial of the enabling technologies followed by a survey of those technologies in emerging communication network scenarios.

Quality of Service (QoS), tunable policy, security, and privacy. It highlights the traditional focus on optimizing AI-based QoS and security for dependable communication, considering privacy with legacy methods. This also depicts our shifted focus in this paper to privacy-preserving, data-driven models atop secure QoS by reevaluating ML/DL models for potential privacy leaks, integrating privacy-preserving techniques with data-driven models, and employing FL for privacy in mobile edge and cloud computing. The research gap is currently being considered by a number of researchers through their efforts in conceptualizing privacy-preserving ML/DL models [25]–[37] in the context of communication networks [38].

III. Taxonomy of Data-Driven Models With Viable Privacy-Preserving Mapping for Communication Network Systems

Recent research work in communication networks is witnessing a sharp increase in data-driven, predictive models, from physical and medium access control (MAC) layers of wireless, cellular, and mobile radio access networks to application layers in the backhaul/core networks. ML and DL techniques are currently popular among researchers, in both their vanilla and customized/hybrid forms, to improve each individual block of the communication system or to perform joint optimization of the entire transmitter or receiver nodes. Data-driven models have gained momentum in the areas of signal detection [42], channel estimation and modeling [43], resource allocation [44], end-to-end communication [16], semantic communications [45], and so forth [46]. It is difficult to enumerate all the communication system/network areas where data-driven models were employed to improve network performance. However, it is possible to narrow down the prominent ML/DL techniques that have been applied to these communication systems to formulate and solve various problems ranging from spectral efficiency maximization [47] to quality of service provisioning [48]. In this section, we present a taxonomy of these enabling data-driven modeling techniques in communication network systems that have been or could be potentially applicable to privacy-preserving communication systems and networks.

Fig. 5 presents our proposed taxonomy for data-driven approaches having the capability of (or the potential for) integration with privacy-preserving technologies. As depicted in the figure, we broadly categorize the privacy-preserving-capable data-driven approaches from three perspectives, namely learning approaches, prediction features, and performance measures, respectively. In the remainder of this section, we summarize these learning approaches.

Learning approaches adopted for trust, privacy, as well as security in computing and communications aspects of network

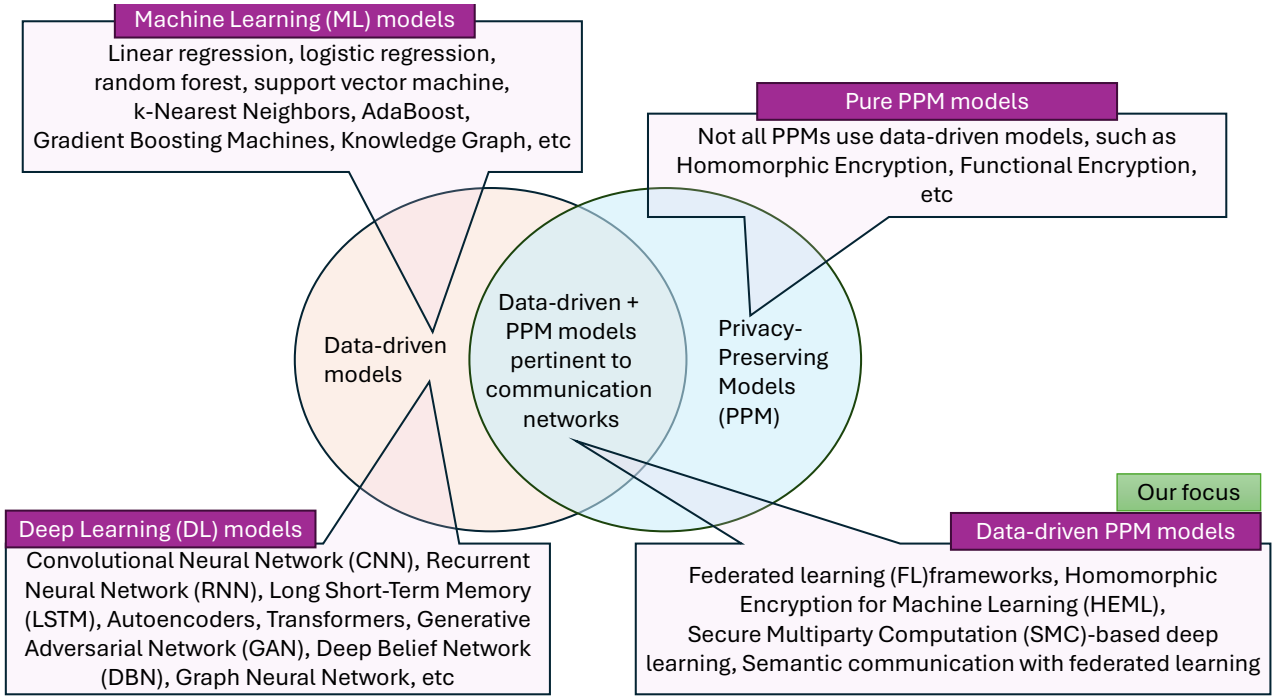


Fig. 2. Targeted focus of our work is on the intersection of data-driven and PPM models that are relevant to emerging communication networks. Note that some of the pure ML/DL/PPM concepts are not used. Some technologies are at the intersection of PPM and data-driven models and only those are elaborated in the core survey in Section V.

TABLE I
COMPARATIVE FEATURES OF EXISTING SURVEYS TO DEMONSTRATE THE RESEARCH GAP AND NEED FOR A NEW SURVEY IN THE AREA OF PRIVACY-PRESERVING DATA-DRIVEN LEARNING MODELS FOR EMERGING COMMUNICATION NETWORKS. NOTATIONS: PRIVACY-PRESERVING (PP), MACHINE LEARNING (ML), DEEP LEARNING (DL), AND FEDERATED LEARNING (FL).

Reference	Objective	PP	Classic ML	DL	PP+DL	Communication networks use-cases considered
Tanuwidjaja *et al.* [25]	Privacy-preserving deep learning on machine learning as a service	✓	×	✓	✓	×
Podschwadt *et al.* [26]	Deep learning architectures for privacy-preserving machine learning with fully Homomorphic encryption	✓	×	✓	✓	×
Falcetta *et al.* [27]	Privacy-preserving deep learning with Homomorphic encryption	✓	×	✓	✓	×
Lee *et al.* [28]	Privacy-preserving machine learning with fully Homomorphic encryption for deep neural network	✓	×	✓	✓	×
Zhang *et al.* [29]	Review of privacy-preserving deep learning based on multiparty secure computation (MPC)	✓	×	✓	✓	×
Sun *et al.* [30]	A survey on machine learning and privacy parameters in 6G environment	✓	✓	✓	×	✓
Guo *et al.* [39]	A survey on space-air-ground-sea integrated network security in 6G	✓	×	×	×	×
Al-Garadi *et al.* [40]	A survey of machine and deep learning methods for internet of things (IoT) security	×	✓	✓	×	✓
Soykan *et al.* [41]	A survey and guideline on privacy enhancing technologies for collaborative machine learning	✓	×	×	- (FL)	×
Our work (this paper)	Survey on privacy-preserving data-driven (machine learning) and deep learning models	✓	✓	✓	✓	✓

systems, are inspired by ML [49]. While ML impacted various application domains, such as computer vision and signal processing, its theoretical foundations on discovering patterns in network data streams, protocol behavior, misconfiguration, and patterns of malicious activity have been instrumental in addressing the communication parameters, as well as the privacy/security parameters. Despite the usefulness of ML methods for privacy and trust in communication systems, the topic of jointly addressing both ML for communication and privacy/security parameters has not been explicitly addressed in the literature. Therefore, it is important to review the enabling ML technologies, which already have the capability of (or may have the potential for integration) with privacy-preserving algorithms. The ML solutions in the communica-

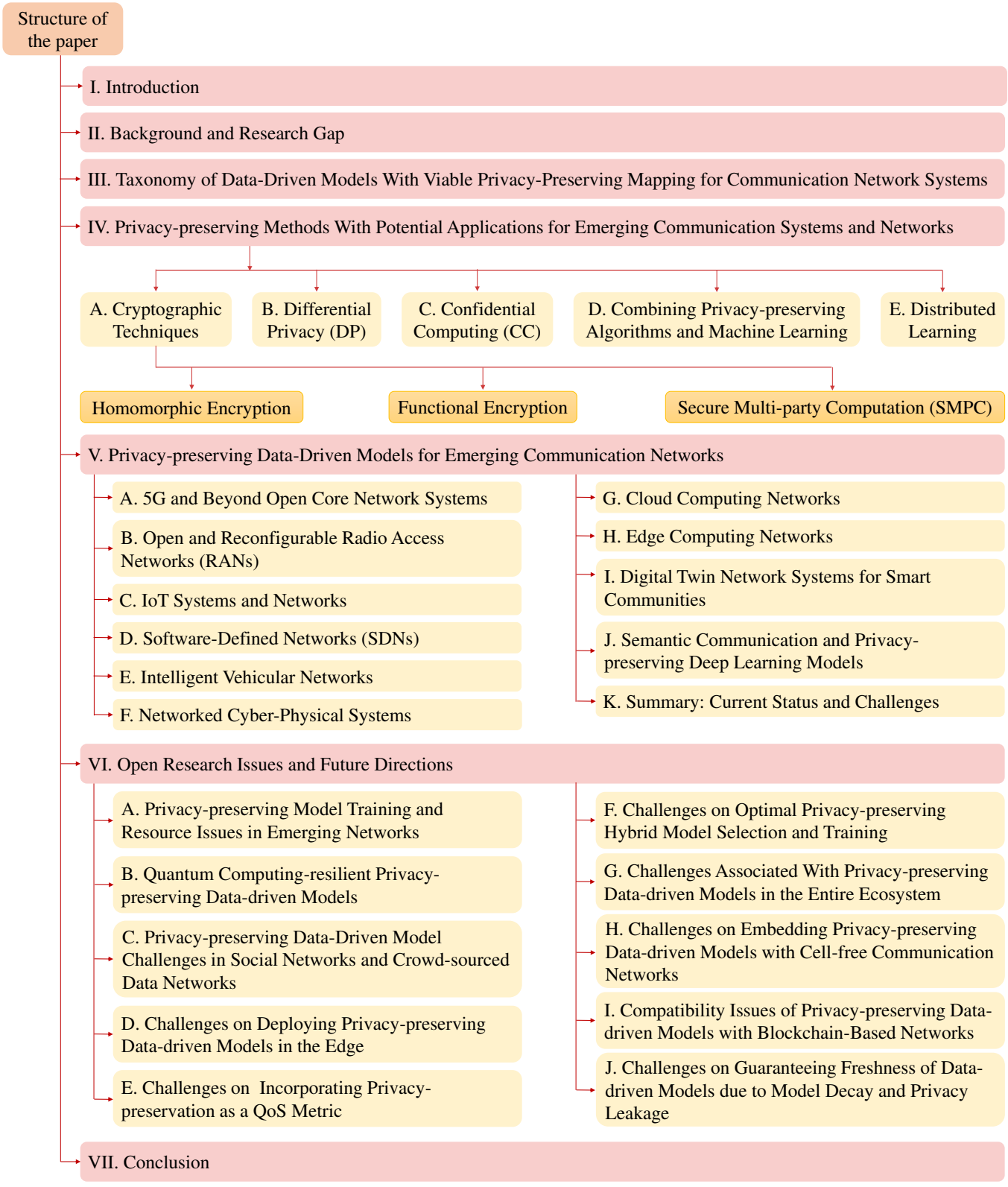


Fig. 3. The structure of this paper.

tion domain of our interest, similar to other disciplines, can be categorized into supervised, unsupervised, semi-supervised, self-supervised, reinforcement, and active learning, as depicted in Fig. 5. The supervised learning paradigm typically facilitates learning from labeled network system data in large network traffic datasets comprising a massive number of traffic

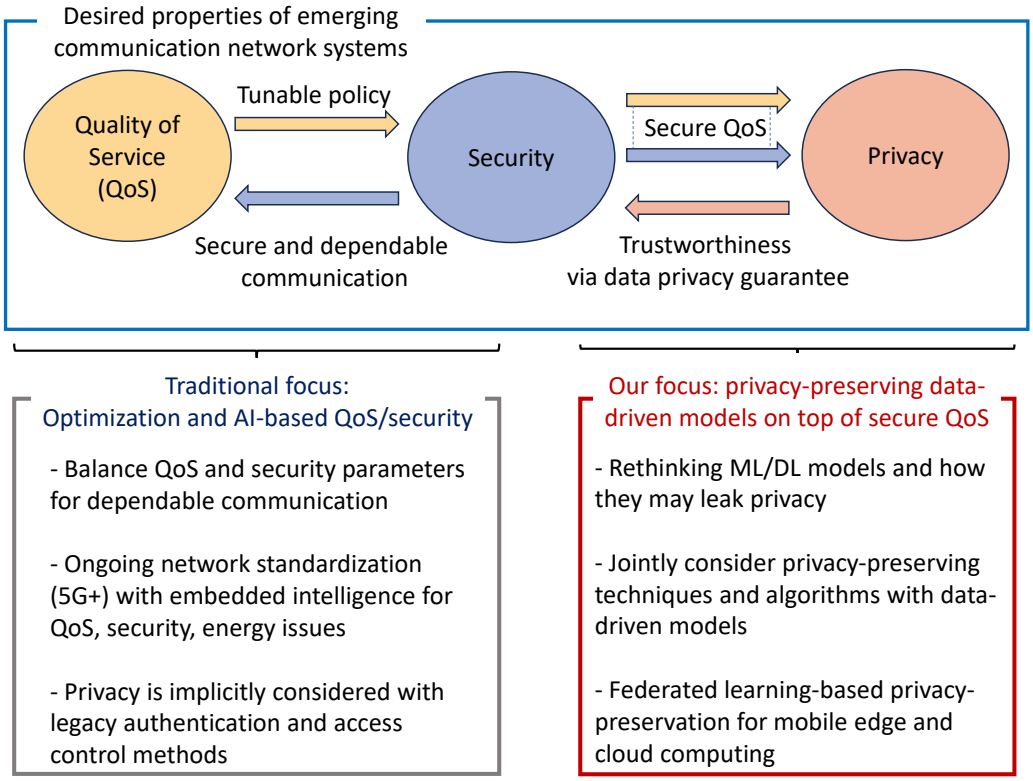


Fig. 4. Our focus in this paper is shown in terms of the prevalent research gap of the overlooked intersection of privacy-preserving foundational techniques and data-driven models with regard to emerging communication systems and networks.

flows. However, localization and mobility patterns of users, in addition to user anonymization, are key privacy elements that may be revealed through such data-driven models. Therefore, contemporary supervised learning techniques for regression and classification tasks need to be carefully integrated with such privacy considerations to construct effective privacy-preserving models based on the training dataset. While supervised models may appear straightforward in carrying out network analytics, the underlying assumptions may or may not hold. For example, Naive Bayes (NB) classification is a simple ML model, which works on some fundamental assumptions with regard to the underlying dataset [50]. If the assumptions are not valid in practice, Naive Bayes classification should not be considered even if its performance appears to be efficient. The need for making valid assumptions for such supervised models is further emphasized for facilitating physical layer privacy and security [51]. Some other notable examples of supervised learning methods in modern network communication settings include linear regression (e.g., for network flow prediction with privacy [52], network throughput prediction [53], and other privacy-preserving network activity prediction tasks [54]–[57]), Logistic Regression (LR) (e.g., for malicious traffic detection [58]), Support Vector Machines (SVMs) (e.g., for wireless transceiver classification [59], wireless signal processing [60], predicted decoupling of WiFi and Long Term Evolution (LTE) in unlicensed spectrum [61]). Decision trees, which are non-linear ML models with simple yet effective decision-based branch and bound approach, are also abundant in the networking literature, with recent research efforts exerted toward secure and scalable edge computing [62], secure and privacy-preserving smart cities [63], and so forth. Random Forests (RFs), which are typically built upon a large number of Decision Trees (DTs), have been applied for network flow classification in both classical and emerging softwarized communication systems [64]–[67] and also for advanced privacy-preserving networking tasks [68]–[71].

A subset of ML techniques, namely the Neural Network (NN)-based structures, also requires a detailed discussion due to their effectiveness in solving a myriad of interesting communication and networking problems, which do not scale well with classical optimization techniques, such as linear programming, convex optimization, stochastic geometry, and geometric programming. The neural network-based learning approaches can be broadly classified into three types, namely artificial neural networks (ANNs), graph neural networks (GNNs), and recurrent neural networks (RNNs). The ANNs cover various structures, such as autoencoders, convolutional neural networks (CNNs), variational autoencoders (VAEs), generative adversarial networks (GANs), and deep belief networks (DBNs). ANN models, when trained with a networking dataset, can capture non-linearities present in the data and can be useful in terms of distinguishing various network features, e.g., malicious vs normal traffic flows, private vs public network flows in the core networks, and so forth. A detailed discussion of these models, without the consideration of privacy-preserving capability, was presented in the coauthors' earlier work in [72]. However, in recent times,

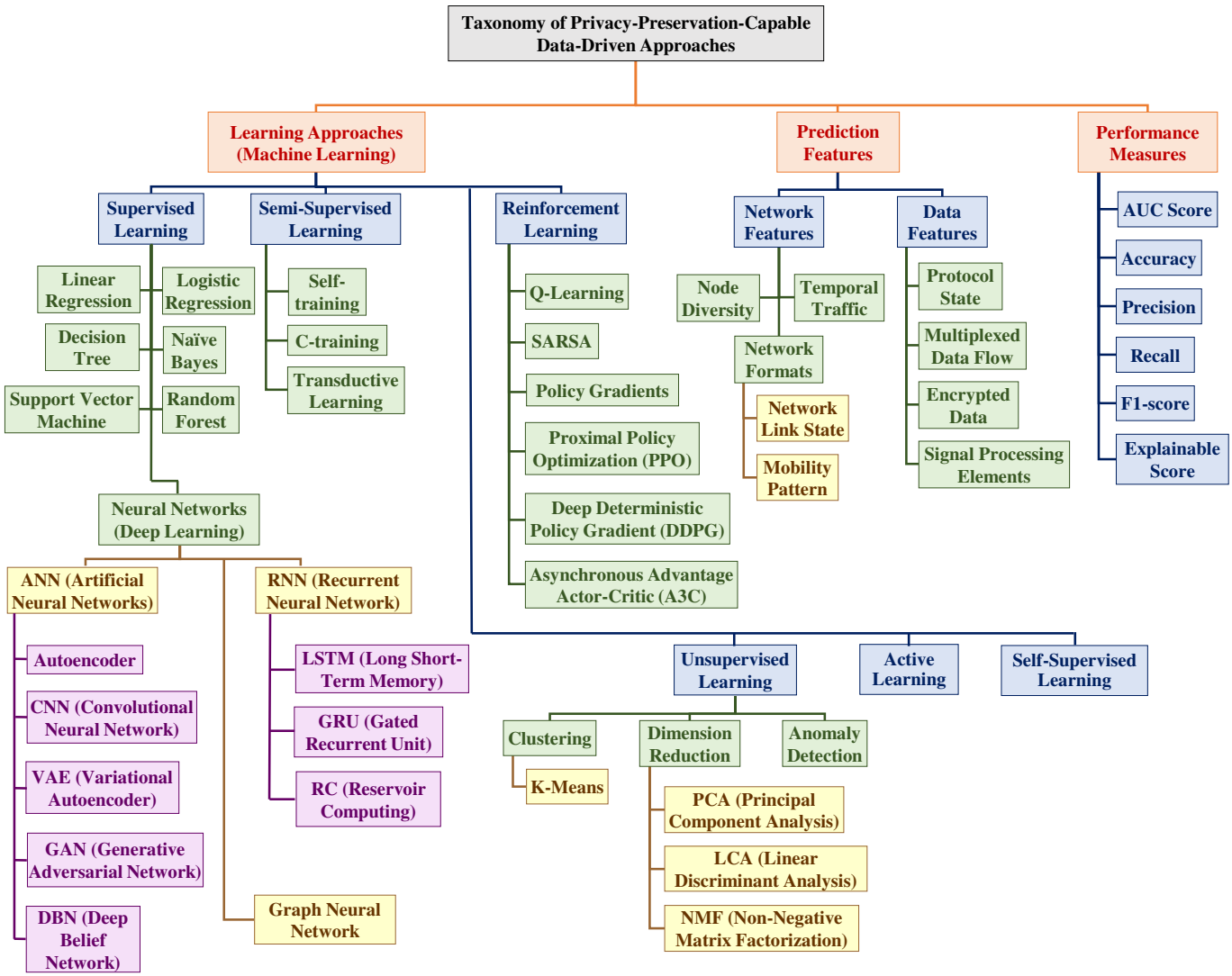


Fig. 5. Taxonomy of data-driven models with potential privacy-preserving integration capability for emerging communication systems and networks. Reconciling with Fig. 2, it is worth noting that some techniques are at the intersection of PPM and data-driven models and only those are elaborated in the core survey in Section V. Other techniques have been mentioned in the taxonomy for the sake of completeness.

there has been a growing trend toward incorporating or at least mapping, the privacy-preserving requirements in many of these ANN-based implementations with regard to network communication systems. For instance, physical layer secret-key generation has been utilized to provide both privacy and security capability to mobile users via AutoEncoders (AEs) in a recent work [73], [74]. The Variational AutoEncoder (VAE), on the other hand, has been recently investigated for privacy-aware communication over a wiretap channel with demonstrated success [75].

IV. Privacy-preserving Methods With Potential Applications for Emerging Communication Systems and Networks

The most important concern in the emergence of data-driven learning models is privacy. Therefore, in this section, we present an overview of various privacy-preserving techniques for communication networks that can be broadly classified into cryptographic methods, DP, confidential computing, and distributed/federated learning to provide privacy-preserving functionality for data-driven and DL models.

A. Cryptographic Techniques

Cryptographic techniques involve mathematical methods and algorithms that can secure communication and protect data, such as text, voice, images, and video, from unauthorized access [41]. These techniques aim to ensure the confidentiality, integrity, and authenticity of information by using encryption, digital signatures, and hash functions. Encryption can be achieved using symmetric or asymmetric keys, while digital signatures and Hash functions provide authenticity and integrity [76]. These techniques are used in various applications, including securing online transactions, protecting email communication, securing data stored in the cloud, etc. [25].

Furthermore, there exist alternative cryptographic methods that allow for secure computations on encrypted data, as

documented in [25], [77]–[79], such as DP, HE, SMPC, and functional encryption (FE) [41]. When choosing a method from this collection, many factors, including the algorithm type of the ML model, the threat model, and the limits on computation and communication overhead imposed by the use case, must be considered. Hence, a comprehensive viewpoint is necessary to determine the most privacy-enhancing resolution.

This section discusses privacy-enhancing technologies, including HE, FE, and SMPC techniques [80]–[82]. These technologies help protect users' privacy and data from attacks. The study focuses on secret sharing in the SMPC framework, which is widely used. SMPC allows data processing while remaining encrypted, while HE and FE systems enable computational operations on ciphertext data without decryption.

1) Homomorphic Encryption

HE is a Paillier cryptosystem-based cryptographic technique that performs computations on encrypted data without requiring the decryption of the data [26], [83], [84], especially when third parties store the data. As shown in Fig. 6(a), HE encrypts the data using a public key and enables the execution of mathematical operations on the encrypted data to ensure its privacy and security. The output of the computation is also encrypted and can only be decrypted by the intended recipient using the decryption key [27]. When the encrypted output is eventually decrypted, it will yield the same outcome as if the operations were conducted on the original unencrypted data. HE includes various encryption techniques such as partially HE (PHE), somewhat HE (SWHE), and fully HE (FHE) [28].

PHE [85] allows for a number of operations on encrypted data, limited to either addition or multiplication. Thus, PHE is categorized into two groups: additive HE and multiplicative HE [83], [84]. It is commonly employed in practical applications like remote keyword search and privacy-preserving data aggregation due to its minimal computational requirements. On the other hand, FHE is computationally expensive; it is less efficient compared to PHE and SWHE [86], making it unsuitable for time-sensitive applications, especially when the message size is substantial [6]. SWHE provides support for a variety of arithmetic and logic operations [87], making it successfully applied in real-time applications, such as those in finance, medicine, and recommendation systems. Despite the long-standing challenge of designing FHE, several studies have been conducted on HE systems utilizing lattices with Learning With Errors (LWE) and Ring Learning With Errors (Ring-LWE) problems, as well as schemes involving integers with the approximate Greatest Common Divisor (GCD) problem [87]–[93].

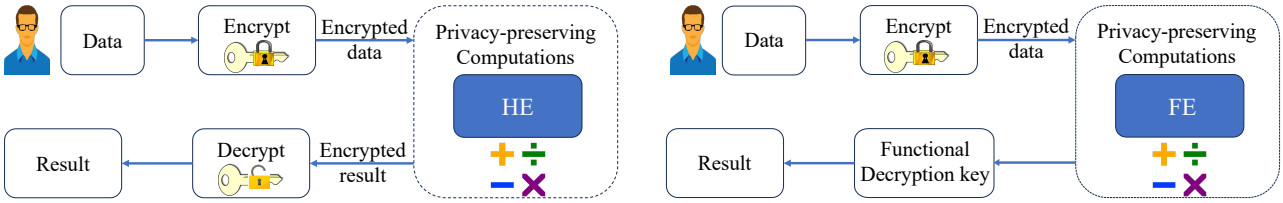
Due to HE's capability to perform computations on encrypted data while preserving privacy, it has a wide range of practical applications, including protecting cloud computing, enabling SMPC, and facilitating secure data analysis. HE facilitates the transmission and processing of encrypted data while keeping the original data out of the hands of the cloud provider in a cloud computing environment [94]. This allows the cloud provider to conduct computing operations while maintaining data privacy. Likewise, SMPC utilizes the HE to enable several entities to conduct operations and tasks on shared data while preserving the confidentiality of the original plaintext. This can be beneficial, especially for applications relevant to marketplaces, auctions, and secure voting. In an SMPC-based system developed by Mouchet et al. [95], computations on encrypted data can be performed by the users in a collaborative manner without requiring a shared key configuration, thereby preventing the server from obtaining client data information [96]. Hence, HE is widely employed in secure data analysis, where insightful information from encrypted data can be extracted without requiring data decryption [97]–[99]. This is especially helpful in highly regulated sectors where data exchange is restricted, such as the case in the healthcare industry [97].

Additionally, ML models are trained and evaluated in distributed computing using HE. To ensure the confidentiality of the training data, one party encrypts the data before passing it to another party for processing. In [100], the authors presented DL system that protects participant privacy by not disclosing local data to a centralized server (CS). They employ additively HE to safeguard the data gradients on the cloud server, which may be honest but curious. The authors in [101] introduced a secure method that utilizes HE to safeguard the training and prediction data in logistic regression. However, CS may be required to retrieve, store, and process the data. HE ensures that the server never has access to the plain data. The authors in [102], [103] introduced the FL architectures for wearable healthcare in their publication. They employ HE to encrypt the user models before uploading them to the server to be aggregated and broadcasted to the users so they can undergo retraining. This technique is iterated until convergence is achieved. The authors in [104]–[106] introduced a method for privacy-preserving multi-party ML using HE, where each node in the system has a unique HE private key.

Despite its advantages in privacy protection, HE has several vulnerabilities [6]. Firstly, constructing secure computing protocols for PHE and SWHE systems can be computationally expensive due to a high number of modular exponent arithmetic operations, leading to reduced efficiency. Secondly, there is a significant increase in storage overhead when comparing ciphertexts to the original plaintext. Finally, HE requires a trusted authority (TA) to generate and distribute public and private keys to all participating parties. Moreover, under the FL framework, clients employ additive HE to conceal their local gradient updates during aggregation, so ensuring their privacy. Nevertheless, the computational and communicative expenses associated with HE operations are exceedingly high [103], [107].

2) Functional Encryption

The concept of FE was introduced by Sahai and Waters in 2005 and then formalized by Boneh *et al.* [108] in 2011. FE is a cryptographic technique that extends public-key cryptography. It allows the encryptor to use an encryption key to encrypt a message $\boldsymbol{x}$ and grants the decryptor the ability to conduct computations on the encrypted message using a functional decryption key to obtain the outcome of a specific function $f(\boldsymbol{x})$. Notably, the decryptor is incapable of uncovering the original message $\boldsymbol{x}$ itself [82], [109], [110]. The decryption key is function-specific and exclusively applicable for performing the designated computation on the ciphertext.



(a) Homomorphic Encryption (HE) workflow. (b) Functional Encryption (FE) workflow.

Fig. 6. Homomorphic Encryption (HE) and Functional Encryption (FE) workflows.

Within the context of privacy-preserving data analysis, FE can be employed to enable data analysis without the need for data decryption [111]. Access control also employs the usage of FE to allocate varying degrees of access to individual users, eliminating the need to decode their data [112].

Lately, there has been a growing emphasis on FE, particularly in the development of effective strategies for specific types of functions or polynomials with limitations, such as linear functions [113], [114] or quadratic functions [115]. FE has the capability to conduct an inner product operation on encrypted data, which is referred to as inner product FE (IPFE) [114]. The IPFE allows to solely acquire the dot product value ($\boldsymbol{x} \cdot \boldsymbol{y}$) of the vectors upon receiving the encrypted vector $\boldsymbol{x}$ and functional decryption key that corresponds to vector $\boldsymbol{y}$, without gaining access to the contents of $\boldsymbol{x}$. Generally, FE comprises three parties as outlined below.

- ***Key Distribution Center (KDC)***: The KDC distributes the encryption key to the encryptor and the functional decryption key, which is linked to a vector $\boldsymbol{y}$, to the decryptor.
- ***Encryptor***: Using the encryption key provided by the KDC, the encryptor can compute a ciphertext of the data vector $\boldsymbol{x}$ to be sent to the decryptor.
- ***Decryptor***: Using the ciphertext provided by the encryptor along with the functional decryption key provided by the KDC, the decryptor can compute only the inner product result $\langle \boldsymbol{x}.\boldsymbol{y} \rangle$.

Both FHE and FE can be utilized to conduct dot product operations on encrypted data. However, unlike HE, which necessitates decrypting the ciphertext to receive the computed result, FE can directly provide the result, as can be seen in Fig. 6(b). In addition, IPFE is more efficient than HE because it utilizes linear operations in encryption [79]. While FE shows promise as a technology and is recognized as a crucial component for secure and privacy-preserving systems, it is still relatively new and requires further research to enhance its performance.

3) Secure Multi-party Computation (SMPC)

SMPC is an alternative approach to doing computations on encrypted data. It enables many participants to collaboratively calculate a function using their individual private inputs while ensuring that no information about their inputs is disclosed to the other participants. This is accomplished by employing encryption to secure the data and conducting computations on the encrypted data without the need for decryption [29], [116]. SMPC supports a set of functions such as private set intersection protocols and secure comparison and equality testing. For instance, the secure equality testing allows two parties to determine if their private inputs are equal without revealing their confidential information.

There are two commonly used protocols for SMPC in the literature: Yao's garbled circuits, which were created by Yao [117] along with oblivious transfer protocol [118] and GMW (the Goldreich-Micali-Wigderson protocol) [119], presented by Goldreich *et al.*. These protocols allow parties to securely exchange their inputs and use Oblivious Transfer (OT) protocol [120], which employs public key cryptographic methods, to compute the output. These protocols require a long time and resources for processing, and there is still a significant communication cost associated with SMPC protocols [121].

Hence, SMPC exhibits a diverse array of uses, encompassing secure voting, auctions, and markets. Secure voting can employ SMPC to guarantee accurate vote counting while maintaining the confidentiality of individual votes. It can also be employed in secure auctions to guarantee the confidentiality of bids while simultaneously enabling fair and transparent conduct of the auction and maintaining price confidentiality in secure marketplaces while simultaneously facilitating efficient market operations.

In the scope of ML, one potential solution for privacy protection in ML training and evaluation is to use SMPC. This involves using solutions such as GMW or Yao's garbled circuits to ensure the safeguarding of confidential information during the entirety of the procedure. The authors in [55], [122]–[124] proposed SMPC-based solutions for safeguarding the privacy of ML techniques, including neural networks, logistic regression, and linear regression. These techniques require data owners to distribute their data among various servers while ensuring that none of them can gain access to sensitive data, which is then used for training the models using SMPC. Other works also combine SMPC and HE, such as the privacy-preserving prediction solution introduced in [125]. However, in order to ensure the security of these techniques against potential adversaries, it becomes necessary to implement supplementary measures such as zero-knowledge proofs [126]. The solutions proposed in the literature also vary in the number of parties involved, with some using two-party SMPC [127]–[129] and others involving three-party communication [130].

Other works related to the FL environment suggested a strategy for securely aggregating the model parameter updates using an SMPC-based secret sharing scheme [55], [127], [131], [132] with two honest-but-curious non-colluding servers

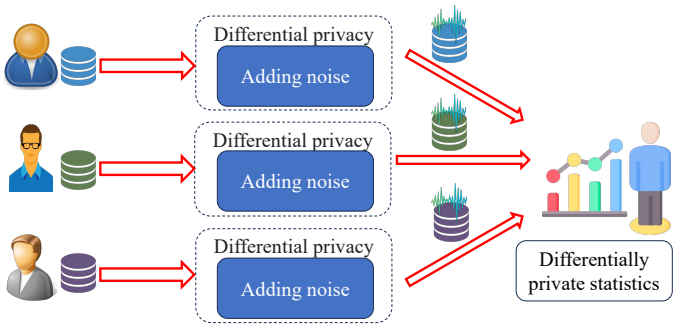


Fig. 7. Differential Privacy (DP) workflow.

required. Moreover, SMPC not only targets privacy protection during the training and execution of the FL but also introduces the necessary measures to prevent security attacks. The paper referenced as [131] presents a method of utilizing SMPC to prevent poisoning attacks while ensuring the confidentiality of sensitive data. Additional approaches utilizing SMPC to safeguard privacy and mitigate backdoor attacks in FL are presented in references [133]–[135].

However, these SMPC-based solutions can be costly due to the complex cryptographic processes involved and the need for communication between data sources [136]. To address this issue, customized SMPC protocols have been developed that incorporate certain sections of the ML and FL training algorithm to improve privacy, such as in the case of FL where safe aggregation of weight updates can mitigate the risk of sensitive data exposure [137]–[139]. In this approach, a trusted authority can be used to minimize communication among data owners, while an aggregator server combines confidential data without gaining access to sensitive information. In summary, SMPC is regarded as a relatively recent technology that requires further investigation to enhance its efficiency and scalability due to its demanding computational nature. It may not be suitable for extensive computation and data analysis at present. However, ongoing research is actively tackling these obstacles.

B. Differential Privacy (DP)

DP is a mathematical framework designed to safeguard the privacy of individuals by adding random noise to data before transmission in a controlled manner to mitigate information disclosure risks while still allowing for accurate data analysis to be conducted [140], [141], as can be seen in Fig. 7. DP can be applied to various tasks such as data mining, ML, and statistical analysis [142]–[144]. In data mining and statistical analysis, DP can maintain the privacy of individuals by ensuring that patterns and relationships are representative of the overall population rather than specific individuals [145]. In the realm of ML, DP allows for training models on sensitive data without revealing any confidential information about individuals [34], [35], [146]–[149]. Consequently, it serves as a new method for preventing privacy and security attacks, including membership and model inference, model extraction, and poisoning [150]. DP also has numerous applications in healthcare [151], [152], finance [153], and social media [154]–[156] by protecting patient, customers, and users privacy, respectively, while enabling for valuable data analysis.

Various methods exist for achieving DP, such as noise addition and data perturbation [157], but the most common DP methods are the exponential mechanism, which adds the noise to data based on a score function, and the Laplace mechanism that is based on the Laplace distribution [158]. Each technique has its strengths and weaknesses and is suited to different types of data and analysis tasks. DP involves a privacy budget, which determines the level of privacy loss allowed for any given analysis based on the privacy parameter epsilon (ϵ) representing the maximum allowed privacy loss. The smaller ϵ is, the higher the level of privacy maintained and lower accurate analysis [159], [160].

DP applications in the FL field can be divided into two categories, namely local DP (LDP) and central DP (CDP) based on the FL trust model [161]. When employing the central trust model, the FL server obtains client updates in plaintext, while CDP applications follow the same model but involve introducing noise on the server's end. This results in the server sending privacy-protected model parameters, which are received by the clients. The clients then perform local training and send their updates back to the server. The server aggregates these updates and adds noise proportionate to the sensitivity, repeating this process until convergence is achieved in each round of FL. DP noise sampling in FL can be done through three mechanisms - Laplace, Gaussian, and exponential [157]. LDP, on the other hand, provides enhanced privacy by eliminating the need to trust the FL server. This is achieved by introducing noise on the client side, reducing the reliance on the server [162]–[168]. LDP has gained significant attention in the literature to address honest-but-curious aggregator threats, especially since its introduction in [158].

The study presented in [169] introduced a new privacy-preserving method, known as LDP-FedSGD (LDP-based Federated Stochastic Gradient Descent), for vehicular communication, combining FL-based LDP with crowd-sourcing applications to predict traffic status using a single numeric characteristic. The research conducted by Wang et al. [170] addressed the challenge of perturbing multidimensional data to achieve optimal worst-case error. They proposed the Hybrid and Piecewise Mechanisms, building upon the work of Duchi et al. [171], which focused on single attribute numerical data. These techniques were extended to handle data with multiple dimensions and both numerical and categorical features. Similarly, the study in [172] also introduces a novel privacy-preserving method for LDP in the context of FL, specifically for handling high-dimensional, continuous, and large-scale data. The method also allows clients to customize their privacy budget.

The authors of [173] aimed to improve the efficiency of LDP, which can be hindered by the large variation in the added noise, leading to more communication overhead between server and clients to obtain the required outcomes [172]. They proposed a method of separating and shuffling gradients before transmission to counteract the privacy issues caused

by multidimensional data and repetitions. Another study [174] evaluated the effectiveness of CDP and LDP against backdoor, membership inference, and property inference threats using experiments. The evaluations indicate that while LDP may be ineffective in protecting against property inference, CDP offers a level of defense but with reduced effectiveness. Nevertheless, they both can successfully defend against backdoor and membership inference threats [175], [176]. Distributed DP (DDP) is a promising approach that combines both methods to find a balance between utility and privacy concerns. This method involves local protection of updates using LDP by clients, while secure aggregation ensures that the FL server does not expose intermediate parameters [138], [177]–[180].

To conclude, the preference and trade-off between CDP and LDP are influenced by the trust model of the implementations. CDP is unable to ensure privacy in scenarios involving a malicious server model. On the other hand, while LDP can safeguard clients from malicious servers, it may compromise the precision of the model. Therefore, it is important to consider the trade-offs between privacy and accuracy when using DP and to carefully manage the privacy budget. Moreover, the adversarial colliding client model is not taken into account in the DP itself. Other privacy-enhancing techniques, such as HE, FE, SMPC, and/or FL, can be used with a hybrid solution to provide a comprehensive privacy and security solution.

C. Confidential Computing (CC)

CC ensures the privacy of users' environments when running programs in virtualized environments by leveraging enclave technologies, hardware security features, and trusted execution environments (TEEs) [181]. Enclaves offer hardware-based protection from other software components on the same platform, such as the operating system and hypervisor, by creating secure and isolated memory regions inaccessible from random access memory (RAM) [182]. This technology is primarily provided by hardware vendors like Intel, ARM, and AMD under various names. Intel developed the enclave concept with Software Guard Extensions (SGX) to improve security and privacy on their processors, starting with the Skylake generation [181]. However, solely relying on SGX for privacy protection is not enough, as the code from the ML as a service (MLaaS) provider may not be trustworthy. To prevent unauthorized data access, SGX must be restricted within a sandbox. The Ryoan sandbox is a commonly used option for SGX, allowing users to verify the execution of enclaves without accessing the model specifications, ensuring the confidentiality of both clients and ML models [183].

Trust-based secure enclave solutions are designed to protect against malicious insiders, like rogue hypervisors in virtualized cloud environments. However, these solutions are still vulnerable to side-channel attacks on the processors [184]. The use of computational confidentiality, facilitated by TEEs, offers a practical and effective solution to this issue. TEEs ensure the secure execution of ML tasks by isolating sensitive computations from untrusted software. However, utilizing TEEs requires additional hardware capabilities which may incur costs. In FL situations, TEEs can be used on either the server or the client side. In large-scale deployments, such as IoT applications, equipping every device with TEEs can be costly. While some IoT-specific solutions, like ARM TrustZone, exist, most implementations of TEEs are on the server side. Recent instances of Sybil attacks highlight the need to also protect against malicious client devices to prevent Sybil-based poisoning attempts [185].

Researchers in [182], [184]–[193] investigated the use of TEEs to protect DL models in the context of MaaS. Due to hardware constraints, it is not viable to execute model inference within TEEs. The limit of the TEEs (enclave) code is constrained by a specified threshold, such as $128\mathrm{MB}$ in the case of Intel SGX. If this limit is exceeded, the process of swapping data takes place, resulting in potential concerns for both performance and security, as the data needs to be decrypted and encrypted during the swapping process. Therefore, strategies such as splitting the model and utilizing GPU (Graphics Processing Unit) accelerators have been proposed to address this problem. The main focus of these studies has been on how to outsource computation to GPUs and how to partition the deep neural network (DNN). Some studies have also employed blinding operations to add a layer of protection by obscuring results during computation outsourcing. After completion, these results are unblinded within the TEEs [187], [190]–[192].

TEEs are being increasingly utilized in FL situations, with two main applications depending on the trust model. One case involves an untrusted aggregating server, where SMPC can protect model updates, but a malicious server can still pose a challenge in semi-honest models. In these cases, TEEs such as Intel SGX can be used to secure server-side activities. The other scenario is when there is a potential for malicious client devices, which can manipulate the protocol despite appearing harmless. In such cases, TEEs such as ARM TrustZone can be used to secure client-side activities. When both server-side and client-side can be malicious, TEEs can be utilized on both ends [193]. Although there has been significant progress in utilizing TEEs in ML on the cloud, there are limited studies on applying TEEs to FL situations. A collaborative effort between Intel and UPenn [194] employed Intel SGX in the FL context to address medical imaging, where data is trained locally, encrypted, and aggregated using the SGX enclave before being transmitted to clients. Both the model data and data updates are safeguarded in the given scenario. In their publication, Chen *et al.* employed TEEs to carry out activities on both the client and server sides [193]. However, this study did not safeguard model updates despite claiming to transmit them securely. Another study [195] utilized ARM TrustZone TEEs to protect client-side activities by dividing the DNN model into segments by employing Ohrimenko's method for side-channel assaults and DP utilized for update protection. This method was further improved upon by utilizing TEEs on both client and server sides in FL [196], [197]. This study also focused on protecting all layers of the DNN, rather than just the most vulnerable ones as in [196], [198]. These studies demonstrate the potential of TEEs in safeguarding FL against various attacks, such as model inversion, property, and model inference attacks.

In conclusion, CC-based techniques facilitate secure executions by leveraging the hardware assurances provided for separated and safeguarded memory regions.

D. Combining Privacy-preserving Algorithms and Machine Learning

In recent years, both industrial and academic stakeholders introduced a variety of HE libraries, such as the Simple Encrypted Arithmetic Library (SEAL) [199], HE Library (HElib) [200], [201], Faster Fully HE (TFHE) [202], PALISADE [203], Compute Unified Device Architecture (CUDA) HE (cuHE) [204], HE for Arithmetic of Approximate Numbers (HEAAN) [205], and HE-transformer [206]. Many of these libraries are built on the Ring Learning with Errors (RLWE) principle and share similar choices regarding underlying rings, error distributions, and parameter settings.

SEAL [199] stands out as the most popular open-source HE tool, supporting both Brakerski/Fan-Vercauteren (BFV) and Cheon-Kim-Kim-Song (CKKS) schemes. Written in C++, SEAL is under continuous development to expand compatibility with other languages like C#, F#, Python, and JavaScript. One of SEAL's key features is its ability to compress data, significantly reducing the memory footprint. The HElib [200], [201] is another open-source tool based on the Brakerski-Gentry-Vaikuntanathan (BGV) scheme and was developed in C++. HElib emphasizes efficient ciphertext packing and data movement optimizations, though it has some limitations in bootstrapping performance.

The TFHE [202] library, open-source and maintained in C/C++, focuses on a Ring variant of the Gentry, Sahai, and Waters (GSW) scheme and uses an alternative torus representation. TFHE is known for its extremely rapid gate-by-gate bootstrapping process, which doesn't limit the number of gates or their arrangement. PALISADE [203] is an open-source initiative that provides an HE library that supports various schemes like BGV, BFV, CKKS, FHEW, and THEW. Developed in C++, it includes features for multi-party extensions and utilizes RNS algorithms for enhanced performance. The cuHE [204] library leverages GPU acceleration through CUDA for parallel computing, implementing arithmetic functions using techniques like the Chinese Remainder Theorem (CRT), Number-Theoretic Transform (NTT), and Barrett reduction for managing large polynomial operands.

The HEAAN library [205], supporting the CKKS scheme, is designed for fixed-point arithmetic with rational numbers, where the error margin is adjustable based on specific parameters. Lastly, the HE transformer for nGraph (HE-transformer) [206] is a project based on SEAL for the Intel nGraph Compiler. This C++ implementation acts as a graph compiler for neural networks (NNs), serving as a proof-of-concept to evaluate the performance of HE schemes in DL applications.

In [207], the authors designed an HE library called GAZELLE that combined with the garbled circuits (GC) to support SMPC for preserving privacy in an MLaaS environment. Gazelle library aims to accelerate the mathematical operations on encrypted data for DL-required processes by leveraging an automatic switch between HE and GC.

In [125], the authors implemented Mini Oblivious Neural Network (MiniONN) library in C++ using the Arithmetic sharing, Boolean sharing, and Yao's garbled circuits (ABY) library [208] for SMPC implementation and Yet Another Somewhat HE(YASHE) [209] for additively HE.

PySyft and Advanced Privacy-Preserving Federated Learning (APPFL) are two Python libraries for secure and private DL. They use FL and DP to decouple private and sensitive data. They can be used within the major DL frameworks, such as TensorFlow and PyTorch.

Marc *et al.* in [210] introduced the FE library, called CiFEr, to build privacy-enhanced ML models. CiFEr library is written in C by combining various libraries like GNU Multiple Precision (GMP), Apache Milagro Crypto Library (AMCL), and libsodium. Another FE library called GoFE is also proposed in [210].

HT2ML [211] is a C++-based framework for PP ML based on HE and Intel SGX TEE. This prototype uses Microsoft OpenEnclave, which is a hardware-agnostic open-source library for developing SGX enclave applications, and HElib library. HT2ML accelerates the HE-based computations for the SGX enclave while preserving the integrity and privacy of the computation to protect users' data and models. Ohrimenko *et al.* [25] proposed a secure enclave platform based on the SGX system for SMPC.

E. Distributed Learning

ML approaches have become widely used in various industries and educational settings [212]; however, due to privacy concerns, Google introduced a decentralized framework known as FL in 2016 [213]. This approach allows multiple participants to collaborate and train an ML model without sharing their training data [214]–[216]. Instead, the participants train the model on their own data and then send only their updated local model parameters to a central aggregator to measure the average value of the gradient descent of the local models received from different participants to update the global model without revealing this data to another party [217]. This process is repeated until convergence [25], [32], [218]–[220]. This preserves the privacy of the participants while still allowing them to learn an accurate global model (as it collects data from different distributions). However, this approach requires more local computation by the participants, although it reduces communication overhead.

Therefore, FL has become increasingly popular in both industry and research due to its ability to address privacy, security, and regulatory concerns when working with data from multiple parties [221]. This applies to various industries, such as healthcare, finance, and transportation. In healthcare, FL allows for model training using patient data without compromising sensitive information between institutions or hospitals [222]–[225]. Similarly, in finance, FL enables banks to train models on financial data without sharing sensitive data [226]–[228]. In the transportation sector, FL can be utilized to train models on traffic data while protecting sensitive information between different organizations [229]–[231].

Despite the advantages that come with FL, it is a relatively new technology and has some challenges that need

to be addressed. These challenges include data heterogeneity, communication efficiency, and privacy and security concerns. Existing studies [100], [232]–[235] have shown that FL can pose privacy and security risks, as model parameters may leak information about the training data as a result of inference attacks [236]. Other privacy risks include the ability to derive private information from a trained model [176], [218] and the potential for model inversion [237], backdoor, and GAN-based attacks [25], [238]. Moreover, FL is computationally intensive and may not be feasible for large-scale computation and data analysis. Additionally, frequent model updates and large data transfers between parties can result in high communication costs, posing a challenge for FL implementation.

Hence, the protection of privacy and reduction of communication costs are important areas of research in FL. To ensure the security and efficiency of FL, three cases must be considered: 1) a malicious aggregation server that falsifies aggregated results or manipulates models, affecting the accuracy of trained models; 2) high communication costs due to the complex DL model and distributed structure; and 3) the potential for participants' original training data to be inferred from the uploaded gradients [239], [240]. Several proposed schemes have attempted to address these concerns, such as using verifiable FL schemes defending against malicious participants in medical applications [241], [242], in which low-accuracy models could cause medical accidents. However, these solutions have limitations, such as high communication costs and impractical solutions due to involving SMPC protocol. The key to protecting privacy and secure aggregation is finding a way to aggregate without revealing the gradient to the aggregation server. To address these challenges, various techniques have been proposed to secure the aggregation process for FL global model construction [243]. These techniques include DP and HE, where DP [32], [168], [169], [172]–[174], [177], [178], [244] adds noise to data to protect individual privacy while HE [101], [103], [104], [106], [107] allows for computations on encrypted data without decryption. For example, Fig. 8 shows how FHE is being utilized to secure the FL process via encrypting the local model updates before transmitting them to the server while allowing the construction of the global model. Some studies [245] combine both techniques to enable a secure FL process, but these methods suffer from high overhead and are vulnerable to collusion attacks if participants work together.

Overall, FL is a promising technology that allows for the training of models on large-scale, decentralized data sets while ensuring the privacy and security of the data. It has many potential applications in various industries, but it still faces challenges that need to be addressed before it can be widely adopted in emerging communication networks. While FL provides an elegant framework for distributed data-driven learning, it has been associated with challenges, such as communication bottlenecks and client data heterogeneity. Coauthors of this paper addressed these challenges in [246] by developing an asynchronous weight updating FL with personalization by tailoring models to individual users based on their local data while exchanging model updates in a pre-scheduled manner. Furthermore, the asynchronous personalized FL technique was combined with Moreau Envelopes-based regularization. This approach leverages the advantages of Moreau Envelopes for handling optimization issues, along with asynchronous weight updates to boost communication efficiency. It also addresses data heterogeneity by creating a personalized learning framework. The method was tested across multiple datasets in [246] and was demonstrated to achieve faster convergence and higher communication efficiency compared to the baseline data-driven model. Practical aspects taken into consideration by such research work advance FL techniques for emerging networks that require communication efficiency by design.

The protection of data security has long been a key area of study when developing deep or FL models. These models are designed to safeguard clients (such as mobile devices) from unauthorized access to their data. The clients are able to keep their original data confidential on their devices while simultaneously participating in the model training process with others. They only need to send updates of their local models to a central server. However, the default privacy measures in place for FL are not enough to fully protect the confidentiality of the local training data [247]. This makes the system vulnerable to privacy breaches if an adversary is able to intercept the local gradient updates shared with the server. This breaching can result in the reconstruction of the private training data with high accuracy. Such model inversion attacks, where attackers discreetly monitor gradient adjustments during iterative training, can lead to the exposure of private data [100]. Attackers can exploit the intermediate gradients to access the training data without any prior knowledge of the learning model.

Table II highlights a high-level comparison of the focused privacy-preserving methods and their functionalities discussed in this section.

It is also worth mentioning that a number of privacy leakage attacks have emerged recently, including Gradient Inversion [248], Client Privacy Leakage (CPL) [249], Deep Leakage Gradient (DLG) [250], and Improved DLG (IDLG) [251]. These attacks aim to steal the training data and labels through the use of gradient information. Many of these attacks are based on iterations, which involve minimizing the distance between dummy gradients and actual gradients. This recovery process is formulated as an iterative optimization problem, with the error between gradients and the dummy inputs used as parameters. To prevent privacy leakage, several techniques have been investigated, including Gaussian or Laplacian noise-based DP. This approach involves adding Gaussian or Laplacian noise to gradients during training before sharing them with the server [252]. However, this can come at the expense of accuracy, as it may decrease below a desired threshold. Another approach is gradient compression, such as gradient pruning [250], where a specific pruning ratio is chosen during training to make the model more robust against leakage attacks. However, pruning in the initial stages of training may cause the loss of important feature-related information. Another approach is to use HE to protect data privacy, while still ensuring model convergence [104]. However, this can be computationally and memory intensive, limiting its practical application. In addition to these defense strategies, increasing local iterations or batch sizes during model training [253] can

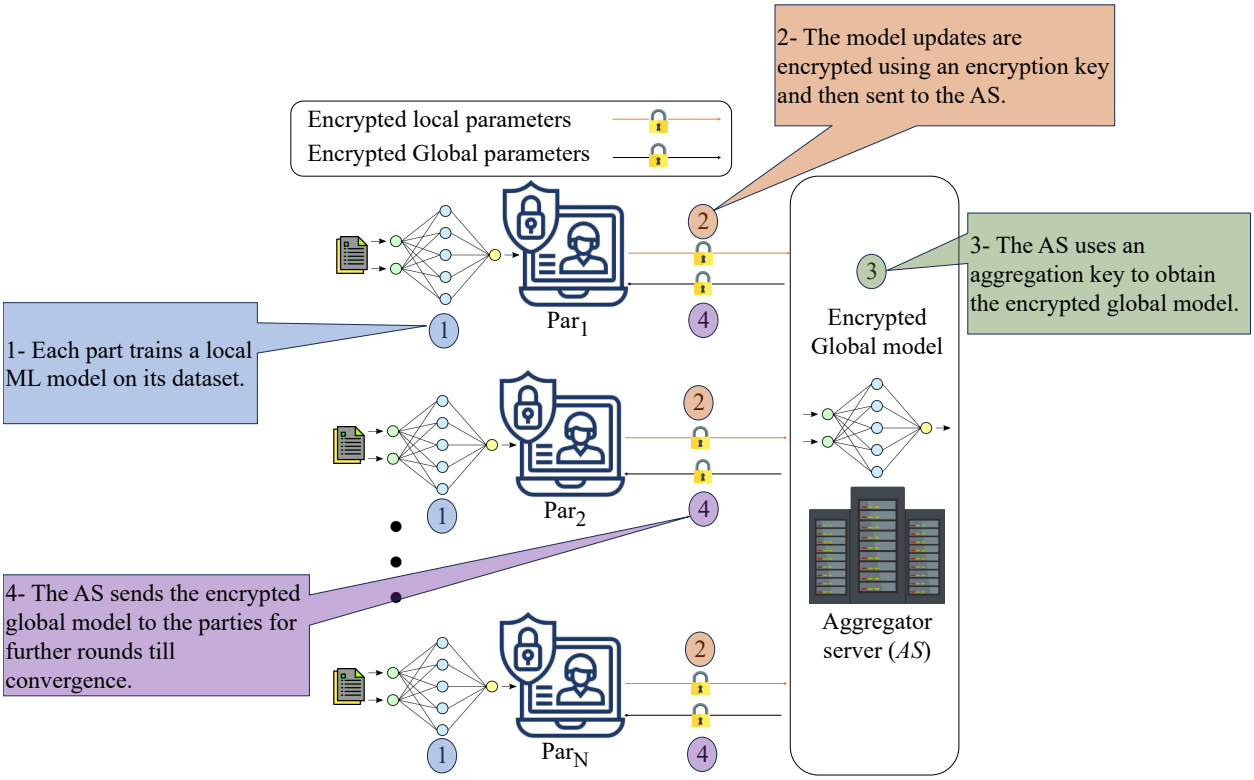


Fig. 8. Applying FHE in federated learning.

also mitigate privacy leakage.

V. Privacy-preserving Data-Driven Models for Emerging Communication Networks

In this section, we first describe how the intersection of privacy-preserving and data-driven models (comprising machine/deep learning techniques), described in Section III and Section IV, respectively, are gaining traction in emerging communication networks. Then we describe the various emerging communication network settings that can utilize privacy-preserving techniques in conjunction with data-driven models.

Guizani *et al.* [254] examined the security and privacy challenges posed by the integration of edge intelligence in 5G and beyond (B5G) networks. The authors emphasized the growing importance of edge intelligence, which enables data processing closer to where data is generated, reducing latency and transmission risks, by employing trained data-driven models. Then their work demonstrated how a decentralized approach brings new security and privacy concerns with regard to resource management in these emerging networks. As a solution, their work investigated the incorporation of blockchain technology for enhanced privacy in B5G networks.

Researchers in [255] empirically elucidated how ensuring privacy in data-driven learning models for 5G and beyond networks is a significant challenge. The architecture of the various learning models including supervised, unsupervised, and reinforcement learning-based adversarial models, while designed to enhance network efficiency, can be vulnerable to privacy threats. Analysis of the adopted models' performance, both before and during privacy breaches, demonstrates that such attacks not only compromise the integrity of the data but can also result in performance degradation that is comparable to or worse than traditional security threats like data leakage. This is evident in the deterioration of key performance metrics under privacy attacks, highlighting the critical need for robust privacy-preserving mechanisms.

Next, the goal of the study conducted by Humayun *et al.* [256] was to find an optimal approach for ensuring privacy and improving energy efficiency in 5G-powered IIoT (Industrial IoT) systems within Industry 4.0. With 5G introducing significant changes across various sectors, its integration with Industry 4.0, which utilizes IoT devices, has become a key industrial trend. Industry 4.0 incorporates ideas like smart infrastructure, intelligent services, and rapid development cycles, leading to the connection of billions of devices. However, this large-scale connectivity of varied devices presents notable privacy concerns, which are a major area of focus for users. In a similar vein, researchers in [257] introduce two protocols designed to address privacy concerns in 5G-enabled positioning systems. The protocols protect the privacy of reference points by encrypting the original data matrix using two random matrices through concatenation and multiplication, without affecting the positioning service. A thorough analysis was conducted to evaluate the security strength, computation cost, and communication overhead of the proposed protocols under machine learning settings. This ensures higher security under specific time and communication constraints. However, adapting these protocols requires further validation in real-world network deployment for the verification of the outsourced computation overhead.

TABLE II
SECTION IV SUMMARY. NOTATIONS: PRIVACY-PRESERVING (PP), MACHINE LEARNING (ML), DEEP LEARNING (DL), FEDERATED LEARNING (FL), COMPUTATION OVERHEAD (COMP), COMMUNICATION OVERHEAD (COMM), ACCURACY LOSS (ACC LOSS), AND SCOPE.

Objective	Reference	Methodology					COMP	COMM	Accuracy loss	Scope
		HE	FE	SMPC	DP	CC				
PP DL	[27], [28], [100]	✓					High	High	Low	–
	[29], [124]			✓			Medium	High	Low	–
	[34], [140], [141], [144], [147], [149], [160]				✓		Low	Low	High	–
	[142]				✓		Low	Low	High	Load Forecasting in smart grid
	[145]				✓		Low	Low	High	Mobile data analytics
	[146]				✓		Low	Low	High	Sensitive crowd-sourcing data
	[148]				✓		Low	Low	High	Distributed web attack detection
	[186], [190], [198]					✓	Low	Low	Low	–
	[153]				✓		Low	Low	High	Financial time-series prediction
PP FL	[105]	✓					High	High	Low	Industrial cyber-physical systems
	[102]	✓					High	High	Low	Healthcare
	[79]		✓				Low	Low	Low	Electricity theft detection in smart grid
	[103], [104], [106], [107]	✓					High	High	Low	–
	[154]				✓		Low	Low	High	Securing IoT-based social media networks
	[138], [168], [172]–[174], [177], [178]				✓		Low	Low	High	–
	[169]				✓		Low	Low	High	IoT
	[193], [195], [197]					✓	Low	Low	Low	–
	[122]			✓			Medium	High	Low	Distributed linear regression
	[131], [132], [134], [135]			✓			Medium	High	Low	–
PP ML	[82]		✓				Low	Low	Low	Electricity theft detection in smart grid
	[116]			✓			Medium	High	Low	Electricity theft detection in smart grid
	[109]		✓				Low	Low	Low	–
	[55], [123], [138]			✓			Medium	High	Low	–
	[182]					✓	Low	Low	Low	ML as a Service
	[187]–[189], [191], [192]					✓	Low	Low	Low	–
	[152]				✓		Low	Low	High	Social media data outsourcing
	[84]	✓					High	High	Low	Secure data mining
	[129]			✓			Medium	High	Low	Data mining
	[101]	✓					High	High	Low	PP logistic regression
PP statistical analysis	[97]	✓					High	High	Low	Healthcare data
	[98], [99]	✓					High	High	Low	–
	[128]			✓			Medium	High	Low	Linear Regression and Classification
	[151]				✓		Low	Low	High	Healthcare data
	[158]				✓		Low	Low	High	–
Encrypted data ordering	[111]		✓				Low	Low	Low	Health
PP data aggregation	[139]			✓			Medium	High	Low	Mobile sensing

A. 5G and Beyond Open Core Network Systems

In Beyond 5G and 6G core network systems, open protocols for interoperability and multi-tenant service provisioning make privacy preservation a critical yet untouched problem. In these emerging open-core networks, resource slicing in a dynamic manner is considered to be a key feature for effective network management to optimize the user-perceived Quality of Service (QoS). Resource slicing in the network, for instance, allows for efficient handling of massive machine-to-machine and IoT traffic without impacting the quality of simultaneous video streaming services. Kline *et al.* [258] identified a number of security and privacy concerns with multiple service providers and operators in emerging 5G core networks that include information exfiltration via side-channels, control spoofing due to compromised infrastructure, and control manipulation across different service/administrative domains. Since distributed and multi-party resource slicing cannot be ensured to be privacy-preserving with existing public-key cryptography schemes, Kline *et al.* discussed the breakthroughs in FHE exploiting lattice-based encryption to provide robust, hierarchical security. They also developed advanced private and secure network control through the Threshold FHE scheme and presented proof-of-concept results. This concept was further augmented with data-driven techniques to conceptualize programmable privacy to enable confidential smart contracts by employing FHE [259].

European Telecommunications Standards Institute (ETSI) recommended Zero touch network and Service Management (ZSM) architecture for the network function orchestration and automation, which splits the core network into operational, technological, and business planes [260]. AI and ML-based data-driven models have been considered in [261] to support closed-loop network functions in the ZSM framework for cyber threat intelligence that requires security data collection points. However, this poses a potential privacy leakage scenario in such massive core network systems, and FL methods were considered to be directly applicable in ZSM-based end-to-end service management in core networks in [262]. Privacy-preserving methods combined with AI-based data-driven models for core network systems were also introduced by an assortment of FL frameworks introduced in [263]–[268]. The privacy-preserving and security parameters aggregation concept for end-to-end QoS management, based on this assortment of research work, is illustrated in Fig. 9.

Lessons Learned

Core networks deal with massive numbers of network flows that could be unstructured and flow at a significantly high speed. Unstructured big network data needs to be converted to structured data prior to applying data-driven models, and a significant challenge exists in this preprocessing step, which is often taken for granted as trivial. However, this preprocessing task may impose significant delays on the network orchestration tasks, and hierarchical data-driven models need to be designed such that the preprocessing of unstructured data can be dynamically handled by the upper-level models, whereas the lower-level ones work in conjunction with privacy-preserving techniques, such as HE, ME, and MPC. FL in this context emerged as a natural choice for distributed processing, as well as learning to prevent raw data leakage while training the models at localized sources while fulfilling their respective resource constraints. Also, in the case of FL-enabled core networks, label generation from the local data may be theoretically possible; however, they may be practically challenging due to the absence of data annotation at the hardware level and non-iid data characteristics. While personalized FL models can be customized for each network function in a given core network, generalizing them may require devising another level of AI models to scale across the entire core network.

B. Open and Reconfigurable Radio Access Networks (RANs)

While the preceding subsection covers the core networks in B5G and 6G networks with regard to their use of privacy-preserving techniques coupled with AI-based systems such as FL, we now turn our attention to radio/wireless access network technologies adopting privacy-preserving data-driven models. The radio access networks of emerging networks connect the wireless/mobile users with the core network under extremely dynamic and unpredictable channel conditions. Numerous research works have been done on ML/DL model-based channel prediction, resource allocation, and mobility prediction techniques to improve communication network performance outcomes. On the other hand, a number of privacy-preserving techniques are now being adopted in wireless fronthaul. However, the seamless fusion of privacy-preserving algorithms with data-driven models remains an interesting avenue where some pioneering research has started to appear.

6G networks are envisioned to surpass 5G in terms of speed, capacity, and latency, enabling transformative applications such as holographic communication, high-fidelity mobile Internet, and pervasive AI. These networks will rely on cutting-edge technologies like edge computing, advanced beamforming, and massive Multiple Input Multiple Output (MIMO) to achieve these feats. However, the complexity and openness of 6G networks also introduce significant privacy and security challenges. To tackle these issues, Ye *et al.* [269] formulated a novel approach that leverages HE and GNNs. HE, as described in the preceding section, is a form of encryption that allows computations to be performed on ciphertexts, generating an encrypted result that, when decrypted, matches the result of operations performed on the plaintext. This property is particularly useful for preserving the privacy of data in cloud computing and, by extension, in 6G networks, where data may need to be processed by intermediate nodes without exposing the underlying sensitive information. In addition, the incorporation of GNNs offers a sophisticated method to analyze and interpret the complex relationships and patterns within the data transmitted across 6G networks. The reason behind introducing GNN is its ability to handle data structured as graphs, making it a natural choice for modeling the intricate interactions and dependencies in network traffic in 6G RAN. By applying GNNs, the system can learn to detect anomalies, optimize network performance, and enhance security measures

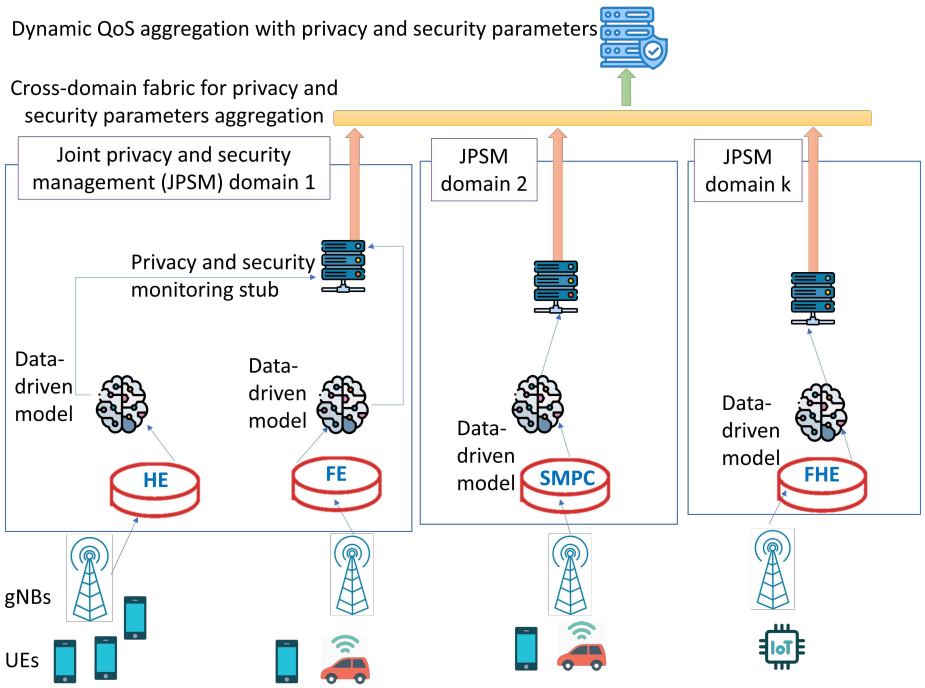


Fig. 9. privacy-preserving and security parameters aggregation in beyond 5G open core networks with end-to-end QoS management.

based on the vast amounts of data flowing through the network, all while maintaining the privacy of the data through HE.

Researchers are recently also investigating the application of deep learning techniques with privacy-preserving techniques for the combined purposes of sensing and safe communication, with an additional focus on semantic communications [270]–[273]. For instance, the system conceptualized in [270] integrates a transmitter and receiver operating over a wireless channel, influenced by noise and fading. At the transmitter, a deep neural network, acting as an encoder, is employed to jointly perform source coding, channel coding, and modulation. On the receiving end, another deep neural network, posing as a decoder, handles demodulation, channel decoding, and source decoding to recover the transmitted data. The transmitted signal fulfills two roles, i.e., it enables communication with the receiver while also facilitating sensing. In the presence of a target, the reflected signal is captured, and a separate deep neural network decoder is employed for sensing, tasked with detecting the target and determining its range. These networks—one encoder and two decoders—are trained jointly using multi-task learning, considering both the data and channel conditions. Researchers in [270] further expanded the system to include semantic communications by introducing an additional deep neural network decoder at the receiver, which acts as a task classifier, evaluating the accuracy of label classification in the received signals. The study employed CIFAR (Canadian Institute For Advanced Research)-10 [274] as input data and took into account channel conditions such as Additive White Gaussian Noise (AWGN) and Rayleigh fading. The findings demonstrate the potential of multi-task deep learning to effectively support high-precision joint sensing and semantic communications that further facilitate privacy-preserving.

Lessons Learned

Combining these two technologies, i.e., privacy-preserving techniques and data-driven models, within 6G networks represents a powerful tool for ensuring privacy preservation at scale. HE ensures that data remains encrypted throughout its journey across the 6G RAN, which is anticipated to support open standards and multiple tenants/service providers, resulting in possible privacy leakage scenarios. Thus, privacy is retained with the introduction of HE even when the data are being processed at the 6G base stations. Meanwhile, GNNs provide the intelligence layer that enables the network to adapt and respond to emerging threats and challenges, ensuring robust security and optimal performance. While the existing research work typically outlines frameworks integrating privacy-preserving algorithms with data-driven models for 6G networks, it is important to also discuss potential challenges, limitations, and future directions for research in this area, emphasizing the importance of developing scalable, efficient solutions to support the anticipated demands of 6G networks in TeraHertz (THz) communication environment where channel models are not yet known. Moreover, the introduction of intelligent and reconfigurable surfaces for 6G networks may add to the complexity of channel models in hyper-dense 6G tiny cells. In such scenarios, privacy-preserving data-driven models may serve as a modular concept on top of the yet-to-be-established physical layer models of such emerging systems.

C. IoT Systems and Networks

The recent proliferation of IoT devices and sensors for facilitating smart community applications has resulted in vulnerabilities that can result in unauthorized access and data

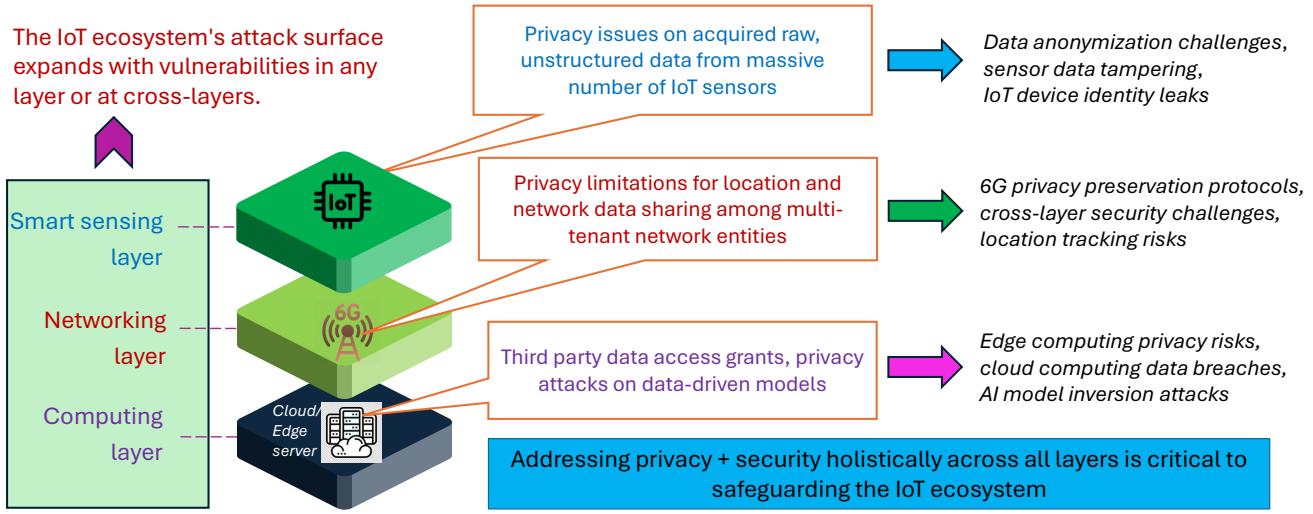


Fig. 10. Privacy issues in sensing, network, and computing layers of IoT systems.

breaches. These may be observed in all three layers of IoT systems, namely sensing, networking, and computing layers, as depicted in Fig. 10. Privacy leakage in IoT systems may be customer-specific and may range from revealing the user behavior to exposing sensitive parameters, data, and even learned models, which may, for example, user-behavior revealing sensitive parameters, data, and even learned models to outside parties [275]. In particular, the correlation between geolocation data and the end users' demographics and usage patterns in IoT systems data acquisition was reported in [276]. To address the privacy-preserving need utilizing data-driven models, Berry *et al.* [277] presented a fusion of a hybrid SMPC with ML in IoT systems. Their data-driven privacy-preserving model was tailored for energy-constrained IoT devices where individual nodes aim to protect their respective data. Therefore, training data are not shared among the nodes. The data-driven model is protected with information-theoretic security/privacy guarantees from being accessed by probing nodes. The hybrid multi-party secure computing allows for a communication-efficient matrix and is scalable over a massive number of low-power IoT devices. Furthermore, an open-source library, referred to as Cicada, was developed that other IoT developers can use on IoT nodes, such as Raspberry Pi devices, even on resource-constrained IoT platforms, such as UAVs/drones.

Next, Bocu *et al.* [278] provided an interesting analysis of personal data gathered via sensors on mobile devices and indicated the privacy risks of the captured sensitive data. In particular, they considered DP to be a key technique for data anonymization to mitigate the possibility of privacy leakage. Their survey also indicated that apparently harmless personal data collection through sensory systems could actually lead to identifying critical personal data items that should be protected according to data protection regulations, e.g., the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR).

Researchers in [279] presented a privacy-preserving data-driven model for predictive maintenance in 6G-enabled industrial IoT network systems. They trained binary neural networks (BNNs) along with HE circuits to ensure that the privacy of all the participating users is guaranteed. The rationale behind adopting the BNN-based model was its lightweight performance capability to ensure that it would not overwhelm the resource-limited IoT nodes. Furthermore, they verified the performance of this privacy-preserving data-driven model approach based on experimental test data. In a similar vein, Wang *et al.* [280] demonstrated the viability of jointly employing HE and a DL-based model based on secure multi-party computing to guarantee the privacy of the users.

Arachchige *et al.* [144] tweaked the global DP to a localized setting and invoked this to a differentially private mechanism for IoT devices that is referred to as LATNET. In other words, LATNET employs the post-processing invariance property of DP and also the composition property while applying the localized DP to a CNN. The computational complexity of LANET was demonstrated to be reasonable on a resource-constrained platform when tested with the well-known CIFAR-10 dataset that yielded approximately 91% testing accuracy while obtaining a high level of privacy.

FL models are also emerging in IoT systems to serve a plethora of objectives, from IoT data analytics to IoT resource allocation [19], [20], [40], [281]–[287]. Among these, the work by Yin *et al.* [287] is note-worthy since it fuses multi-party data sharing and FL based on Bayesian DP. Recent research work conducted by co-authors of this survey [11], [288]–[291] addresses communication-efficiency challenges in IoT-based systems by examining the communication overhead and privacy risks associated with FL. Then the work designed an algorithm that integrates Knowledge Distillation (KD) and DP to mitigate these issues. The operational flow and network architectures of model-based and model-agnostic (KD-based) FL algorithms were provided that enables customization of model architectures for each client to account for heterogeneous and constrained system resources. Proof-of-concept experiments, based on the MNIST dataset [292], demonstrated that KD-based FL algorithms can surpass local accuracy and achieve

performance comparable to centralized training. Furthermore, we show that applying DP to KD-based FL significantly reduces its utility, resulting in up to 70% accuracy loss for considered privacy budgets.

Lessons Learned

The combined approach of privacy-preserving algorithms and ML/DL models needs to be lightweight subject to the resource constraints of the target IoT systems. While the main bottleneck is energy (i.e., IoT nodes should not transmit the acquired data at all times), the processing limitations of such devices may vary. For instance, Raspberry Pi devices may be more limited than Nvidia Jetson microcontrollers on an industrial IoT platform. On the other hand, such IoT boards may be even more constrained when used on aerial systems, such as UAVs. Programmable privacy, as well as programmable computing, should be integrated into data-driven models to take into consideration their resource availability in a dynamic manner. Also, it is important to consider encouraging research outcomes in this domain, such as the aforementioned LATNET [144], as lightweight solution benchmarks to compare the performance tradeoffs of emerging privacy-preserving ML/DL models.

D. Software-Defined Networks (SDNs)

SDNs decouple the control plane from the data plane and bring forth the concept of re-programmable routing and re-configurable network tasks by replacing many network middleboxes with one or several SDN controllers as shown in Fig. 11. Network operators and service providers are embracing SDN architecture in their backbone networks and also in the data center networks where virtualization is a key feature. Therefore, it is of paramount importance to design privacy-preserving solutions for SDN to prevent data privacy leakage. In this vein, Wu *et al.* [293] conceptualized a joint DL and DP data protection mechanism for SDN. This method comprised a GAN to synthesize artificial samples to respond to an adversary with the appropriate response. By doing so, they reinforced user location privacy in 5G-enabled SDN systems.

Guo *et al.* [294], on the other hand, devised an intelligent zero-trust secure framework for SDN systems that comprises a data collection module, trust assessment engine, and a user behavior analysis engine that can be implemented in the SDN controller. LSTM and CNN-based self-attention networks were customized to protect every resource and network connection in the considered SDN, thereby facilitating dynamic authorization and guaranteeing the data privacy of users.

Next, Mendis *et al.* [295] envisioned blockchain as a service for decentralized secure computing and privacy-preserving in SDN systems. Their main motivation was the privacy-preserving data-driven technique implemented in a distributed manner instead of centralized data acquisition and processing. In spirit, their solution was comparable to FL frameworks for SDN traffic flow control and resource allocation [296]. They demonstrated that in particular SDN settings that they considered, more effective computing paradigms could be possible to process private or scattered data for training

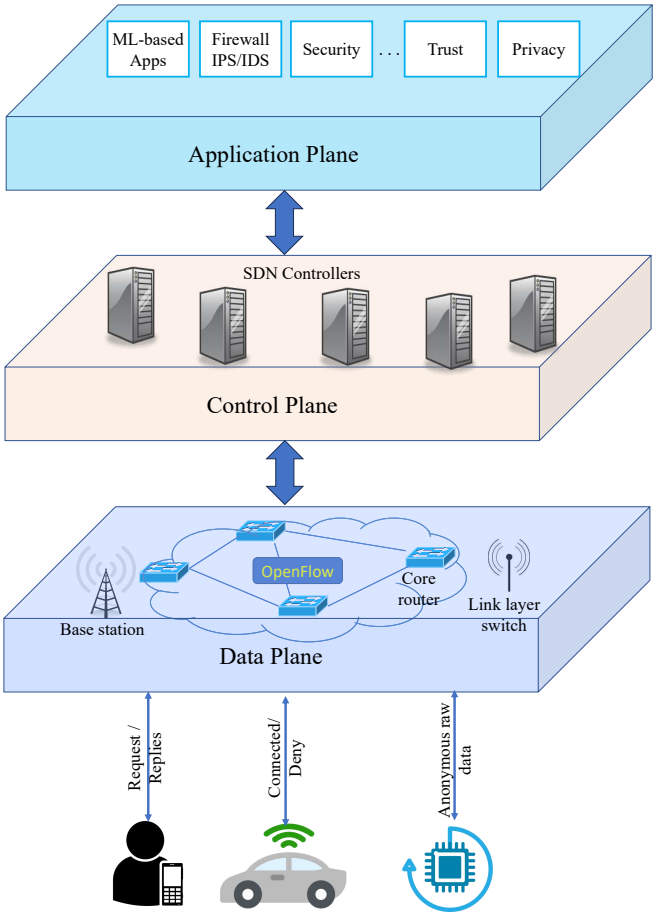


Fig. 11. Privacy-preserving functionality can be deployed to the SDN network controller along with other network functionalities.

appropriate ML models. Their technique was, in essence, a synchronized cooperative computing process exploiting HE and blockchain among the distributed, untrusted SDN nodes, each with constrained processing resources.

Lessons Learned

SDN controllers are designed to centralize the functions of diverse middleboxes, streamlining network management and control. This centralization is critical for implementing advanced technologies like distributed FL or blockchain-based privacy preservation techniques within an SDN framework. While placing such functionalities to a single or geographically distributed SDN controller(s) is critical, reliable coordination between the controller(s) and distributed network nodes is a key challenge for maintaining privacy standards that may inadvertently impact QoS, potentially degrading network performances in terms of delay and reliability to meet the actual privacy needs.

To address the aforementioned challenges, a nuanced understanding of the practical trade-offs between QoS and privacy parameters needs to be developed. For instance, devising privacy-preserving methods may require additional computational resources and demand more feature-rich networking protocols. This translates into increased delay and/or a drop in

throughput. This is evident in the case of FL, which requires coordination among distributed, less powerful user nodes to share the model parameters, resulting in significant communication overhead in already congested delivery networks. On the other hand, blockchain-based distributed ledgers for enhancing security and privacy could be associated with additional network delay because of the consensus update time. In order to effectively address the QoS trade-off with desired privacy levels, it is, therefore, essential to develop lightweight predictive models to proactively balance these contrasting needs. Designing such models needs to thoroughly take into account a number of factors, such as the current network configuration, data sensitivity, network traffic types, and their priorities, and so forth. At the same time, the SDN controller(s) require dynamic adaptation of coordination strategies with the distributed nodes to prioritize the critical data flows and adjust privacy level settings as needed to combat dynamic network conditions. Thus, the SDN controller(s) may ensure that the deployed privacy-preserving models do not exhaust the resources required for adequate QoS while maintaining an optimal balance with privacy protection needs.

E. Intelligent Vehicular Networks

Vehicle-to-vehicle/infrastructure (V2X) communication networks have received renewed interest as B5G and 6G networks meet autonomous driving, electric vehicles (EVs), and vehicular metaverse. Embedded intelligence in V2X communication became prominent and facilitated automated collision alerts, lane change alerts, data sharing among vehicles and roadside units (RSUs), navigation status, and so forth. In addition, an EV is known to generate tens of terabytes of data on a daily basis [297] that require high bandwidth and low-delay communication networks for taking prompt decisions and actions. However, vehicular data contains location information and other personalized user information that is associated with strict privacy needs, and the ML models are vulnerable to various privacy leakage scenarios [17], [22], [30], [298], [299]. Therefore, integrating privacy-preserving techniques with data-driven models is imperative, according to recent research work [300], [301].

Talat *et al.* provided a taxonomy of threat models in EVs and discussed privacy preservation strategies in [302]. The major attack vectors are illustrated in Fig. 12. The adoption of DP perturbation approach in intelligent transportation systems (ITSs) was extensively reported in [4]. According to [300], HE, along with ML models, can protect the privacy of EV (Electric Vehicles) users in a myriad of scenarios, including real-time data transmission, database analysis, collaborative learning, and so on. [303] discussed ML, particularly reinforcement learning techniques, combined with privacy-preserving technologies, for dynamic resource management of highly mobile EV networks. [300] highlighted the importance of preserving the privacy of vehicular network routing mechanisms based on ML models. Furthermore, [300] identified the shortcomings of intrusion detection systems that collect data from EVs to detect adversaries in the EV network that may result in privacy leakage. For example, when EVs collaborate to detect an intrusion, they need to share their location and routing information with one another and could possibly share sensitive information with an eavesdropping node. Therefore, [300] pointed out the importance of privacy-preserving data-driven models for intrusion detection. Furthermore, the researchers in that work also demonstrated how privacy-preserving data-driven models are useful for energy demand predictions for EV networks, EV energy trading, and optimal EV charging schedules.

Lessons Learned

Many services for EVs depend on the exchange of precise location and movement data with relevant entities. For instance, to identify nearby points of interest (PoIs) like charging stations and restaurants, an EV must share its current location with the system. Additionally, ML algorithms use this information to predict factors related to these PoIs. While the collection of such data is useful for identifying pertinent PoIs, it also risks revealing personal patterns of EV users, such as their religious practices, preferred dining spots, and shopping preferences. If this sensitive information were to fall into the hands of malicious individuals or if an attacker were to intercept these data exchanges, it could lead to significant privacy invasions. Consequently, it is crucial to safeguard the privacy of EVs when they interact with any Location-Based Service (LBS) provider.

F. Networked Cyber-Physical Systems

Networked cyber-physical systems emerged as facilitators for critical infrastructures and other smart city/community applications in recent decades. Among these systems, the smart energy grid, shortly referred to as the smart grid, may be regarded as an important study case of networked cyber-physical systems where privacy-preserving techniques and data-driven models need to be utilized.

A smart grid (SG) is a modern enhancement of the traditional power grid system to ensure reliable electricity delivery, optimize grid operations, and engage consumers [82]. In SG, SMs are installed at consumer homes to report the consumers' power consumption readings periodically (every few minutes) to the system operator (SO) for real-time monitoring, energy management, and billing [304]. However, SG is susceptible to cyber-attacks, where deceitful consumers manipulate their reported electricity consumption to illegally reduce their bills. These attacks not only result in financial losses but also jeopardize the grid's performance as the consumption data is used for grid management. To accurately detect such adversaries, current methods rely on ML models that use the consumption data, violating consumers' privacy by revealing such information about their lifestyle, such as travel habits and appliance usage [116]. To address these privacy and security challenges, a privacy-preserving electricity theft detection scheme, known as PPETD, was proposed in [116]. This scheme employs secret sharing techniques to transmit masked consumption data, allowing the SO to compute aggregated readings for load monitoring and billing without compromising consumers' privacy. It also utilizes SMPC protocols, incorporating arithmetic and binary circuits, to interactively evaluate a CNN-based electricity theft detector on the masked consumption

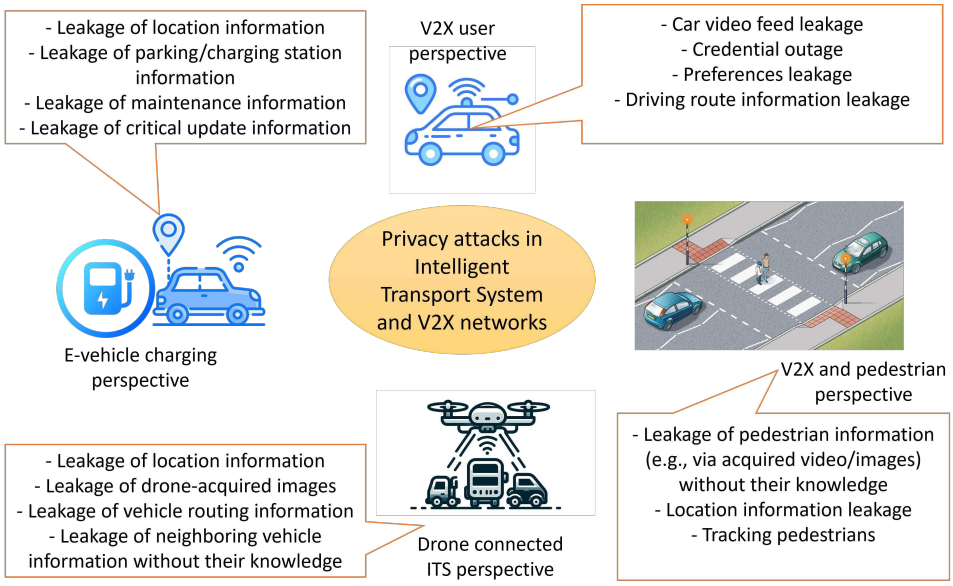


Fig. 12. Privacy attack vectors of V2X and ITS networks that require advanced privacy-preserving techniques integrated with data-driven models.

data, ensuring the privacy of consumers' readings. However, this scheme suffers from considerable computation and communication overhead, as the model evaluation is conducted online through interactive communication between the SO and each SM. Additionally, a trade-off exists between overhead and model accuracy, as it uses approximated operations such as addition, multiplication, and comparison. Furthermore, both the SM and SO know the model's classification, which should only be known by the SO. Dataset from the Irish energy grid [305] has been leveraged by researchers to incorporate data-driven models with privacy-preserving techniques.

To address the limitations in PPETD [116], the authors in [82] proposed a more efficient scheme, called ETDFE, that achieves the same system objectives in terms of monitoring load, computing bills, and identifying electricity theft while protecting the privacy of consumers. This is achieved through the use of FE, where the encrypted data readings are aggregated for load monitoring and billing, and only the aggregated value is known to the SO. Additionally, [79] introduces a novel approach for privacy-preserving, decentralized FL that can detect energy theft cyberattacks. To ensure privacy, an efficient FE-based aggregation method is developed that eliminates the need for a trusted KDC. This approach allows electricity theft detection stations (ETDS) to train local models using their individual customers' power consumption data. The encrypted training parameters are then sent to the aggregator server rather than revealing the model's parameters, which could potentially leak customers' private data through attacks such as membership and inference [79]. The experimental findings demonstrate that this FL-based energy theft detection method offers improved detection accuracy, with reduced computational and communication overhead, compared to previous efforts that rely on the Paillier cryptosystem [306].

On the other hand, the authors of [78] proposed an FL-based energy predictor that considers privacy and communication efficiency for net-metering systems. These systems are commonly utilized to decrease greenhouse gas emissions by installing renewable energy sources, such as solar panels, and selling excess energy back to the grid [80], [307]. In this case, the SMs report the difference between energy consumption and generation, i.e., a net reading, rather than solely reporting energy consumption [304], [308]. The authors employed a real power consumption/generation data set to develop a multi-data-source hybrid DL-based predictor that considers historical net readings and solar irradiance values to accurately predict future net readings. In addition, they proposed an IPFE scheme to enable secure data aggregation and protect customer privacy by encrypting the parameters of their models during FL training. To further address communication efficiency, the authors utilized the change-and-transmit (CAT) approach, which updates local model parameters only when significant changes occur, reducing unnecessary communication.

Lessons Learned

The smart grid is a critical infrastructure that needs to protect its user privacy to thwart possible manipulations and privacy exposure attacks. The solutions discussed need to be generalized as well as customized for other networked cyber-physical systems in smart communities that may range from smart homes, smart hospitals, smart societies, and smart factories. The key challenge is to acquire enough datasets for the other cyber-physical system use cases and validate the privacy-preserving data-driven models for those scenarios based on the experiences derived from the smart grid study case. Furthermore, cyber-physical systems have a data sensing layer (physical plane) and a data computing layer (cyber plane) that are interconnected by the network layer comprising heterogeneous communication protocols. Therefore, it is also important to design an end-to-end privacy-preserving solution across all the layers in the entire cyber-physical ecosystem.

G. Cloud Computing Networks

Cloud computing is a well-known and widely adopted method of delivery of computational resources in networked data centers to users as per their computing needs. Data leaks, however, have emerged as a significant threat to the cloud computing paradigm. Therefore, privacy-preserving techniques are being heavily considered for cloud computing [309] to thwart outsourcing and leaking data to third-party data centers. Researchers indicated the usefulness of FHE for ensuring data privacy under cloud computing settings in [310]. They also demonstrated the lack of adoption of privacy-preserving ML techniques while processing sensitive data (e.g., medical datasets) outsourced into a cloud environment. A combined neural network and HE was then presented to elucidate their agility and feasibility for ML as a service in cloud computing with privacy-preserving properties.

Gupta *et al.* [311] pioneered in presenting a unique system model of cloud computing for privacy-preserving outsourced classification schemes. Their system model consists of data owners, data collectors, and classifier owners, specifically for cloud computing platforms. A data owner that desires to store data in the cloud introduces a statistical model-based noise by exploiting ϵ-DP into the data prior to dispatching it to the data collector, which in turn offers cloud services, including storage, computing, and data sharing to other data owners and the classified owner. The classified owner, on the other hand, performs computing tasks on the acquired data (mixed with noise) from the data collector. Then, a novel privacy-preserving model was conceptualized by combining the strengths of both DP and ML approaches to perform privacy-preserving computation on noisy data. In this method, the ML task exploits the ϵ-DP-induced noisy data rather than encrypted data. Empirical results based on the blood transfusion service center, phoneme, and Wilt datasets demonstrate its robustness in preventing adversaries from accessing the original data of the data owners.

Privacy leakage in cross-silo collaborative learning may lead to data leakages. To address this issue, FL has been considered in the cloud computing paradigm where distributed data centers are considered as participating clients while the parameter aggregator entity resides in a single data center or is virtualized across multiple data centers [312]. Cross-silo FL typically needs to handle a massive number of data samples, which leads to much computation, and computation/communication-efficient FL techniques are emerging to solve these issues along with other challenges, such as statistical, model, and system heterogeneity.

Lessons Learned

Existing research work [311] hints at performance degradation while preserving privacy as complex ML models are used in tandem with privacy-preserving methods. Therefore, performance degradation needs to be carefully formulated and quantified to address the issue optimally. In other words, there should be new performance metrics that jointly address and balance both QoS and Quality of Privacy (QoP) parameters. Also, many of these privacy-preserving data-driven models are not standardized since researchers develop these in a scattered way as proof-of-concepts. It is important to have a standardized set of privacy-preserving data-driven libraries for benchmarking purposes and comparative performance evaluation.

H. Edge Computing Networks

In the study conducted by Hrzich *et al.* [313], an extensive examination of HE techniques is presented, focusing on their integration with ML within cloud and edge computing environments to address privacy concerns [314]. As intelligent edge services, including those in transportation systems and medical IoT, become increasingly integrated into various domains, ML emerges as a key enabler. This shift from centralized ML in cloud data centers to ubiquitous computing on end devices highlights the necessity of preserving the privacy of sensitive data processed by these services [313].

The paper explores the application of Partial, Somewhat, and Fully HE methods across multiple ML models, training these models on encrypted data to produce classification predictions without compromising the data's confidentiality. This approach presents two promising directions: privacy-preserving training and privacy-preserving classification, thereby enabling ML over encrypted data while maintaining acceptable levels of accuracy and computational efficiency. This experimental evaluation serves as a foundational piece, guiding future investigations into which ML models and encryption techniques best balance privacy preservation with performance, particularly in edge computing scenarios where data privacy and security are paramount [314].

Moreover, the adoption of Machine Learning-as-a-Service (MLaaS) by cloud-collaborative edge computing technology leaders as a delivery model further underlines the importance of integrating HE with ML to ensure data privacy during model training and inference phases. This integration is crucial in enabling a wide range of pervasive computing applications to leverage MLaaS while ensuring the confidentiality and integrity of sensitive data [313]. Moreover, researchers in [145] conceptualized the EdgeSanitizer framework that adopts DP in mobile edge computing scenarios by injecting noise into the actual data. The additional layer of data protection achieved by that framework was theoretically validated and empirically evaluated to demonstrate its scalability with resource-constrained edge devices and resilience against invasive inference.

On the other hand, the research work in [315] conceptualized a privacy-preserving AI-based service composition technique for the network edge that exploits FHE. This provides an effective balance between the QoS need of the edge devices and AI model performance for their privacy assurance. FHE permits computations on encrypted data without decryption, thus thwarting potential data manipulation by attackers. Experimental evaluations using a synthetic QoS dataset demonstrate the framework's effectiveness in preserving privacy without compromising the performance of service composition tasks in edge networks. Other works also discussed how ML meets computation and communication control in emerging edge and

cloud computing network systems [18], [24], [221], [316]. Moreover, FL frameworks, to alleviate the computation burden and privacy leakage at the cloud computing level, have been considered to be deployed on the last mile users to facilitate privacy-preserving edge computing [244].

Lessons Learned

The privacy-preserving data-driven models for edge computing scenarios in the literature so far assume that edge devices, which abstract edge functionality as services, are stationary. This assumption may not hold true in dynamic edge environments where devices frequently move or change their operational parameters. Moreover, many of the edge devices in FL have different capabilities in terms of computational resources and the residual energy level. Additionally, some edge devices require more incentives to contribute to collaborative learning due to selfish behavior. Such considerations are theoretically mentioned; however, they are not practically demonstrated in the available proof-of-concepts.

I. Digital Twin Network Systems for Smart Communities

Ahmadi-Assalemi *et al.* [317] discussed the integration of Privacy-Enhancing Technologies (PETs) in the design of Digital Twins (DTs) for smart cities. It highlights the importance of embedding privacy preservation mechanisms from the outset, given the privacy risks posed by data-rich DT models in urban ecosystems. The work outlines the growing value and challenges of DTs, privacy threats, and the role of PETs like HE and SMPC in safeguarding data privacy. The authors emphasize the need for a privacy-aware design in DTs to manage ethical and legal considerations, ensuring privacy and data protection in smart city applications.

In [318], Alisic *et al.* explored the intricate challenges of safeguarding Cyber-Physical Systems (CPS) from learning-based cyber-attacks, with a particular focus on the pivotal role of privacy-preserving measures. A significant portion of their study is dedicated to the use of HE as a tool to prevent adversaries from gaining valuable insights from encrypted data, thereby thwarting potential attacks at their nascent stage. The research meticulously evaluates the impact of encryption parameters and the feasibility of conducting anomaly detection over encrypted data, aiming to complicate the adversaries' efforts without compromising the essential functionalities of CPS.

A key feature of the work conducted in [318] is the practical implementation of a digital twin, i.e., the KTH Live-In Lab Testbed, that translates the above-mentioned theory into practice. The deployed digital twin is powered by the IDA ICE 4.8 software that utilizes real-time sensor data in a smart building for real-time monitoring and sophisticated analysis of behavior of the users (i.e., residents of the building). The digital twin demonstrates how real world modeling can lead to effective smart system control that effectively improves energy efficiency and comfort of the residents while protecting their data privacy.

Lessons Learned

The existing deployment of privacy-preserving technologies within digital twin network systems faces several obstacles. First, the inherent risk of data compromise remains a major concern even when employing data-driven models with privacy-preserving algorithms. Another challenge is that the implementation of these technologies can be computationally intensive due to the need for a high degree of expertise and understanding of these technologies besides the particular application context. The breadth of privacy-preserving data-driven models ranges from initial concepts to advanced tested solutions, showing changing reliability and readiness for the implementation of the digital twin environments. Moreover, the continuous change in digital twin technology poses a unique challenge that is considered a constantly evolving technology for potential attack vectors. This element calls for a flexible and proactive approach to user data privacy and security, predicting and mitigating risks before they materialize. In particular, Advanced Persistent Threats (APTs) should be well-addressed because they are formidable enemies that can use AI-based techniques to take advantage of new vulnerabilities. This emphasizes the need for privacy-preserving techniques to be an integral part of digital twin design to provide robust data exfiltration controls throughout the data lifecycle.

It is also important to underscore the real-world implications of privacy concerns in various sectors, such as autonomous vehicles, healthcare, pharmaceuticals, supply chains, and industrial control systems. The risks to data privacy, anonymity, and security in these areas are deemed substantial, necessitating thorough consideration of privacy and security measures at all stages of digital development and operation. Therefore, organizations transitioning towards digital twins should have a comprehensive understanding of digital twin components, their values, and the critical importance of data security and privacy. This includes actionable steps to manage privacy risks with seamless integration of privacy-preserving techniques with ML/DL models.

J. Semantic Communication and Privacy-preserving Deep Learning Models

Jianrui *et al.* [15] discussed various concepts of semantic communication, where deep learning plays a crucial role in extracting features and facilitating communication. While much of the focus has been on optimizing the local DL models for semantic encoding/decoding, an equally important issue is the challenge of developing distributed multi-user semantic communication for the Metaverse. With the expected device density in 5G+ and emerging 6G networks, significant improvements in spectral efficiency will be needed. Non-orthogonal multiple access (NOMA) can help achieve this by allowing multiple users to share the same frequency and time resources, using advanced spatial division multiple access (SDMA) techniques. These techniques separate users based on their unique antenna patterns and signal characteristics. However, reliable separation of these signals relies heavily on accurate iterative channel estimation and data detection. This system can support up to twice as many users as there are

antennas. Additionally, as the source signals are often non-independent and not identically distributed (non-i.i.d.), it becomes more challenging to train the DL models, which require well-matched knowledge bases (KBs) to function effectively. Users will need to share large amounts of personal data to fully synchronize with the system, raising privacy concerns as this data could be intercepted by malicious actors. Most users will likely prefer to sacrifice some performance in exchange for better privacy protection.

K. Summary: Current Status and Challenges

Table III highlights a high-level comparison of the focused privacy-preserving data-driven models for emerging communication networks discussed in this section. It is worth noting as a caveat that we have investigated specific applications that benefit from privacy-preserving data-driven models, such as smart health, smart energy, and smart cities. While communication is a key enabler, not all verticals require privacy. Our survey does not propose a one-size-fits-all solution; instead, it highlights tailored privacy-preserving, data-driven approaches for different networking applications.

Implementing privacy-preserving models in real-world communication networks presents several practical challenges. One major issue is interoperability, as these models often need to integrate with various existing systems, including data-driven models and standards, which may not be fully compatible. Additionally, the hardware requirements for supporting advanced privacy-preserving techniques can be significant, necessitating investment in high-performance computing resources. Scalability is another concern, as ensuring that privacy measures can handle large volumes of data without compromising performance is critical. Latency introduced by complex encryption and data processing techniques can also impact the real-time performance of communication networks. Furthermore, the complexity of maintaining and updating these models to adapt to evolving privacy threats and regulatory requirements adds to the implementation burden. Addressing these challenges requires careful planning, robust infrastructure, and ongoing monitoring and optimization.

VI. Open Research Issues and Future Directions

While privacy-preserving data-driven models offer promising opportunities in emerging 6G network communications, they also come with several inherent challenges, as well as more subtle, complex ones. In this section, we discuss the key constraints and open challenges that researchers may need to carefully consider.

A. Privacy-preserving Model Training and Resource Issues in Emerging Networks

Significant communication resources are required by privacy-preserving techniques, such as HE, SMPC, and DP, that result in a noticeable increase of network latency [319], [320], which is not desirable for emerging networks due to their low latency requirements. FL also requires computational resources on resource-constrained systems, which may provide a unique challenge [321]. Thus, the privacy-preserving algorithms on top of data-driven models significantly increase the computational burden on not only network devices but also the overall networking infrastructure. As a consequence, training time and energy consumption could be significantly impacted with regard to desired 6G network key performance metrics, such as energy efficiency and sustainability.

In addition to the introduced communication burden, the privacy-preserving techniques, along with data-driven models, are intuitively prone to consuming more communication bandwidth. For instance, sharing encrypted gradients periodically for large-sized data over a large number of users can significantly degrade communication efficiency. Similarly, SMPC parameters exchange involving a large number of user devices may contribute to a substantial increase in the network traffic, thereby impacting bandwidth and delay requirements of emerging 6G network systems.

With regard to the massive number of user devices in 6G networks, particularly in IoT systems, privacy-preserving data-driven models may not scale well [322]. With the growing number and diversity of participants in FL or SMPC, the resultant complexity and overhead of adequately maintaining privacy may significantly rise, inhibiting their deployability at scale. In addition, model performance in DP-assisted models may add noise to the data or gradients to ensure data privacy, and thereby adversely impact the desired accuracy of those models. Therefore, it is imperative to fine-tune the model performance and privacy level to scale well with emerging communication systems.

Besides the model performance tradeoffs mentioned above, the deployment and seamless adoption of privacy-preserving techniques with data-driven emerging network systems warrants standardization. This is a huge challenge in the context of 6G systems due to the heterogeneity in networking equipment and user devices [246]. When the open radio access networks and open 5G/6G core network standards are being developed, work groups for privacy preservation, data-driven models, and their integration on network functions management need to be clearly drafted before the actual implementation. In other words, our survey thus far revealed that there are initiatives from various researchers/industry stakeholders; however, they are mostly proof-of-work at this point. Appropriate standardization planning should be prioritized in the domain of privacy-preserving data-driven models for 6G network systems. By adopting the right strategies for data protection regulation, aligned with the existing practices (such as GDPR introduced in the European Union), privacy-preserving ML/DL models can be usefully embedded in various tiers of emerging networks.

In order to effectively address the aforementioned limitations pertaining to privacy-preserving data-driven model training, it is important to develop lightweight algorithmic solutions as well as adequate regulatory frameworks to protect data privacy without significantly impacting computing and communication efficiency.

TABLE III
SECTION V SUMMARY, PRESENTING EACH SUBSECTION'S KEY FOCUS AND FINDINGS, TECHNIQUES, AND CHALLENGES ADDRESSED.

Section	Key Focus	Key Findings/Techniques	Challenges Addressed
V-A: 5G and Beyond Open Core Network Systems	Privacy-preserving data-driven models in 5G/6G networks	Integration of Fully HE (FHE) for secure operations	High computational overhead, complexity of implementation
V-B: Open and Reconfigurable Radio Access Networks (RANs)	Privacy in dynamic and complex 6G RAN environments	Use of Graph Neural Networks (GNNs) combined with Homomorphic Encryption (HE)	Privacy preservation in open network structures
V-C: IoT Systems and Networks	Privacy issues in IoT layers (sensing, networking, computing)	Hybrid Secure Multi-Party Computation (SMPC) and ML techniques	Energy constraints, data privacy, scalability
V-D: Software-Defined Networks (SDNs)	Privacy in centralized SDN frameworks	Integration of Differential Privacy with Generative Adversarial Networks (GANs)	Balancing privacy with network performance
V-E: Intelligent Vehicular Networks	Privacy in V2X communications	Use of Differential Privacy and HE for secure vehicular communication	High bandwidth and low latency requirements
V-F: Networked Cyber-Physical Systems	Privacy in Smart Grids and Cyber-Physical Systems	Functional Encryption and Federated Learning for secure energy management	Computational overhead, maintaining privacy in real-time data
V-G: Cloud Computing Networks	Privacy in cloud-based data processing	Privacy-preserving ML using Homomorphic Encryption and Differential Privacy	Performance degradation, data leakage risks
V-H: Edge Computing Networks	Privacy at the edge with limited resources	Homomorphic Encryption and Differential Privacy for edge devices	Resource constraints, dynamic environments
V-I: Digital Twin Network Systems for Smart Communities	Privacy in Digital Twins for smart cities	Integration of Privacy-Enhancing Technologies (PETs) in Digital Twins	Scalability, evolving threat landscapes
V-J: Semantic Communication and Privacy-preserving Data-driven Models	Privacy-performance tradeoff in semantic communication	DL model training based on well-matched knowledge bases while preserving user data-privacy	Scalability, evolving privacy protection requirements.

B. Quantum Computing-resilient Privacy-preserving Data-driven Models

Quantum computing poses a significant threat to current encryption schemes due to its ability to solve complex mathematical problems much more efficiently than classical computers. Algorithms like Shor's algorithm can factorize large integers exponentially faster, rendering many widely used encryption methods, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), vulnerable to decryption. This impending risk necessitates a proactive approach to evaluate the resilience of privacy-preserving models against quantum attacks. By understanding the specific ways quantum computing can compromise these models, we can better prepare for a future where classical encryption may no longer be secure.

To mitigate these threats, researchers have explored various post-quantum cryptography methods that can be integrated to enhance the resilience of privacy-preserving models. These methods include lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography techniques [323], all of which are designed to withstand quantum attacks. Lattice-based cryptography, for example, leverages the hardness of lattice problems, which remain difficult for quantum computers to solve. Additionally, hash-based cryptographic methods provide security through hash functions, which are resistant to quantum decryption techniques. Integrating these post-quantum methods into existing privacy-preserving models will ensure they remain robust and secure in the face of advancing quantum computing capabilities. This proactive integration is crucial for maintaining data privacy and security in future communication networks as explored in recent research work such as [324].

Researchers are paying a great deal of attention to quantum computing-resilient security protocols for communication systems, and this is also applicable to privacy-preserving data-driven models. This is because of the quantum computer's anticipated capability to handle complex computations

with unprecedented speeds that may make inversion attacks against data-driven models viable [325]. Privacy-preserving data-driven models relying on HE and FE, i.e., cryptographic measures, could be, in turn, vulnerable to quantum computing-capable adversaries. In particular, quantum computing is assumed to be able to invalidate the security assumptions made by current HE schemes, thereby nullifying their provided privacy guarantees. Moreover, quantum computing may facilitate novel manipulations against the cryptographic primitives utilized in SMPC. This may reveal the private data or compromise the computational integrity required for SMPC. In the case of DP, quantum computers could be harnessed to process and analyze the noisy outputs at unprecedented efficiency and speeds that might render the privacy-preserving technique ineffective. Furthermore, the data-driven models could be subject to quantum computing-enabled adversarial attacks that may cause corrupt model training.

In order to address the impact of quantum computing on privacy-preserving data-driven models, embedding post-quantum cryptography is important, albeit challenging, due to the need for substantial change in contemporary communication systems and networks. Regulatory and standardization policies to combat the quantum-computing adversaries in emerging networks are required to be drafted in a proactive and systemic manner. In this vein, rethinking the vulnerabilities of privacy and security protocols of communication systems and networks is required through an interdisciplinary collaboration among networking researchers, cryptographers, and quantum physicists.

C. Privacy-preserving Data-Driven Model Challenges in Social Networks and Crowd-sourced Data Networks

Emerging communication networks support social networking data and crowd-sourced data networks, and preserving the privacy of such networks remains a daunting task. This is due to the inherent properties of crowd-sourced and social networks that have diverse users with dynamic user behavior. While they involve location information, personal preferences, interactions, and other sensitive data exchange over the emerging communication networks, perfect anonymization for training large data-driven models may not be possible due to issues such as cross-referencing with other datasets, reverse engineering network architecture, and so forth [326]. Furthermore, training data-driven models in conjunction with privacy-preserving techniques may take the informed consent of the users of such networks for granted along with other challenges, e.g., dynamic join, departure, and change of activities of the users [327]. However, this may be difficult to facilitate with one-shot training of privacy-preserving data-driven models. This issue becomes even more complex with big data, which are typically unstructured and have heterogeneous data types and formats. Such unstructured data from social networks and crowd-sourced environments need to be processed and converted to appropriate structured types for training privacy-preserving data-driven models.

Effectively addressing the aforementioned challenges pertaining to crowd-sourced and social networks warrants a multi-dimensional approach comprising both technical and regulatory advancements of privacy-preserving techniques fused with data-driven models. A robust and informed consent mechanism, although challenging, requires to be embedded with emerging networks to guarantee compliance with privacy regulations [328].

D. Challenges on Deploying Privacy-preserving Data-driven Models in the Edge

As described throughout this survey, FL and other forms of collaborative learning techniques to overcome the heterogeneous users' computational resource limitations in the edge have recently appeared as an appealing privacy-preserving mechanism. However, data heterogeneity, coupled with user device heterogeneity and their selfish behavior to participate in collaborative learning in the absence of an incentive mechanism, may be a key barrier to utilizing such learning frameworks. The communication overhead is also a key bottleneck in such collaborative learning paradigms, which researchers are taking into consideration; however, their findings need to motivate seamless incorporation of communication-efficient FL protocols in B5G and 6G networks. Also, in the face of adversarial participants, how privacy leakage can be prevented needs to be thoroughly investigated with possible scalability implications. The scalability of such environments is also subject to the synchronization among heterogeneous user devices and the central aggregator entity.

To design more robust and scalable FL frameworks with adequate privacy-preserving guarantees, the integration of SMPC, HE, and DP is being considered by researchers. However, their seamless incorporation appears challenging and needs to be clarified with comprehensive and quantitative performance metrics, particularly on participating node fairness and privacy outcomes. Furthermore, personalized FL asynchronicity options and model compression techniques to optimize the limited resources available on edge devices need to be considered. Detection and mitigation of model poisoning, as well as malicious updates, are also of paramount importance in such collaborative learning settings. Future iterations of FL could also exploit fully decentralized parameter aggregation without relying on a centralized entity, and blockchain or similar techniques could be exploited for coordination and trust on parameter exchange and updates that may not be mutable. Personalized models are particularly important in FL due to the non-IID (non-independent and identically distributed) nature of data across different participants. Recent research has made significant strides in this area, such as the FedProto method proposed by Tan et al. [329]. FedProto enables personalized learning by creating prototypes that represent heterogeneous data distributions across clients, allowing each client to learn a model that is better suited to its specific data. This approach significantly improves model accuracy and generalization across diverse data sources. Furthermore, the PFedHN (Personalized Federated Learning using Hypernetwork) framework is introduced [330], which utilizes hypernetworks to generate personalized models for each client. This framework effectively addresses the challenge

of non-IID (non-Independent and Identically Distributed) data by tailoring models to individual clients while preserving the benefits of FL's collaborative nature.

Privacy-preserving data-driven models, if trained with somewhat limited and/or perturbed data, may be subject to overfitting problems. This leads to a lack of generalization, which is even more amplified in collaborating learning scenarios. As a remedy, knowledge distillation has been considered in FL to enhance model performance, particularly in scenarios where communication efficiency and privacy preservation are paramount. For instance, researchers in [331] introduced pFedCo-TA (Personalized Federated Learning method based on Teacher Assistant Knowledge Distillation). The pFedCo-TA approach utilizes knowledge distillation to improve model accuracy and communication efficiency. The approach clusters clients based on data similarity, assigns assistants to facilitate knowledge transfer between teacher and student models, and demonstrates significant performance improvements over traditional methods. [332] proposes a privacy-preserving and communication-efficient FL framework using ensemble cross-domain knowledge distillation. The method employs one-shot offline knowledge distillation with unlabeled, cross-domain public data, ensuring stronger privacy guarantees by introducing quantized and noisy ensemble predictions. Experimental results across image and text classification tasks demonstrate that this approach outperforms traditional FL methods in both accuracy and communication efficiency while maintaining robust privacy protection. The work in [333] proposes a communication-efficient and privacy-preserving personalized FL framework that introduces a feature fusion-based mutual learning approach that enables personalized learning while reducing communication costs by only sharing a small-scale shared model with the global model. Additionally, the framework incorporates a gradient compression technique with chaotic encrypted cyclic measurement matrices to enhance privacy without adding significant computational overhead, demonstrating superior performance and privacy preservation in FL scenarios with heterogeneous data. Moreover, The authors in [291] present an FL algorithm that integrates KD with LDP to achieve communication efficiency and enhanced privacy in heterogeneous systems. The proposed method allows clients to design their own local models while protecting sensitive data through LDP and extends the privacy guarantees to the exchanged soft labels using the post-processing immunity property of DP.

E. Challenges on Incorporating privacy-preserving as a QoS Metric

While emerging networks focus heavily on fine-tuning QoS and QoE (quality of experience) along with various security attributes, researchers often investigate the tradeoff between QoS/QoE and security parameters [334]. The interplay between QoS and privacy in adversarial deep learning models has been demonstrated to be a tradeoff problem [335], which is worth investigating further in the context of emerging networks. However, privacy is an additional metric that warrants careful research investigation, which is indeed unexplored in the literature. Doing so can allow privacy to be addressed as an intrinsic service quality attribute, which can then be appropriately fine-tuned with other QoS/QoE requirements, such as bandwidth, delay, fairness, and so forth. However, the actual definition of such a comprehensive QoS-privacy metric is an open research issue since it may consist of various elements, such as data leakage risk factor, anonymity level, and so forth. Also, such a privacy-based QoS metric may not be generalizable or scale well with a wide spectrum and sizes of datasets that are required to train robust data-driven models with privacy-preserving capabilities. The lack of standardized privacy-preserving techniques in emerging network systems also makes it challenging to quantitatively compare the privacy aspects of different service providers.

In addition, even though privacy introduced as a tunable input to service performance metrics is appealing, it may result in an additional layer of complexity to the training of the data-driven models. In particular, hyperparameter tuning may require more effort, and robust methods to accurately fine-tune the hyperparameters need to be developed in the future.

F. Challenges on Optimal Privacy-preserving Hybrid Model Selection and Training

Privacy-preserving hybrid model training is an important aspect, which warrants careful attention due to the unique challenge involved in managing and coordinating between diverse model architectures [336]. In addition, the hybrid model frameworks may result in synchronized model update issues, and possible privacy leakage across the hybrid model layers, particularly when distributed, collaborative learning frameworks are used for IoT systems [337]. Because the distributed nodes may have different privacy requirements, their lack of synergistic participation may degrade model convergence and stability performances, along with possible privacy leakage of user data. Furthermore, integrating hybrid models with multiple privacy preservation mechanisms, such as DP, SMPC, and HE, may lead to heavier models, which may not scale well with emerging networks leaning toward edge computing solutions. As a result, the computational burden of privacy-preserving hybrid data-driven models and their communication efficiency that may impact the network systems need to be carefully studied in the future.

G. Challenges Associated With Privacy-preserving Data-driven Models in the Entire Ecosystem

In emerging networks, there is a focus on integrated satellite-aerial-terrestrial-underwater networks. These networks have different radio access technologies and have inherently different communication protocols to cater to unique user needs [2]. As a consequence, embedding the same set of privacy-preserving data-driven models across such a broad ecosystem of networks may lead to side effects in terms of unexpected communication and privacy performance outcomes [338]. Recent research work [339] in this area shows a number of key challenges where AI-assisted privacy-preserving task offloading in integrated satellite-terrestrial networks is discussed. The integration of privacy-preserving data-driven model-based mechanisms could be naturally suited in

core networks that address a high volume of data generated from various access networks at extremely high speeds. Since SDNs and other emerging solutions for core networks can handle big network data at scale, it makes sense to deploy such privacy-preserving models at the core network level and study the actual impact on throughput, latency, and bandwidth usage. However, optimizing the privacy-preserving mechanism overhead so that the effect on communication performance is minimized requires further investigation. On the other hand, deploying them in terrestrial and/or aerial access networks requires more careful planning for actual field implementation. This is also applicable to IoT network systems that connect massive numbers of devices and sensors that may not scale naturally with privacy-preserving AI models. Therefore, the IoT sensing (data generation) plane could be deemed as a privacy bottleneck in the entire ecosystem, and it is critical to safeguard against potential privacy leakage in the "weak links" of the ecosystem.

H. Challenges on Embedding Privacy-preserving Data-driven Models with Cell-free Communication Networks

Cell-free communication networks recently appeared as an exciting alternative to cellular communications, whereby a dense cluster of base stations aims to serve mobile users in tandem. The concept of privacy preservation of users is garnering attention in cell-free network systems in recent times [340], [341] in addition to their traditional focus on the physical layer performance improvement. However, when a group of base stations obtains the location information of the mobile users, it may take just one compromised base station to leak out location information or other sensitive information of the user that it serves. This may introduce additional complexities to the already complex resource and cluster optimization problems in cell-free network systems. The reason behind this is that the privacy-preserving data-driven models need to be deployed and managed by the already overburdened base stations, and this may substantially impact the existing optimization problem formulation. Furthermore, metadata and signal patterns exchanged between the base stations could potentially leak the users' location in a cell-free network environment. While some researchers started investigating channel estimation with regard to privacy preservation in cell-free network systems [341], it is still not a mature area of research, and further investigations are required.

I. Compatibility Issues of Privacy-preserving Data-driven Models with Blockchain-Based Networks

Different implementations of blockchains in recent years appeared as an exciting security provisioning technique for network providers to facilitate transparent transactions. While there is a genuine debate about scaling the distributed database/ledger construct of the blockchain in emerging networks [342], blockchain's role in conceptualizing transparent network slicing contracts in these networks has been considered in 3GPP studies. How blockchain-enabled networks can co-exist with privacy-preserving data-driven models is appearing as a hot research topic recently [343], [344] that requires careful assessment of these inherently different enabling technologies. Researchers need to investigate whether these two technologies can complement each other or are mutually disjoint. For instance, the security, audibility, and non-mutability of blockchain result in transparent transactions that are visible to all the users that may unwillingly expose private information (e.g., at what time the user committed the record, at which location the user was, and so forth) [345]. Even if blockchain and privacy-preserving data-driven models have non-complementary roles, it is critical to demonstrate how the joint consideration of both may impact the latency and throughput performance of B5G and 6G systems.

J. Challenges on Guaranteeing Freshness of Data-driven Models due to Model Decay and Privacy Leakage

Data-driven models equipped with privacy-preserving mechanisms may need to be periodically retrained and redeployed to combat the decaying model's effect as investigated by recent research work in [283], [346]. As new data continue to arrive at the network, old models may become outdated. This may be particularly valid for collaborative learning frameworks. It is, therefore, important to determine the frequency of model updates. Also, determining the threshold of model decay in dynamically changing massive network systems is a challenging yet important topic of research that needs much research attention. The additional overhead from privacy-preserving techniques, such as SMPC, DP, and HE, may contribute to delayed model updates. Furthermore, the topic of model freshness in privacy-sensitive applications overlaps with ethical and regulatory standards, and 3GPP needs to step in its efforts to have an interdisciplinary lens to tie all these considerations together in a cohesive manner.

VII. Conclusion

Recently, safeguarding privacy while harnessing data for emerging networks appeared as a top priority across communication landscapes, ranging from the core fabrics of the Internet to the ever-expanding realms of IoT systems. Our survey in this paper demonstrated an important research gap in the literature, namely the fusion of privacy with data-driven models to complement the communication performance outcome with privacy-preserving requirements. Our survey, therefore, paves the way for future networks to explicitly embed the consideration of user privacy into network function orchestration.

Emerging networks with embedded AI may predict traffic flows, detect malicious activities, and self-optimize to recover from failure, and our survey connects the topic of privacy preservation to make such embedded AI models even more robust. As privacy-preserving techniques, we explained how HE, SMPC, DP, and collaborative learning can be coupled with data-driven models. By seamless integration of privacy-preserving techniques with data-driven models, we demonstrated how the expected communication performance can be met while guaranteeing the data privacy of network users. The survey also revealed the status quo and actual

challenges involved in integrating these advanced privacy-preserving methods with data-driven models in emerging networks. Tradeoff problems, such as maintaining privacy and, at the same time, achieving high-quality model predictions for relevant network functions, were discussed in the survey. In addition, the topic of deployment scalability of the privacy-preserving data-driven models in emerging networks was also covered both in breadth and depth through a number of lessons learned. The survey also provided a list of open research issues and possible research directions in the realm of privacy-preserving AI models that range from the model training overhead and privacy quantification as a QoS metric to model decaying phenomena under the effect of privacy-preserving techniques. Therefore, this paper is anticipated to stimulate a wide spectrum of research work in an interdisciplinary domain of communication networks, privacy and security practitioners, and regulatory bodies.

REFERENCES

[1] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Cell-free massive MIMO: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 492–523, 2022, doi: 10.1109/COMST.2021.3123267.

[2] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2714–2741, 2018, doi: 10.1109/COMST.2018.2841996.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[4] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2020, doi: 10.1109/COMST.2019.2944748.

[5] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. P. Fitzek, and N. Aaraj, "Survey on fully homomorphic encryption, theory, and applications," *Proceedings of the IEEE*, vol. 110, no. 10, pp. 1572–1609, 2022, doi: 10.1109/JPROC.2022.3205665.

[6] Y. Yang, X. Huang, X. Liu, H. Cheng, J. Weng, X. Luo, and V. Chang, "A comprehensive survey on secure outsourced computation and its applications," *IEEE Access*, vol. 7, pp. 159 426–159 465, 2019, doi: 10.1109/ACCESS.2019.2949782.

[7] X. Yin, Y. Zhu, and J. Hu, "A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions," *ACM Computing Surveys*, vol. 54, no. 6, article no. 131, 2021, doi: 10.1145/3460427.

[8] K. Bedda, Z. M. Fadlullah, and M. M. Fouda, "Efficient wireless network slicing in 5G networks: An asynchronous federated learning approach," in *2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 2022, doi: 10.1109/IoTaIS56727.2022.9976007.

[9] Y. Gupta, Z. M. Fadlullah, and M. M. Fouda, "Toward asynchronously weight updating federated learning for AI-on-edge IoT systems," in *2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 2022, doi: 10.1109/IoTaIS56727.2022.9975908.

[10] N. Nasser, Z. M. Fadlullah, M. M. Fouda, A. Ali, and M. Imran, "A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept," *Computer Networks*, vol. 205, article no. 108672, 2022, doi: 10.1016/j.comnet.2021.108672.

[11] G. Gad, Z. M. Fadlullah, K. Rabie, and M. M. Fouda, "Communication-efficient privacy-preserving federated learning via knowledge distillation for human activity recognition systems," in *ICC 2023 - IEEE International Conference on Communications*, 2023, doi: 10.1109/ICC45041.2023.10278987.

[12] H. Zhang, H. Wang, Y. Li, K. Long, and A. Nallanathan, "DRL-driven dynamic resource allocation for task-oriented semantic communication," *IEEE Transactions on Communications*, vol. 71, no. 7, pp. 3992–4004, 2023, doi: 10.1109/TCOMM.2023.3274145.

[13] Z. Weng, Z. Qin, X. Tao, C. Pan, G. Liu, and G. Y. Li, "Deep learning enabled semantic communications with speech recognition and synthesis," *arXiv preprint arXiv:2205.04603*, 2023, doi: 10.48550/arXiv.2205.04603.

[14] D. B. Kurka and D. Gündüz, "DeepJSCC-f: Deep joint-source channel coding of images with feedback," *arXiv preprint arXiv:1911.11174*, 2019, doi: 10.48550/arXiv.1911.11174.

[15] J. Chen, J. Wang, C. Jiang, Y. Ren, and L. Hanzo, "Trustworthy semantic communications for the metaverse relying on federated learning," *IEEE Wireless Communications*, vol. 30, 2023, doi: 10.1109/MWC.001.2200587.

[16] F. Tang, B. Mao, Y. Kawamoto, and N. Kato, "Survey on machine learning for intelligent end-to-end communication toward 6G: From network access, routing to traffic control and streaming adaption," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1578–1598, 2021, doi: 10.1109/COMST.2021.3073009.

[17] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2020, doi: 10.1109/JPROC.2019.2954595.

[18] T. K. Rodrigues, K. Suto, H. Nishiyama, J. Liu, and N. Kato, "Machine learning meets computation and communication control in evolving edge and cloud: Challenges and future perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 38–67, 2020, doi: 10.1109/COMST.2019.2943405.

[19] E. Baccour, N. Mhaisen, A. A. Abdellatif, A. Erbad, A. Mohamed, M. Hamdi, and M. Guizani, "Pervasive AI for IoT applications: A survey on resource-efficient distributed artificial intelligence," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2366–2418, 2022, doi: 10.1109/COMST.2022.3200740.

[20] V. Chamola, V. Hassija, S. Gupta, A. Goyal, M. Guizani, and B. Sikdar, "Disaster and pandemic management using machine learning: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 16 047–16 071, 2021, doi: 10.1109/JIOT.2020.3044966.

[21] B. Mao, F. Tang, Y. Kawamoto, and N. Kato, "AI models for green communications towards 6G," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 210–247, 2022, doi: 10.1109/COMST.2021.3130901.

[22] F. Tang, B. Mao, N. Kato, and G. Gui, "Comprehensive survey on machine learning in vehicular network: Technology, applications and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 2027–2057, 2021, doi: 10.1109/COMST.2021.3089688.

[23] I. Ilahi, M. Usama, J. Qadir, M. U. Janjua, A. Al-Fuqaha, D. T. Hoang, and D. Niyato, "Challenges and countermeasures for adversarial attacks on deep reinforcement learning," *IEEE Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 90–109, 2022, doi: 10.1109/TAI.2021.3111139.

[24] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 869–904, 2020, doi: 10.1109/COMST.2020.2970550.

[25] H. C. Tanuwidjaja, R. Choi, S. Baek, and K. Kim, "Privacy-preserving deep learning on machine learning as a service—a comprehensive survey," *IEEE Access*, vol. 8, pp. 167 425–167 447, 2020, doi: 10.1109/ACCESS.2020.3023084.

[26] R. Podschwadt, D. Takabi, P. Hu, M. H. Rafiei, and Z. Cai, "A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption," *IEEE Access*, vol. 10, pp. 117 477–117 500, 2022, doi: 10.1109/ACCESS.2022.3219049.

[27] A. Falcetta and M. Roveri, "Privacy-preserving deep learning with homomorphic encryption: An introduction," *IEEE Computational Intelligence Magazine*, vol. 17, no. 3, pp. 14–25, 2022, doi: 10.1109/MCI.2022.3180883.

[28] J.-W. Lee, H. Kang, Y. Lee, W. Choi, J. Eom, M. Deryabin, E. Lee, J. Lee, D. Yoo, Y.-S. Kim, and J.-S. No, "Privacy-preserving machine learning with fully homomorphic encryption for deep neural network," *IEEE Access*, vol. 10, pp. 30 039–30 054, 2022, doi: 10.1109/ACCESS.2022.3159694.

[29] Q. Zhang, C. Xin, and H. Wu, "Privacy-preserving deep learning based on multiparty secure computation: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 412–10 429, 2021, doi: 10.1109/JIOT.2021.3058638.

[30] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2694–2724, 2020, doi: 10.1109/COMST.2020.3011561.

[31] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021, doi: 10.1109/COMST.2021.3108618.

[32] A. E. Ouadrhiri and A. Abdelhadi, "Differential privacy for deep and federated learning: A survey," *IEEE Access*, vol. 10, pp. 22 359–22 380, 2022, doi: 10.1109/ACCESS.2022.3151670.

[33] J. Zhao, Y. Chen, and W. Zhang, "Differential privacy preservation in deep learning: Challenges, opportunities and solutions," *IEEE Access*, vol. 7, pp. 48 901–48 911, 2019, doi: 10.1109/ACCESS.2019.2909559.

[34] X. Li, Y. Chen, C. Wang, and C. Shen, "When deep learning meets differential privacy: Privacy,security, and more," *IEEE Network*, vol. 35, no. 6, pp. 148–155, 2021, doi: 10.1109/MNET.001.2100256.

[35] W. Wei and L. Liu, "Gradient leakage attack resilient deep learning," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 303–316, 2022, doi: 10.1109/TIFS.2021.3139777.

[36] S. Ali, M. M. Irfan, A. Bomai, and C. Zhao, "Towards privacy-preserving deep learning: Opportunities and challenges," in *2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA)*, 2020, doi: 10.1109/DSAA49011.2020.00077.

[37] D. Mercier, A. Lucieri, M. Munir, A. Dengel, and S. Ahmed, "Evaluating privacy-preserving machine learning in critical infrastructures: A case study on time-series classification," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7834–7842, 2022, doi: 10.1109/TII.2021.3124476.

[38] Q. Xu, Z. Su, and R. Li, "Security and privacy in artificial intelligence-enabled 6G," *IEEE Network*, vol. 36, no. 5, pp. 188–196, 2022, doi: 10.1109/MNET.117.2100730.

[39] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 53–87, 2022, doi: 10.1109/COMST.2021.3131332.

[40] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[41] E. Ustundag Soykan, L. Karaçay, F. Karakoç, and E. Tomur, "A survey and guideline on privacy enhancing technologies for collaborative machine learning," *IEEE Access*, vol. 10, pp. 97 495–97 519, 2022, doi: 10.1109/ACCESS.2022.3204037.

[42] C. Liu, Z. Wei, D. W. K. Ng, J. Yuan, and Y.-C. Liang, "Deep transfer learning for signal detection in ambient backscatter communications," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1624–1638, 2021, doi: 10.1109/TWC.2020.3034895.

[43] K. Mei, J. Liu, X. Zhang, N. Rajatheva, and J. Wei, "Performance analysis on machine learning-based channel estimation," *IEEE Transactions on Communications*, vol. 69, no. 8, pp. 5183–5193, 2021, doi: 10.1109/TCOMM.2021.3083597.

[44] Y. Xu, G. Gui, H. Gacanin, and F. Adachi, "A survey on resource allocation for 5G heterogeneous networks: Current research, future trends, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 668–695, 2021, doi: 10.1109/COMST.2021.3059896.

[45] G. Nan, X. Liu, X. Lyu, Q. Cui, X. Xu, and P. Zhang, "UD-Sem: A unified distributed learning framework for semantic communications over wireless networks," *IEEE Network*, 2023, doi: 10.1109/MNET.131.2200409. Early access.

[46] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2595–2621, 2018, doi: 10.1109/COMST.2018.2846401.

[47] M. Sengly, K. Lee, and J.-R. Lee, "Joint optimization of spectral efficiency and energy harvesting in D2D networks using deep neural network," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8361–8366, 2021, doi: 10.1109/TVT.2021.3055205.

[48] M. Z. Islam, R. Ali, A. Haider, and H. S. Kim, "QoS provisioning: Key drivers and enablers toward the tactile internet in beyond 5G era," *IEEE Access*, vol. 10, pp. 85 720–85 754, 2022, doi: 10.1109/ACCESS.2022.3197900.

[49] C.-L. Chen, H. Wang, A. Chen, C. Han, Y.-C. Wei, and X. Li, "Machine learning for trust, security, and privacy in computing and communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2023, article no. 40, 2023, doi: 10.1186/s13638-023-02249-0.

[50] K. Agarwal and T. Kumar, "Email spam detection using integrated approach of naïve bayes and particle swarm optimization," in *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2018, doi: 10.1109/ICCONS.2018.8662957.

[51] A. Weinand, C. Lipps, M. Karrenbauer, and H. Schotten, "Naïve bayes supervised learning based physical layer authentication: Anti-spoofing techniques for industrial radio systems," vol. 18, 03 2023, doi: 10.34190/iccws.18.1.983.

[52] G. He, Y. Ren, M. Bian, G. Feng, and X. Zhang, "Privacy-enhanced and non-interactive linear regression with dropout-resilience," *Information Sciences*, vol. 632, pp. 69–86, 2023, doi: 10.1016/j.ins.2023.02.080.

[53] S. Sakib, T. Tazrin, M. M. Fouda, Z. M. Fadlullah, and N. Nasser, "A deep learning method for predictive channel assignment in beyond 5G networks," *IEEE Network*, vol. 35, no. 1, pp. 266–272, 2021, doi: 10.1109/MNET.011.2000301.

[54] G. Qiu, X. Gui, and Y. Zhao, "Privacy-preserving linear regression on distributed data by homomorphic encryption and data masking," *IEEE Access*, vol. 8, pp. 107 601–107 613, 2020, doi: 10.1109/ACCESS.2020.3000764.

[55] P. Mohassel and Y. Zhang, "SecureML: A system for scalable privacy-preserving machine learning," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, doi: 10.1109/SP.2017.12.

[56] H. Kikuchi, H. Hashimoto, H. Yasunaga, and T. Saito, "Scalability of privacy-preserving linear regression in epidemiological studies," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, 2015, doi: 10.1109/AINA.2015.229.

[57] X. Dong, J. Chen, K. Zhang, and H. Qian, "Privacy-preserving locally weighted linear regression over encrypted millions of data," *IEEE Access*, vol. 8, pp. 2247–2257, 2020, doi: 10.1109/ACCESS.2019.2962700.

[58] A. Shanbhag, S. Vincent, S. B. B. Gowda, O. P. Kumar, and S. A. J. Francis, "Leveraging metaheuristics for feature selection with machine learning classification for malicious packet detection in computer networks," *IEEE Access*, vol. 12, pp. 21 745–21 764, 2024, doi: 10.1109/ACCESS.2024.3362246.

[59] R. Marsalek, K. Youssefova, and M. Pospisil, "Support vector machine - based classification of wireless transceivers," in *2021 31st International Conference Radioelektronika (RADIOELEKTRONIKA)*, 2021, doi: 10.1109/RADIOELEKTRONIKA52220.2021.9420191.

[60] K. Tekbiyik, Akbunar, A. R. Ekti, A. Görçin, and G. Karabulut Kurt, "Multi–dimensional wireless signal identification based on support vector machines," *IEEE Access*, vol. 7, pp. 138 890–138 903, 2019, doi: 10.1109/ACCESS.2019.2942368.

[61] F. Tian, Y. Yu, X. Yuan, B. Lyu, and G. Gui, "Predicted decoupling for coexistence between WiFi and LTE in unlicensed band," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4130–4141, 2020, doi: 10.1109/TVT.2020.2976939.

[62] D. Puthal, E. Damiani, and S. P. Mohanty, "Secure and scalable collaborative edge computing using decision tree," in *2022 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2022, doi: 10.1109/ISVLSI54635.2022.00055.

[63] A. Kjamilji, "A constant time secure and private evaluation of decision trees in smart cities enabled by mobile IoT," in *2023 IEEE International Conference on Smart Mobility (SM)*, 2023, doi: 10.1109/SM57895.2023.10112275.

[64] C. Wang, T. Xu, and X. Qin, "Network traffic classification with improved random forest," in *2015 11th International Conference on Computational Intelligence and Security (CIS)*, 2015, doi: 10.1109/CIS.2015.27.

[65] Y. Y. Aung and M. M. Min, "An analysis of random forest algorithm based network intrusion detection system," in *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2017, doi: 10.1109/SNPD.2017.8022711.

[66] Y. Chang, W. Li, and Z. Yang, "Network intrusion detection based on random forest and support vector machine," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 1, 2017, doi: 10.1109/CSE-EUC.2017.118.

[67] Y. Zhai and X. Zheng, "Random forest based traffic classification method in SDN," in *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)*, 2018, doi: 10.1109/ICCBB.2018.8756496.

[68] Q. Liao, B. Cabral, J. P. Fernandes, and N. Lourenço, "Herb: Privacy-preserving random forest with partially homomorphic encryption," in *2022 International Joint Conference on Neural Networks (IJCNN)*, 2022, doi: 10.1109/IJCNN55064.2022.9892321.

[69] Y. Zhang, P. Feng, and Y. Ning, "Random forest algorithm based on differential privacy protection," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021, doi: 10.1109/TrustCom53373.2021.00172.

[70] J. Hou, Q. Li, S. Meng, Z. Ni, Y. Chen, and Y. Liu, "DPRF: A differential privacy protection random forest," *IEEE Access*, vol. 7, pp. 130 707–130 720, 2019, doi: 10.1109/ACCESS.2019.2939891.

[71] R. Gong and M. Li, "A random forest based encryption algorithm for privacy data of e-commerce information," in *2022 Global Reliability and Prognostics and Health Management (PHM-Yantai)*, 2022, doi: 10.1109/PHM-Yantai55411.2022.9942133.

[72] N. Kato, Z. M. Fadlullah, B. Mao, F. Tang, O. Akashi, T. Inoue, and K. Mizutani, "The deep learning vision for heterogeneous network traffic control: Proposal, challenges, and future perspective," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 146–153, 2017, doi: 10.1109/MWC.2016.1600317WC.

[73] J. Han, X. Zeng, X. Xue, and J. Ma, "Physical layer secret key generation based on autoencoder for weakly correlated channels," in *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, 2020, doi: 10.1109/ICCC49849.2020.9238931.

[74] B. Khadem and S. Mohebalizadeh, "Efficient UAV physical layer security based on deep learning and artificial noise," *arXiv preprint arXiv:2004.01343*, 2020, doi: 10.48550/arXiv.2004.01343.

[75] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-aware communication over a wiretap channel with generative networks," in *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2022, doi: 10.1109/ICASSP43922.2022.9747068.

[76] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques*, 2003, doi: 10.1007/3-540-39200-9_16.

[77] M. I. Ibrahem, M. M. Badr, M. M. Fouda, M. Mahmoud, W. Alasmary, and Z. M. Fadlullah, "PMBFE: Efficient and privacy-preserving monitoring and billing using functional encryption for AMI networks," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, doi: 10.1109/ISNCC49221.2020.9297246.

[78] M. M. Badr, M. M. E. A. Mahmoud, Y. Fang, M. Abdulaal, A. J. Aljohani, W. Alasmary, and M. I. Ibrahem, "Privacy-preserving and communication-efficient energy prediction scheme based on federated learning for smart grids," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7719–7736, 2023, doi: 10.1109/JIOT.2022.3230586.

[79] M. I. Ibrahem, M. Mahmoud, M. M. Fouda, B. M. ElHalawany, and W. Alasmary, "Privacy-preserving and efficient decentralized federated learning-based energy theft detector," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, doi: 10.1109/GLOBECOM48099.2022.10000881.

[80] M. M. Badr, M. I. Ibrahem, M. Mahmoud, W. Alasmary, M. M. Fouda, K. H. Almotairi, and Z. M. Fadlullah, "Privacy-preserving federated-learning-based net-energy forecasting," in *SoutheastCon 2022*, 2022, doi: 10.1109/SoutheastCon48659.2022.9764093.

[81] M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, W. Alasmary, and X. Shen, "Privacy preserving and efficient data collection scheme for AMI networks using deep learning," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 17 131–17 146, 2021, doi: 10.1109/JIOT.2021.3077897.

[82] M. I. Ibrahem, M. Nabil, M. M. Fouda, M. M. E. A. Mahmoud, W. Alasmary, and F. Alsolami, "Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for AMI networks," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1243–1258, 2021, doi: 10.1109/JIOT.2020.3026692.

[83] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques*, 1999, doi: 10.1007/3-540-48910-X_16.

[84] D. Mittal, D. Kaur, and A. Aggarwal, "Secure data mining in cloud using homomorphic encryption," in *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 2014, doi: 10.1109/CCEM.2014.7015496.

[85] L. Morris, "Analysis of partially and fully homomorphic encryption," *Rochester Institute of Technology*, vol. 10, pp. 1–5, 2013.

[86] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the forty-first annual ACM symposium on Theory of computing*, 2009, doi: 10.1145/1536414.1536440.

[87] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption," *Cryptology ePrint Archive*, 2012.

[88] J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, and A. Yun, "Batch fully homomorphic encryption over the integers," in *Advances in Cryptology–EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2013, doi: 10.1007/978-3-642-38348-9_20.

[89] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, 2011, doi: 10.1109/FOCS.2011.12.

[90] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory*, vol. 6, no. 3, article no. 13, 2014, doi: 10.1145/2633600.

[91] M. Clear and C. Mcgoldrick, "Attribute-based fully homomorphic encryption with a bounded number of inputs," in *Proceedings of the 8th International Conference on Progress in Cryptology – AFRICACRYPT 2016*, 2016, doi: 10.1007/978-3-319-31517-1_16.

[92] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachene, "Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds," in *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security*, 2016, doi: 10.1007/978-3-662-53887-6_1.

[93] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "TFHE: fast fully homomorphic encryption over the torus," *Journal of Cryptology*, vol. 33, no. 1, pp. 34–91, 2020, doi: 10.1007/s00145-019-09319-x.

[94] W. Utami, I. Syafalni, M. I. Arsyad, A. Indrayanto, and T. Adiono, "Homomorphic encryption versus RSA: Cloud security performance analysis," in *2021 International Symposium on Electronics and Smart Devices (ISESD)*, 2021, doi: 10.1109/ISESD53023.2021.9501717.

[95] C. Mouchet, J. Troncoso-Pastoriza, J.-P. Bossuat, and J.-P. Hubaux, "Multiparty homomorphic encryption from ring-learning-with-errors," *Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. CONF, pp. 291–311, 2021, doi: 10.2478/popets-2021-0071.

[96] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proceedings of the forty-fourth annual ACM symposium on Theory of computing (STOC)*, 2012, doi: 10.1145/2213977.2214086.

[97] M. Ghadamyari and S. Samet, "Privacy-preserving statistical analysis of health data using paillier homomorphic encryption and permissioned blockchain," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, doi: 10.1109/BigData47090.2019.9006231.

[98] A. Biswas, A. Karan, N. Nigam, H. Doreswamy, S. Sadykanova, and M. Z. Rauliyevna, "Implementation of cyber security for enabling data protection analysis and data protection using robot key homomorphic encryption," in *2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2022, doi: 10.1109/I-SMAC55078.2022.9987407.

[99] T.-Y. Youn, N.-S. Jho, and K.-Y. Chang, "Practical additive homomorphic encryption for statistical analysis over encrypted data," in *2016 International Conference on Platform Technology and Service (PlatCon)*, 2016, doi: 10.1109/PlatCon.2016.7456817.

[100] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1333–1345, 2018, doi: 10.1109/TIFS.2017.2787987.

[101] Y. Aono, T. Hayashi, L. T. Phong, and L. Wang, "Privacy-preserving logistic regression with distributed data sources via homomorphic encryption," *IEICE Transactions on Information and Systems*, vol. 99, no. 8, pp. 2079–2089, 2016, doi: 10.1587/transinf.2015INP0020.

[102] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "FedHealth: A federated transfer learning framework for wearable healthcare," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 83–93, 2020, doi: 10.1109/MIS.2020.2988604.

[103] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, and Y. Liu, "BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning," in *Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC 2020)*, 2020. [Online]. Available: https://www.usenix.org/conference/atc20/presentation/zhang-chengliang

[104] H. Fang and Q. Qian, "Privacy preserving machine learning with homomorphic encryption and federated learning," *Future Internet*, vol. 13, no. 4, article no. 94, 2021, doi: 10.3390/fi13040094.

[105] L. Zhang, Z. Zhang, and C. Guan, "Accelerating privacy-preserving momentum federated learning for industrial cyber-physical systems," *Complex & Intelligent Systems*, vol. 7, pp. 3289–3301, 2021, doi: 10.1007/s40747-021-00519-2.

[106] J. Park and H. Lim, "Privacy-preserving federated learning using homomorphic encryption," *Applied Sciences*, vol. 12, no. 2, article no. 734, 2022, doi: 10.3390/app12020734.

[107] S. Hardy, W. Henecka, H. Ivey-Law, R. Nock, G. Patrini, G. Smith, and B. Thorne, "Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption," *arXiv preprint arXiv:1711.10677*, 2017, doi: 10.48550/arXiv.1711.10677.

[108] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in *Theory of Cryptography: 8th Theory of Cryptography Conference (TCC)*, 2011, doi: 10.1007/978-3-642-19571-6_16.

[109] P. Panzade and D. Takabi, "Towards faster functional encryption for privacy-preserving machine learning," in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2021, doi: 10.1109/TPSISA52974.2021.00003.

[110] M. I. Ibrahem and M. M. Fouda, "A lightweight privacy-preserving load forecasting and monitoring scheme supporting dynamic billing for smart grids: No KDC required," *IEEE Internet of Things Journal*, vol. 11, no. 19, pp. 32 160–32 171, 2024, doi: 10.1109/JIOT.2024.3426486.

[111] D. Sharma and D. C. Jinwala, "Encrypted data ordering with functional encryption," in *2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, 2018, doi: 10.1109/RAIT.2018.8389084.

[112] J. Wang, C. Huang, K. Yang, J. Wang, X. Wang, and X. Chen, "MAVP-FE: Multi-authority vector policy functional encryption with efficient encryption and decryption," *China Communications*, vol. 12, no. 6, pp. 126–140, 2015, doi: 10.1109/CC.2015.7122471.

[113] S. Agrawal, B. Libert, and D. Stehlé, "Fully secure functional encryption for inner products, from standard assumptions," in *Advances in Cryptology – CRYPTO 2016: Annual International Cryptology Conference*, 2016, doi: 10.1007/978-3-662-53015-3_12.

[114] M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval, "Simple functional encryption schemes for inner products," in *Public-Key Cryptography – PKC 2015: IACR International Workshop on Public Key Cryptography*, 2015, doi: 10.1007/978-3-662-46447-2_33.

[115] C. Baltico, D. Catalano, D. Fiore, and R. Gay, "Practical functional encryption for quadratic functions with applications to predicate encryption," in *Advances in Cryptology – CRYPTO 2017, Annual International Cryptology Conference*, 2017, doi: 10.1007/978-3-319-63688-7_3.

[116] M. Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmary, and E. Serpedin, "PPETD: Privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks," *IEEE Access*, vol. 7, pp. 96 334–96 348, 2019, doi: 10.1109/ACCESS.2019.2925322.

[117] A. C.-C. Yao, "How to generate and exchange secrets," in *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, 1986, doi: 10.1109/SFCS.1986.25.

[118] M. O. Rabin, "How to exchange secrets with oblivious transfer," *Cryptology ePrint Archive, Paper 2005/187*, 2005. [Online]. Available: https://eprint.iacr.org/2005/187

[119] O. Goldreich, S. Micali, and A. Wigderson, *How to Play Any Mental Game, or a Completeness Theorem for Protocols with Honest Majority*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 307–328. ISBN 9781450372664, doi: 10.1145/3335741.3335755.

[120] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivious transfers efficiently," in *Advances in Cryptology - CRYPTO 2003: Annual International Cryptology Conference*, 2003, doi: 10.1007/978-3-540-45146-4_9.

[121] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, P. Rindal, and P. Scholl, "Efficient two-round ot extension and silent non-interactive secure computation," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019, doi: 10.1145/3319535.3354255.

[122] A. Gascón, P. Schoppmann, B. Balle, M. Raykova, J. Doerner, S. Zahur, and D. Evans, "Privacy-preserving distributed linear regression on high-dimensional data," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, pp. 345–364, 2017, doi: 10.1515/popets-2017-0053.

[123] M. Barni, C. Orlandi, and A. Piva, "A privacy-preserving protocol for neural-network-based computation," in *Proceedings of the 8th Workshop on Multimedia and Security*, 2006, doi: 10.1145/1161366.1161393. . ISBN 1595934936

[124] B. D. Rouhani, M. S. Riazi, and F. Koushanfar, "Deepsecure: Scalable provably-secure deep learning," in *Proceedings of the 55th Annual Design Automation Conference (DAC)*, 2018, doi: 10.1145/3195970.3196023.

[125] J. Liu, M. Juuti, Y. Lu, and N. Asokan, "Oblivious neural network predictions via MiniONN transformations," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2017, doi: 10.1145/3133956.3134056.

[126] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, article no. 12, 2019, doi: 10.1145/3298981.

[127] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A framework for fast privacy-preserving computations," in *Computer Security - ESORICS 2008*, 2008, doi: 10.1007/978-3-540-88313-5_13.

[128] W. Du, Y. S. Han, and S. Chen, "Privacy-preserving multivariate statistical analysis: Linear regression and classification," in *Proceedings of the 2004 SIAM International Conference on Data Mining (SDM)*, doi: 10.1137/1.9781611972740.21. pp. 222–233.

[129] Y. Li and W. Xu, "PrivPy: General and scalable privacy-preserving data mining," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge (KDD)*, 2019, doi: 10.1145/3292500.3330920.

[130] P. Mohassel and P. Rindal, "ABY3: a mixed protocol framework for machine learning," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018, doi: 10.1145/3243734.3243760.

[131] Y. Khazbak, T. Tan, and G. Cao, "MLGuard: mitigating poisoning attacks in privacy preserving distributed collaborative learning," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, 2020, doi: 10.1109/ICCCN49398.2020.9209670.

[132] Y. Zhang, G. Bai, X. Li, C. Curtis, C. Chen, and R. K. L. Ko, "PrivColl: Practical privacy-preserving collaborative machine learning," in *Computer Security - ESORICS 2020: European Symposium on Research in Computer Security*, 2020, doi: 10.1007/978-3-030-58951-6_20.

[133] F. Karakoç, M. Önen, and Z. Bilgin, "Secure aggregation against malicious users," in *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies (SACMAT)*, 2021, doi: 10.1145/3450569.3463572.

[134] T. D. Nguyen, P. Rieger, H. Chen, H. Yalame, H. Möllering, H. Fereidooni, S. Marchal, M. Miettinen, A. Mirhoseini, S. Zeitouni, F. Koushanfar, A.-R. Sadeghi, and T. Schneider, "FLAME: Taming backdoors in federated learning," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/nguyen

[135] H. Fereidooni, S. Marchal, M. Miettinen, A. Mirhoseini, H. Möllering, T. D. Nguyen, P. Rieger, A.-R. Sadeghi, T. Schneider, H. Yalame, and S. Zeitouni, "SAFELearn: secure aggregation for private federated learning," in *2021 IEEE Security and Privacy Workshops (SPW)*, 2021, doi: 10.1109/SPW53761.2021.00017.

[136] A. Blanco-Justicia, J. Domingo-Ferrer, S. Martínez, D. Sánchez, A. Flanagan, and K. E. Tan, "Achieving security and privacy in federated learning systems: Survey, research challenges and future directions," *Engineering Applications of Artificial Intelligence*, vol. 106, article no. 104468, 2021, doi: https://doi.org/10.1016/j.engappai.2021.104468.

[137] E. Shi, H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Annual Network & Distributed System Security Symposium (NDSS)*, 2011. [Online]. Available: https://www.ndss-symposium.org/ndss2011/privacy-preserving-aggregation-of-time-series-data/

[138] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2017, doi: 10.1145/3133956.3133982.

[139] Q. Li and G. Cao, "Efficient and privacy-preserving data aggregation in mobile sensing," in *2012 20th IEEE International Conference on Network Protocols (ICNP)*, 2012, doi: 10.1109/ICNP.2012.6459985.

[140] L. Xiang, W. Li, J. Yang, X. Wang, and B. Li, "Differentially-private deep learning with directional noise," *IEEE Transactions on Mobile Computing*, vol. 22, no. 5, pp. 2599–2612, 2023, doi: 10.1109/TMC.2021.3130060.

[141] Z. Xu, S. Shi, A. X. Liu, J. Zhao, and L. Chen, "An adaptive and fast convergent approach to differentially private deep learning," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, doi: 10.1109/INFOCOM41043.2020.9155359.

[142] E. Ustundag Soykan, Z. Bilgin, M. A. Ersoy, and E. Tomur, "Differentially private deep learning for load forecasting on smart grid," in *2019 IEEE Globecom Workshops (GC Wkshps)*, 2019, doi: 10.1109/GCWkshps45667.2019.9024520.

[143] T. Zhu, D. Ye, W. Wang, W. Zhou, and P. S. Yu, "More than privacy: Applying differential privacy in key areas of artificial intelligence," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 6, pp. 2824–2843, 2022, doi: 10.1109/TKDE.2020.3014246.

[144] P. C. Mahawaga Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "Local differential privacy for deep learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5827–5842, 2020, doi: 10.1109/JIOT.2019.2952146.

[145] C. Xu, J. Ren, L. She, Y. Zhang, Z. Qin, and K. Ren, "EdgeSanitizer: locally differentially private deep inference at the edge for mobile data analytics," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5140–5151, 2019, doi: 10.1109/JIOT.2019.2897005.

[146] Y. Wang, M. Gu, J. Ma, and Q. Jin, "DNN-DP: differential privacy enabled deep neural network learning framework for sensitive crowdsourcing data," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 1, pp. 215–224, 2020, doi: 10.1109/TCSS.2019.2950017.

[147] D. Li, J. Wang, Z. Tan, X. Li, and Y. Hu, "Differential privacy preservation in interpretable feedforward-designed convolutional neural networks," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, doi: 10.1109/TrustCom50675.2020.00089.

[148] A.-T. Tran, T. D. Luong, X. S. Pham, and T. L. Tran, "Deep models with differential privacy for distributed web attack detection," in *2022 14th International Conference on Knowledge and Systems Engineering (KSE)*, 2022, doi: 10.1109/KSE56063.2022.9953788.

[149] F. Kerschbaum, "Towards privacy in deep learning," in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2021, doi: 10.1109/TPSISA52974.2021.00031.

[150] A. Wood, M. Altman, A. Bembenek, M. Bun, M. Gaboardi, J. Honaker, K. Nissim, D. R. O'Brien, T. Steinke, and S. Vadhan, "Differential privacy: A primer for a non-technical audience," *Vanderbilt Journal of Entertainment & Technology Law*, vol. 21, no. 1, article no. 4, pp. 209–276, 2018, doi: 10.2139/ssrn.3338027.

[151] R. Subramanian, "Differential privacy techniques for healthcare data," in *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*, 2022, doi: 10.1109/IDSTA55301.2022.9923037.

[152] J. Zhang, J. Sun, R. Zhang, Y. Zhang, and X. Hu, "Privacy-preserving social media data outsourcing," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2018, doi: 10.1109/INFOCOM.2018.8486242.

[153] H. Li, Y. Cui, S. Wang, J. Liu, J. Qin, and Y. Yang, "Multivariate financial time-series prediction with certified robustness," *IEEE Access*, vol. 8, pp. 109 133–109 143, 2020, doi: 10.1109/ACCESS.2020.3001287.

[154] S. Salim, B. Turnbull, and N. Moustafa, "A blockchain-enabled explainable federated learning for securing internet-of-things-based social media 3.0 networks," *IEEE Transactions on Computational Social Systems*, 2021, doi: 10.1109/TCSS.2021.3134463. Early access.

[155] H. Jiang, J. Pei, D. Yu, J. Yu, B. Gong, and X. Cheng, "Applications of differential privacy in social network analysis: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 1, pp. 108–127, 2023, doi: 10.1109/TKDE.2021.3073062.

[156] N. Zhou and S. Long, "Social network data publishing model satisfying differential privacy," in *2022 International Conference on Informatics, Networking and Computing (ICINC)*, 2022, doi: 10.1109/ICINC58035.2022.00040.

[157] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014, doi: 10.1561/0400000042.

[158] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, 2006, doi: 10.1007/11681878_14.

[159] I. Mironov, "Rényi differential privacy," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, 2017, doi: 10.1109/CSF.2017.11.

[160] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2016, doi: 10.1145/2976749.2978318.

[161] Q. Ye, H. Hu, X. Meng, and H. Zheng, "PrivKV: Key-value data collection with local differential privacy," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, doi: 10.1109/SP.2019.00018.

[162] H. Shin, S. Kim, J. Shin, and X. Xiao, "Privacy enhanced matrix factorization for recommendation with local differential privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 9, pp. 1770–1782, 2018, doi: 10.1109/TKDE.2018.2805356.

[163] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, 2013, doi: 10.1109/FOCS.2013.53.

[164] J. Hsu, S. Khanna, and A. Roth, "Distributed private heavy hitters," in *Automata, Languages, and Programming*, 2012, doi: 10.1007/978-3-642-31594-7_39.

[165] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," *arXiv preprint arXiv:1710.06963*, 2017, doi: 10.48550/arXiv.1710.06963.

[166] N. Agarwal, A. T. Suresh, F. Yu, S. Kumar, and H. B. McMahan, "cpSGD: communication-efficient and differentially-private distributed SGD," in *NIPS'18: Proceedings of the 32nd International Conference on Neural Information Processing Systems*, 2018. [Online]. Available: https://dl.acm.org/doi/10.5555/3327757.3327856

[167] A. Bhowmick, J. Duchi, J. Freudiger, G. Kapoor, and R. Rogers, "Protection against reconstruction and its applications in private federated learning," *arXiv preprint arXiv:1812.00984*, 2018, doi: 10.48550/arXiv.1812.00984.

[168] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," *arXiv preprint arXiv:1712.07557*, 2017, doi: 10.48550/arXiv.1712.07557.

[169] Y. Zhao, J. Zhao, M. Yang, T. Wang, N. Wang, L. Lyu, D. Niyato, and K.-Y. Lam, "Local differential privacy-based federated learning for internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8836–8853, 2021, doi: 10.1109/JIOT.2020.3037194.

[170] N. Wang, X. Xiao, Y. Yang, J. Zhao, S. C. Hui, H. Shin, J. Shin, and G. Yu, "Collecting and analyzing multidimensional data with local differential privacy," in *2019 IEEE 35th International Conference on Data Engineering (ICDE)*, 2019, doi: 10.1109/ICDE.2019.00063.

[171] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Minimax optimal procedures for locally private estimation," *Journal of the American Statistical Association*, vol. 113, no. 521, pp. 182–201, 2018, doi: 10.1080/01621459.2017.1389735.

[172] S. Truex, L. Liu, K.-H. Chow, M. E. Gursoy, and W. Wei, "Ldp-fed: Federated learning with local differential privacy," in *Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking (EdgeSys)*, 2020, doi: 10.1145/3378679.3394533.

[173] L. Sun, J. Qian, and X. Chen, "LDP-FL: Practical private aggregation in federated learning with local differential privacy," in *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence (IJCAI)*, 2021, doi: 10.24963/ijcai.2021/217.

[174] M. Naseri, J. Hayes, and E. De Cristofaro, "Local and central differential privacy for robustness and privacy in federated learning," *arXiv preprint arXiv:2009.03561*, 2020, doi: 10.48550/arXiv.2009.03561.

[175] Z. Sun, P. Kairouz, A. T. Suresh, and H. B. McMahan, "Can you really backdoor federated learning?" *arXiv preprint arXiv:1911.07963*, 2019, doi: 10.48550/arXiv.1911.07963.

[176] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, doi: 10.1109/SP.2017.41.

[177] G. Yang, S. Wang, and H. Wang, "Federated learning with personalized local differential privacy," in *2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS)*, 2021, doi: 10.1109/ICCCS52626.2021.9449232.

[178] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. Vincent Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3454–3469, 2020, doi: 10.1109/TIFS.2020.2988575.

[179] G. Ács and C. Castelluccia, "I have a DREAM! (DiffeRentially privatE smArt Metering)," in *IH 2011: Information Hiding - International Workshop on Information Hiding*, 2011, doi: 10.1007/978-3-642-24178-9_9.

[180] S. Goryczka and L. Xiong, "A comprehensive comparison of multiparty secure additions with differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 5, pp. 463–477, 2017, doi: 10.1109/TDSC.2015.2484326.

[181] J. Doweck, W.-F. Kao, A. K.-y. Lu, J. Mandelblat, A. Rahatekar, L. Rappoport, E. Rotem, A. Yasin, and A. Yoaz, "Inside 6th-generation intel core: New microarchitecture code-named skylake," *IEEE Micro*, vol. 37, no. 2, pp. 52–62, 2017, doi: 10.1109/MM.2017.38.

[182] T. Hunt, C. Song, R. Shokri, V. Shmatikov, and E. Witchel, "Chiron: Privacy-preserving machine learning as a service," *arXiv preprint arXiv:1803.05961*, 2018, doi: 10.48550/arXiv.1803.05961.

[183] T. Hunt, Z. Zhu, Y. Xu, S. Peter, and E. Witchel, "Ryoan: A distributed sandbox for untrusted computation on secret data," *ACM Transactions on Computer Systems*, vol. 35, no. 4, article no. 13, 2017, doi: 10.1145/3231594.

[184] A. Nilsson, P. N. Bideh, and J. Brorsson, "A survey of published attacks on intel SGX," *arXiv preprint arXiv:2006.13598*, 2020, doi: 10.48550/arXiv.2006.13598.

[185] C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Mitigating sybils in federated learning poisoning," *arXiv preprint arXiv:1808.04866*, 2018, doi: 10.48550/arXiv.1808.04866.

[186] T. Lee, Z. Lin, S. Pushp, C. Li, Y. Liu, Y. Lee, F. Xu, C. Xu, L. Zhang, and J. Song, "Occlumency: Privacy-preserving remote deep-learning inference using SGX," in *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2019, doi: 10.1145/3300061.3345447.

[187] F. Tramer and D. Boneh, "Slalom: Fast, verifiable and private execution of neural networks in trusted hardware," *arXiv preprint arXiv:1806.03287*, 2018, doi: 10.48550/arXiv.1806.03287.

[188] Z. Gu, H. Jamjoom, D. Su, H. Huang, J. Zhang, T. Ma, D. Pendarakis, and I. Molloy, "Reaching data confidentiality and model accountability on the CalTrain," in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2019, doi: 10.1109/DSN.2019.00044.

[189] N. Hynes, R. Cheng, and D. Song, "Efficient deep learning on multi-source private data," *arXiv preprint arXiv:1807.06689*, 2018, doi: 10.48550/arXiv.1807.06689.

[190] K. G. Narra, Z. Lin, Y. Wang, K. Balasubramaniam, and M. Annavaram, "Privacy-preserving inference in machine learning services using trusted execution environments," *arXiv preprint arXiv:1912.03485*, 2019, doi: 10.48550/arXiv.1912.03485.

[191] H. Hashemi, Y. Wang, and M. Annavaram, "DarKnight: A data privacy scheme for training and inference of deep neural networks," *arXiv preprint arXiv:2006.01300*, 2020, doi: 10.48550/arXiv.2006.01300.

[192] L. K. L. Ng, S. S. M. Chow, A. P. Y. Woo, D. P. H. Wong, and Y. Zhao, "Goten: GPU-outsourcing trusted execution of neural network training," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 35, no. 17, pp. 14 876–14 883, 2021, doi: 10.1609/aaai.v35i17.17746.

[193] Y. Chen, F. Luo, T. Li, T. Xiang, Z. Liu, and J. Li, "A training-integrity privacy-preserving federated learning scheme with trusted execution environment," *Information Sciences*, vol. 522, pp. 69–79, 2020, doi: 10.1016/j.ins.2020.02.037.

[194] M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Pati, A. Kotrotsou, M. Milchenko, W. Xu, D. Marcus, R. R. Colen *et al.*, "Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data," *Scientific reports*, vol. 10, no. 1, article no. 12598, 2020, doi: 10.1038/s41598-020-69250-1.

[195] F. Mo and H. Haddadi, "Efficient and private federated learning using TEE," in *EuroSys 2019*, 2019. [Online]. Available: https://eurosys2019.org/wp-content/uploads/2019/03/eurosys19posters-abstract66.pdf

[196] F. Mo, A. S. Shamsabadi, K. Katevas, S. Demetriou, I. Leontiadis, A. Cavallaro, and H. Haddadi, "DarkneTZ: Towards model privacy at the edge using trusted execution environments," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2020, doi: 10.1145/3386901.3388946.

[197] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis, "PPFL: Privacy-preserving federated learning with trusted execution environments," in *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2021, doi: 10.1145/3458864.3466628.

[198] Z. Gu, H. Huang, J. Zhang, D. Su, H. Jamjoom, A. Lamba, D. Pendarakis, and I. Molloy, "Confidential inference via ternary model partitioning," *arXiv preprint arXiv:1807.00969*, 2020, doi: 10.48550/arXiv.1807.00969.

[199] H. Chen, K. Laine, and R. Player, "Simple encrypted arithmetic library - SEAL v2.1," Cryptology ePrint Archive, Paper 2017/224, 2017. [Online]. Available: https://eprint.iacr.org/2017/224

[200] S. Halevi and V. Shoup, "Algorithms in HElib," Cryptology ePrint Archive, Paper 2014/106, 2014. [Online]. Available: https://eprint.iacr.org/2014/106

[201] ——, "Design and implementation of HElib: a homomorphic encryption library," Cryptology ePrint Archive, Paper 2020/1481, 2020. [Online]. Available: https://eprint.iacr.org/2020/1481

[202] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "TFHE: Fast fully homomorphic encryption library," August 2016, https://tfhe.github.io/tfhe/.

[203] D. B. Cousins, G. W. Ryan, K. Rohloff, and Y. Polyakov, "Palisade homomorphic encryption software library," 2019. [Online]. Available: https://palisade-crypto.org/

[204] W. Dai and B. Sunar, "cuHE: A homomorphic encryption accelerator library," in *Cryptography and Information Security in the Balkans*, 2016, doi: 10.1007/978-3-319-29172-7_11.

[205] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Advances in Cryptology – ASIACRYPT 2017*, 2017, doi: 10.1007/978-3-319-70694-8_15.

[206] F. Boemer, Y. Lao, R. Cammarota, and C. Wierzynski, "nGraph-HE: a graph compiler for deep learning on homomorphically encrypted data," in *Proceedings of the 16th ACM International Conference on Computing Frontiers*, 2019, doi: 10.1145/3310273.3323047.

[207] C. Juvekar, V. Vaikuntanathan, and A. Chandrakasan, "GAZELLE: A low latency framework for secure neural network inference," in *27th USENIX Security Symposium (USENIX Security)*, 2018, pp. 1651–1669. [Online]. Available: https://dl.acm.org/doi/10.5555/3277203.3277326

[208] G. E. Dahl, D. Yu, L. Deng, and A. Acero, "Context-dependent pre-trained deep neural networks for large-vocabulary speech recognition," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 20, no. 1, pp. 30–42, 2012, doi: 10.1109/TASL.2011.2134090.

[209] J. W. Bos, K. Lauter, J. Loftus, and M. Naehrig, "Improved security for a ring-based fully homomorphic encryption scheme," in *IMACC 2013–Cryptography and Coding: IMA International Conference on Cryptography and Coding*, 2013, doi: 10.1007/978-3-642-45239-0_4.

[210] T. Marc, M. Stopar, J. Hartman, M. Bizjak, and J. Modic, "Privacy-enhanced machine learning with functional encryption," in *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security*, 2019, doi: 10.1007/978-3-030-29959-0_1.

[211] Q. Wang, L. Zhou, J. Bai, Y. S. Koh, S. Cui, and G. Russello, "HT2ML: An efficient hybrid framework for privacy-preserving machine learning using HE and TEE," *Computers & Security*, vol. 135, p. 103509, 2023, doi: 10.1016/j.cose.2023.103509.

[212] R. Xu, N. Baracaldo, Y. Zhou, A. Anwar, and H. Ludwig, "HybridAlpha: An efficient approach for privacy-preserving federated learning," in *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (AISec)*, 2019, doi: 10.1145/3338501.3357371.

[213] H. B. McMahan, E. Moore, D. Ramage, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2023, doi: 10.48550/arXiv.1602.05629.

[214] V. Mugunthan, A. Peraire-Bueno, and L. Kagal, "PrivacyFL: A simulator for privacy-preserving and secure federated learning," in *Proceedings of the 29th ACM International Conference on Information & Knowledge Management (CIKM)*, 2020, doi: 10.1145/3340531.3412771.

[215] J. So, B. Guler, A. S. Avestimehr, and P. Mohassel, "CodedPrivateML: A fast and privacy-preserving framework for distributed machine learning," *arXiv preprint arXiv:1902.00641*, 2019, doi: 10.48550/arXiv.1902.00641.

[216] J. Hamm, A. C. Champion, G. Chen, M. Belkin, and D. Xuan, "Crowd-ML: A privacy-preserving learning framework for a crowd of smart devices," in *2015 IEEE 35th International Conference on Distributed Computing Systems*, 2015, doi: 10.1109/ICDCS.2015.10.

[217] S. Abdulrahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani, "A survey on federated learning: The journey from centralized to distributed on-site learning and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5476–5497, 2021, doi: 10.1109/JIOT.2020.3030072.

[218] L. Liu, Y. Wang, G. Liu, K. Peng, and C. Wang, "Membership inference attacks against machine learning models via prediction sensitivity," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 2341–2347, 2023, doi: 10.1109/TDSC.2022.3180828.

[219] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G internet of things: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, 2022, doi: 10.1109/JIOT.2021.3103320.

[220] M. Nabil, A. Sherif, M. Mahmoud, W. Alsmary, and M. Alsabaan, "Accurate and privacy-preserving person localization using federated-learning and the camera surveillance systems of public places," *IEEE Access*, vol. 10, pp. 109 894–109 907, 2022, doi: 10.1109/ACCESS.2022.3214227.

[221] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020, doi: 10.1109/COMST.2020.2986024.

[222] S. Sai, V. Hassija, V. Chamola, and M. Guizani, "Federated learning and NFT-based privacy-preserving medical-data-sharing scheme for intelligent diagnosis in smart healthcare," *IEEE Internet of*

Things Journal, vol. 11, no. 4, pp. 5568–5577, 2024, doi: 10.1109/JIOT.2023.3308991.

[223] M. Akter, N. Moustafa, T. Lynar, and I. Razzak, "Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 12, pp. 5805–5816, 2022, doi: 10.1109/JBHI.2022.3192648.

[224] J. Li, Y. Meng, L. Ma, S. Du, H. Zhu, Q. Pei, and X. Shen, "A federated learning based privacy-preserving smart healthcare system," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2021–2031, 2022, doi: 10.1109/TII.2021.3098010.

[225] A. Khanna, V. Schaffer, G. Gürsoy, and M. Gerstein, "Privacy-preserving model training for disease prediction using federated learning with differential privacy," in *2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, 2022, doi: 10.1109/EMBC48229.2022.9871742.

[226] A. K. Singh, P. M. Sharma, M. Bhatt, A. Choudhary, S. Sharma, and S. Sadhukhan, "Comparative analysis on artificial intelligence technologies and its application in FinTech," in *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 2022, doi: 10.1109/ICAISS55157.2022.10010573.

[227] Y. Liang, Z. Liu, Y. Song, A. Yang, X. Ye, and Y. Ouyang, "A methodology of trusted data sharing across telecom and finance sector under china's data security policy," in *2021 IEEE International Conference on Big Data (Big Data)*, 2021, doi: 10.1109/BigData52589.2021.9671857.

[228] S. Dhiman, S. Nayak, G. K. Mahato, A. Ram, and S. K. Chakraborty, "Homomorphic encryption based federated learning for financial data security," in *2023 4th International Conference on Computing and Communication Systems (I3CS)*, 2023, doi: 10.1109/I3CS58314.2023.10127502.

[229] X. Yuan, J. Chen, N. Zhang, X. Fang, and D. Liu, "A federated bidirectional connection broad learning scheme for secure data sharing in internet of vehicles," *China Communications*, vol. 18, no. 7, pp. 117–133, 2021, doi: 10.23919/JCC.2021.07.010.

[230] X. Zhou, R. Ke, Z. Cui, Q. Liu, and W. Qian, "STFL:spatio-temporal federated learning for vehicle trajectory prediction," in *2022 IEEE 2nd International Conference on Digital Twins and Parallel Intelligence (DTPI)*, 2022, doi: 10.1109/DTPI55838.2022.9998967.

[231] S. Chuprov, K. M. Bhatt, and L. Reznik, "Federated learning for robust computer vision in intelligent transportation systems," in *2023 IEEE Conference on Artificial Intelligence (CAI)*, 2023, doi: 10.1109/CAI54212.2023.00019.

[232] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, doi: 10.1109/SP.2019.00029.

[233] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction APIs," in *Proceedings of the 25th USENIX Conference on Security Symposium*, 2016, pp. 601–618. [Online]. Available: https://dl.acm.org/doi/10.5555/3241094.3241142

[234] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman, "SoK: Security and privacy in machine learning," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018, doi: 10.1109/EuroSP.2018.00035.

[235] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "Adversarial attacks and defences: A survey," *arXiv preprint arXiv:1810.00069*, 2018, doi: 10.48550/arXiv.1810.00069.

[236] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, doi: 10.1109/SP.2019.00065.

[237] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," 2015, doi: 10.1145/2810103.2813677.

[238] Z. Wang, M. Song, Z. Zhang, Y. Song, Q. Wang, and H. Qi, "Beyond inferring class representatives: User-level privacy leakage from federated learning," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, doi: 10.1109/INFOCOM.2019.8737416.

[239] B. Kuang, A. Fu, S. Yu, G. Yang, M. Su, and Y. Zhang, "Esdra: An efficient and secure distributed remote attestation scheme for iot swarms," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8372–8383, 2019, doi: 10.1109/JIOT.2019.2917223.

[240] A. Fu, Z. Chen, Y. Mu, W. Susilo, Y. Sun, and J. Wu, "Cloud-based outsourcing for enabling privacy-preserving large-scale non-negative matrix factorization," *IEEE Transactions on Services Computing*, vol. 15, no. 1, pp. 266–278, 2022, doi: 10.1109/TSC.2019.2937484.

[241] W. Zheng, R. A. Popa, J. E. Gonzalez, and I. Stoica, "Helen: Maliciously secure coopetitive learning for linear models," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, doi: 10.1109/SP.2019.00045.

[242] X. Ma, F. Zhang, X. Chen, and J. Shen, "Privacy preserving multi-party computation delegation for deep learning in cloud computing," *Information Sciences*, vol. 459, pp. 103–116, 2018, doi: 10.1016/j.ins.2018.05.005.

[243] X. Zhang, A. Fu, H. Wang, C. Zhou, and Z. Chen, "A privacy-preserving and verifiable federated learning scheme," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, doi: 10.1109/ICC40277.2020.9148628.

[244] B. Jiang, J. Li, H. Wang, and H. Song, "Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1136–1144, 2023, doi: 10.1109/TII.2021.3131175.

[245] T. Ryffel, A. Trask, M. Dahl, B. Wagner, J. V. Mancuso, D. Rueckert, and J. Passerat-Palmbach, "A generic framework for privacy preserving deep learning," *ArXiv preprint arXiv:1811.04017*, vol. abs/1811.04017, 2018, doi: 10.48550/arXiv.1811.04017.

[246] A. Asad, M. M. Fouda, Z. M. Fadlullah, M. I. Ibrahem, and N. Nasser, "Moreau envelopes-based personalized asynchronous federated learning: Improving practicality in network edge intelligence," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, doi: 10.1109/GLOBECOM54140.2023.10437327.

[247] P. R. Ovi and A. Gangopadhyay, "A comprehensive study of gradient inversion attacks in federated learning and baseline defense strategies," in *2023 57th Annual Conference on Information Sciences and Systems (CISS)*, 2023, doi: 10.1109/CISS56502.2023.10089719.

[248] H. Yin, A. Mallya, A. Vahdat, J. M. Alvarez, J. Kautz, and P. Molchanov, "See through gradients: Image batch recovery via gradinversion," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021, doi: 10.1109/CVPR46437.2021.01607.

[249] W. Wei, L. Liu, M. Loper, K. H. Chow, M. E. Gursoy, S. Truex, and Y. Wu, "A framework for evaluating gradient leakage attacks in federated learning," *CoRR*, vol. abs/2004.10397, 2020. [Online]. Available: https://arxiv.org/abs/2004.10397

[250] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in *Advances in Neural Information Processing Systems*, H. Wallach, H. Larochelle, A. Beygelzimer, F. d'Alché-Buc, E. Fox, and R. Garnett, Eds., vol. 32. Curran Associates, Inc., 2019. [Online]. Available: https://proceedings.neurips.cc/paper_files/paper/2019/file/60a6c4002cc7b29142def8871531281a-Paper.pdf

[251] B. Zhao, K. R. Mopuri, and H. Bilen, "idlg: Improved deep leakage from gradients," *CoRR*, vol. abs/2001.02610, 2020. [Online]. Available: http://arxiv.org/abs/2001.02610

[252] W. Wei, L. Liu, Y. Wu, G. Su, and A. Iyengar, "Gradient-leakage resilient federated learning," in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*, 2021, doi: 10.1109/ICDCS51616.2021.00081. pp. 797–807.

[253] Y. Huang, S. Gupta, Z. Song, K. Li, and S. Arora, "Evaluating gradient inversion attacks and defenses in federated learning," in *Advances in Neural Information Processing Systems*, M. Ranzato, A. Beygelzimer, Y. Dauphin, P. Liang, and J. W. Vaughan, Eds., vol. 34. Curran Associates, Inc., 2021, pp. 7232–7241. [Online]. Available: https://proceedings.neurips.cc/paper_files/paper/2021/file/3b3fff6463464959dcd1b68d0320f781-Paper.pdf

[254] Y. Li, Y. Yu, W. Susilo, Z. Hong, and M. Guizani, "Security and privacy for edge intelligence in 5G and beyond networks: Challenges and solutions," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 63–69, 2021, doi: 10.1109/MWC.001.2000318.

[255] M. Usama, I. Ilahi, J. Qadir, R. Mitra, and M. K. Marina, "Examining machine learning for 5G and beyond through an adversarial lens," *IEEE Internet Computing*, vol. 25, no. 2, pp. 26–34, 2021, doi: 10.1109/MIC.2021.3049190.

[256] M. Humayun, N. Jhanjhi, M. Alruwaili, S. S. Amalathas, V. Balasubramanian, and B. Selvaraj, "Privacy protection and energy optimization for 5G-aided industrial internet of things," *IEEE Access*, vol. 8, pp. 183 665–183 677, 2020, doi: 10.1109/ACCESS.2020.3028764.

[257] S. Liu and Z. Yan, "Efficient privacy protection protocols for 5G-enabled positioning in industrial IoT," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18 527–18 538, 2022, doi: 10.1109/JIOT.2022.3161148.

[258] E. Kline, S. Ravi, D. Cousins, and S. Rv, "Securing 5G slices using homomorphic encryption," in *2022 IEEE Wireless*

Communications and Networking Conference (WCNC), 2022, doi: 10.1109/WCNC51071.2022.9771895.

[259] A. Names, "FHEVM Whitepaper," GitHub repository: https://github.com/zama-ai/fhevm/blob/main/fhevm-whitepaper.pdf, 2023, accessed: 2024-02-17.

[260] European Telecommunications Standards Institute, "Zsm - zero touch network & service management," https://www.etsi.org/technologies/zero-touch-network-service-management, 2024, accessed: 2024-02-19.

[261] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: Opportunities and challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[262] S. Jayasinghe, Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Federated learning based anomaly detection as an enabler for securing network and service management automation in beyond 5G networks," in *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2022, doi: 10.1109/EuCNC/6GSummit54941.2022.9815754.

[263] G. T. Maale, G. Sun, N. A. E. Kuadey, T. Kwantwi, R. Ou, and G. Liu, "DeepFESL: Deep federated echo state learning-based proactive content caching in UAV-assisted networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 12 208–12 220, 2023, doi: 10.1109/TVT.2023.3268541.

[264] W. Yang and Z. Liu, "Efficient vehicular edge computing: A novel approach with asynchronous federated and deep reinforcement learning for content caching in VEC," *IEEE Access*, vol. 12, pp. 13 196–13 212, 2024, doi: 10.1109/ACCESS.2024.3355462.

[265] D. Li, H. Zhang, T. Li, H. Ding, and D. Yuan, "Community detection and attention-weighted federated learning based proactive edge caching for D2D-assisted wireless networks," *IEEE Transactions on Wireless Communications*, vol. 22, no. 11, pp. 7287–7303, 2023, doi: 10.1109/TWC.2023.3249756.

[266] W. Zhu, J. Chen, L. You, J. Chen, X. Cheng, K. Guo, C. Liao, and X. Huang, "A federated-CNN based proactive caching algorithm for vCDN system," in *2022 Asia Conference on Algorithms, Computing and Machine Learning (CACML)*, 2022, doi: 10.1109/CACML55074.2022.00017.

[267] S. Oualil, R. Oucheikh, M. El Kamili, and I. Berrada, "A personalized learning scheme for internet of vehicles caching," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, doi: 10.1109/GLOBECOM46510.2021.9685308.

[268] X. Huang, C. Yu, F. Wang, and Q. Chen, "Hierarchical federated learning for collaborative caching in fog computing," in *2023 International Conference on Wireless Communications and Signal Processing (WCSP)*, 2023, doi: 10.1109/WCSP58612.2023.10404642.

[269] W. Ye, C. Qian, X. An, X. Yan, and G. Carle, "Advancing federated learning in 6G: A trusted architecture with graph-based analysis," *arXiv preprint arXiv:2309.05525v3*, 2023, doi: 10.48550/arXiv.2309.05525.

[270] Y. E. Sagduyu, T. Erpek, A. Yener, and S. Ulukus, "Joint sensing and semantic communications with multi-task deep learning," *arXiv preprint arXiv:2311.05017*, 2023, doi: 10.48550/arXiv.2311.05017.

[271] P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, Z. Laaroussi, and S. Köpsell, "Addressing privacy concerns in joint communication and sensing for 6g networks: Challenges and prospects," *arXiv preprint arXiv:2405.01742*, 2024, doi: 10.48550/arXiv.2405.01742.

[272] Martins, J. P. Vilela, and M. Gomes, "Poster: Privacy-preserving joint communication and sensing," in *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2023, doi: 10.1109/WoWMoM57956.2023.00053. pp. 329–331.

[273] Y. Yang, P. Hu, J. Shen, H. Cheng, Z. An, and X. Liu, "Privacy-preserving human activity sensing: A survey," *High-Confidence Computing*, vol. 4, no. 1, article no. 100204, 2024, doi: 10.1016/j.hcc.2024.100204.

[274] A. Krizhevsky and G. Hinton, "Learning multiple layers of features from tiny images," University of Toronto, Toronto, Canada, Tech. Rep., 2009, technical Report. [Online]. Available: https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf

[275] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, and I. Ahmad, "Machine learning threatens 5G security," *IEEE Access*, vol. 8, pp. 190 822–190 842, 2020, doi: 10.1109/ACCESS.2020.3031966.

[276] A. Almaatouq, F. Prieto-Castrillo, and A. Pentland, "Mobile communication signatures of unemployment," in *SocInfo 2016: Social Informatics*, 2016, doi: 10.1007/978-3-319-47880-7_25.

[277] J. W. Berry, A. Ganti, K. Goss, C. D. Mayer, U. Onunkwo, C. A. Phillips, J. Saia, and T. M. Shead, "Adapting secure multiparty computation to support machine learning in radio frequency sensor networks," U.S. Department of Energy Office of Scientific and Technical Information, Tech. Rep., 2021, doi: 10.2172/1842271.

[278] R. Bocu, D. Bocu, and M. Iavich, "An extended review concerning the relevance of deep learning and privacy techniques for data-driven soft sensors," *Sensors*, vol. 23, no. 1, article no. 294, 2023, doi: 10.3390/s23010294.

[279] H. Li, S. Li, and G. Min, "Lightweight privacy-preserving predictive maintenance in 6G enabled IIoT," *Journal of Industrial Information Integration*, vol. 39, article no. 100548, 2024, doi: 10.1016/j.jii.2023.100548.

[280] Y. Wang, X. Liang, X. Hei, W. Ji, and L. Zhu, "Deep learning data privacy protection based on homomorphic encryption in AIoT," *Mobile Information Systems*, vol. 2021, article no. 5510857, Jun 2021, doi: 10.1155/2021/5510857.

[281] J. Jiang, G. Han, L. liu, L. Shu, and M. Guizani, "Outlier detection approaches based on machine learning in the internet-of-things," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 53–59, 2020, doi: 10.1109/MWC.001.1900410.

[282] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018, doi: 10.1109/COMST.2018.2844341.

[283] X. Liu, H. Li, G. Xu, S. Liu, Z. Liu, and R. Lu, "Padl: Privacy-aware and asynchronous deep learning for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6955–6969, 2020, doi: 10.1109/JIOT.2020.2981379.

[284] W. Du, A. Li, P. Zhou, Z. Xu, X. Wang, H. Jiang, and D. Wu, "Approximate to be great: Communication efficient and privacy-preserving large-scale distributed deep learning in internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 678–11 692, 2020, doi: 10.1109/JIOT.2020.2999594.

[285] N. Bugshan, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and S. Badsha, "Toward trustworthy and privacy-preserving federated deep learning service framework for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1535–1547, 2023, doi: 10.1109/TII.2022.3209200.

[286] L. Lyu, J. C. Bezdek, J. Jin, and Y. Yang, "FORESEEN: Towards differentially private deep inference for intelligent internet of things," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 10, pp. 2418–2429, 2020, doi: 10.1109/JSAC.2020.3000374.

[287] L. Yin, J. Feng, H. Xun, Z. Sun, and X. Cheng, "A privacy-preserving federated learning for multiparty data sharing in social iots," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2706–2718, 2021, doi: 10.1109/TNSE.2021.3074185.

[288] G. Gad, E. Gad, Z. M. Fadlullah, M. M. Fouda, and N. Kato, "Communication-efficient and privacy-preserving federated learning via joint knowledge distillation and differential privacy in bandwidth-constrained networks," *IEEE Transactions on Vehicular Technology*, early access, doi: 10.1109/TVT.2024.3423718.

[289] G. Gad, Z. M. Fadlullah, M. M. Fouda, M. I. Ibrahem, and N. Kato, "Federated learning with selective knowledge distillation over bandwidth-constrained wireless networks," in *ICC 2024 - IEEE International Conference on Communications*, 2024, doi: 10.1109/ICC51166.2024.10622906.

[290] G. Gad, A. Farrag, A. Aboulfotouh, K. Bedda, Z. M. Fadlullah, and M. M. Fouda, "Joint self-organizing maps and knowledge-distillation-based communication-efficient federated learning for resource-constrained UAV-IoT systems," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15 504–15 522, 2024, doi: 10.1109/JIOT.2023.3349295.

[291] G. Gad, Z. M. Fadlullah, M. M. Fouda, M. I. Ibrahem, and N. Nasser, "Joint knowledge distillation and local differential privacy for communication-efficient federated learning in heterogeneous systems," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, doi: 10.1109/GLOBECOM54140.2023.10437358. pp. 2051–2056.

[292] L. Deng, "The MNIST database of handwritten digit images for machine learning research [best of the web]," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 141–142, 2012, doi: 10.1109/MSP.2012.2211477.

[293] W. Wu, Q. Qi, and X. Yu, "Deep learning-based data privacy protection in software-defined industrial networking," *Computers and Electrical Engineering*, vol. 106, p. 108578, 2023, doi: 10.1016/j.compeleceng.2023.108578.

[294] X. Guo, H. Xian, T. Feng, Y. Jiang, D. Zhang, and J. Fang, "An intelligent zero trust secure framework for software defined networking," *PeerJ Computer Science*, vol. 9, article no. e1674, 2023, doi: 10.7717/peerj-cs.1674.

[295] G. J. Mendis, Y. Wu, J. Wei, M. Sabounchi, and R. Roche, "A blockchain-powered decentralized and secure computing paradigm," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 2201–2222, 2021, doi: 10.1109/TETC.2020.2983007.

[296] X. Ma, L. Liao, Z. Li, R. X. Lai, and M. Zhang, "Applying federated learning in software-defined networks: A survey," *Symmetry*, vol. 14, no. 2, article no. 195, 2022, doi: 10.3390/sym14020195.

[297] N. Chen, M. Wang, N. Zhang, and X. Shen, "Energy and information management of electric vehicular network: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 967–997, 2020, doi: 10.1109/COMST.2020.2982118.

[298] R. A. Agyapong, M. Nabil, A.-R. Nuhu, M. I. Rasul, and A. Homaifar, "Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning," in *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2021, doi: 10.1109/SSCI50451.2021.9659972.

[299] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1243–1274, 2019, doi: 10.1109/COMST.2018.2888904.

[300] A. R. Sani, M. U. Hassan, and J. Chen, "Privacy preserving machine learning for electric vehicles: A survey," *ArXiv*, vol. abs/2205.08462, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:248834382

[301] M. Rigaki and S. Garcia, "A survey of privacy attacks in machine learning," *ACM Computing Surveys*, vol. 56, no. 4, article no. 101, 2024, doi: 10.1145/3624010.

[302] H. Talat, T. Nomani, M. Mohsin, and S. Sattar, "A survey on location privacy techniques deployed in vehicular networks," in *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2019, doi: 10.1109/IBCAST.2019.8667248.

[303] K. Tan, D. Bremner, J. Le Kernec, L. Zhang, and M. Imran, "Machine learning in vehicular networking: An overview," *Digital Communications and Networks*, vol. 8, no. 1, pp. 18–24, 2022, doi: https://doi.org/10.1016/j.dcan.2021.10.007.

[304] M. M. Badr, M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, and W. Alasmary, "Detection of false-reading attacks in smart grid net-metering system," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1386–1401, 2022, doi: 10.1109/JIOT.2021.3087580.

[305] "Irish social science data archive," http://www.ucd.ie/issda/data/commissionforenergyregulationcer/, accessed: Mar. 2020.

[306] M. Wen, R. Xie, K. Lu, L. Wang, and K. Zhang, "FedDetect: a novel privacy-preserving federated learning framework for energy theft detection in smart grid," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6069–6080, 2022, doi: 10.1109/JIOT.2021.3110784.

[307] V. B. Krishna, C. A. Gunter, and W. H. Sanders, "Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 790–805, 2018, doi: 10.1109/JSTSP.2018.2833749.

[308] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3428–3437, 2020, doi: 10.1109/TSG.2020.2973681.

[309] Cloud Security Alliance, "Top threats to cloud computing: Egregious eleven," Cloud Security Alliance Press Release, Aug. 2019, available online at https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven.

[310] B. Pulido-Gaytan, A. Tchernykh, J. Cortés-Mendoza *et al.*, "Privacy-preserving neural networks with homomorphic encryption: Challenges and opportunities," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 1666–1691, 2021, doi: 10.1007/s12083-021-01076-8.

[311] R. Gupta and A. K. Singh, "Privacy-preserving cloud data model based on differential approach," in *2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T)*, 2022, doi: 10.1109/ICPC2T53885.2022.9776691.

[312] G. Bao and P. Guo, "Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges," *Journal of Cloud Computing*, vol. 11, article no. 94, 2022, doi: 10.1186/s13677-022-00377-4.

[313] J. Hrzich, G. Basra, and T. Halabi, "Experimental evaluation of homomorphic encryption in cloud and edge machine learning," in *2022 14th International Conference on Knowledge and Systems Engineering (KSE)*, 2022, doi: 10.1109/KSE56063.2022.9953624.

[314] L. B. Pulido-Gaytan, A. Tchernykh, J. M. Cortés-Mendoza, M. Babenko, and G. Radchenko, "A survey on privacy-preserving machine learning with fully homomorphic encryption," in *CARLA 2020: High Performance Computing*, 2021, doi: 10.1007/978-3-030-68035-0_9.

[315] M. S. Rahman, I. Khalil, M. Atiquzzaman, and X. Yi, "Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption," *Engineering Applications of Artificial Intelligence*, vol. 94, article no. 103737, 2020, doi: 10.1016/j.engappai.2020.103737.

[316] R. Han, D. Li, J. Ouyang, C. H. Liu, G. Wang, D. Wu, and L. Y. Chen, "Accurate differentially private deep learning on the edge," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 9, pp. 2231–2247, 2021, doi: 10.1109/TPDS.2021.3064345.

[317] G. Ahmadi-Assalemi, H. Al-Khateeb, and A. Aggoun, "Privacy-enhancing technologies in the design of digital twins for smart cities," *Network Security*, vol. 2022, 07 2022, doi: 10.12968/S1353-4858(22)70046-3.

[318] R. Alisic, "Defense of cyber-physical systems against learning-based attackers," PhD dissertation, KTH Royal Institute of Technology, Stockholm, 2023.

[319] Q. Lou and L. Jiang, "HEMET: A homomorphic-encryption-friendly privacy-preserving mobile neural network architecture," *arXiv preprint arXiv:2106.00038*, 2021, doi: 10.48550/arXiv.2106.00038.

[320] A. Brutzkus, O. Elisha, and R. Gilad-Bachrach, "Low latency privacy preserving inference," *arXiv preprint arXiv:1812.10659*, 2018, doi: 10.48550/arXiv.1812.10659.

[321] S. S. Rodríguez, L. Wang, J. Zhao, R. Mortier, and H. Haddadi, "Personal model training under privacy constraints," *arXiv preprint arXiv:1703.00380*, 2017, doi: 10.48550/arXiv.1703.00380.

[322] S. El-Gendy, M. Elsayed, A. Jurcut, and M. Azer, "Privacy preservation using machine learning in the internet of things," *Mathematics*, vol. 11, no. 16, article no. 3477, 2023, doi: 10.3390/math11163477.

[323] Archon Secure, "Post-quantum cryptography guide," https://www.archonsecure.com/post-quantum-cryptography-guide, 2023, accessed: 2024-09-29.

[324] W. M. Watkins, S.-Y. C. Chen, and S. Yoo, "Quantum machine learning with differential privacy," *Scientific Reports*, vol. 13, article no. 2453, 2023, doi: 10.1038/s41598-022-24082-z.

[325] R. Shi and Y. Li, "Privacy-preserving quantum protocol for finding the maximum value," *EPJ Quantum Technology*, vol. 9, no. 13, 2022, doi: 10.1140/epjqt/s40507-022-00132-3.

[326] A. Parimala and Y. Vijayalata, "Privacy and data control on social networks using deep learning," in *2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, 2022, doi: 10.1109/ICCCMLA56841.2022.9989244.

[327] R. Aljably, Y. Tian, and M. Al-Rodhaan, "Preserving privacy in multimedia social networks using machine learning anomaly detection," *Security and Communication Networks*, vol. 2020, article no. 5874935, 2020, doi: 10.1155/2020/5874935.

[328] 6G Smart Networks and Services Infrastructure Association, "Data protection declaration," https://6g-ia.eu/data-protection-declaration/, accessed: 2024-03-10.

[329] Y. Tan, G. Long, L. LIU, T. Zhou, Q. Lu, J. Jiang, and C. Zhang, "Fedproto: Federated prototype learning across heterogeneous clients," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 8, pp. 8432–8440, Jun. 2022, doi: 10.1609/aaai.v36i8.20819.

[330] A. Shamsian, A. Navon, E. Fetaya, and G. Chechik, "Personalized federated learning using hypernetworks," in *Proceedings of the 38th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, M. Meila and T. Zhang, Eds., vol. 139. PMLR, 18–24 Jul 2021, pp. 9489–9502. [Online]. Available: https://proceedings.mlr.press/v139/shamsian21a.html

[331] H. Huang and J. Kong, "Personalized federated learning based on knowledge distillation using teacher assistants," in *2024 5th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, 2024, doi: 10.1109/AINIT61980.2024.10581694. pp. 521–525.

[332] X. Gong, A. Sharma, S. Karanam, Z. Wu, T. Chen, D. Doermann, and A. Innanje, "Preserving privacy in federated learning with ensemble cross-domain knowledge distillation," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 11, pp. 11 891–11 899, Jun. 2022, doi: 10.1609/aaai.v36i11.21446.

[333] Q. Wang, S. Chen, and M. Wu, "Communication-efficient personalized federated learning with privacy-preserving," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2374–2388, 2024, doi: 10.1109/TNSM.2023.3323129.

[334] Z. M. Fadlullah, B. Mao, and N. Kato, "Balancing qos and security in the edge: Existing practices, challenges, and 6G opportunities with machine learning," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2419–2448, 2022, doi: 10.1109/COMST.2022.3191697.
[335] Z. Sun, L. Yin, C. Li, W. Zhang, A. Li, and Z. Tian, "The QoS and privacy trade-off of adversarial deep learning: An evolutionary game approach," *Computers & Security*, vol. 96, p. 101876, 2020, doi: 10.1016/j.cose.2020.101876.
[336] S. A. Osia, A. Shahin Shamsabadi, S. Sajadmanesh, A. Taheri, K. Katevas, H. R. Rabiee, N. D. Lane, and H. Haddadi, "A hybrid deep learning architecture for privacy-preserving mobile analytics," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4505–4518, 2020, doi: 10.1109/jiot.2020.2967734.
[337] A. Yazdinejad, A. Dehghantanha, G. Srivastava, H. Karimipour, and R. M. Parizi, "Hybrid privacy preserving federated learning against irregular users in next-generation internet of things," *Journal of Systems Architecture*, vol. 148, article no. 103088, 2024, doi: 10.1016/j.sysarc.2024.103088.
[338] M. Wu, G. Cheng, P. Li, R. Yu, Y. Wu, M. Pan, and R. Lu, "Split learning with differential privacy for integrated terrestrial and non-terrestrial networks," *IEEE Wireless Communications*, vol. 31, no. 3, pp. 177–184, 2024, doi: 10.1109/MWC.015.2200462.
[339] W. Lan, K. Chen, Y. Li, J. Cao, and Y. Sahni, "Deep reinforcement learning for privacy-preserving task offloading in integrated satellite-terrestrial networks," *IEEE Transactions on Mobile Computing*, vol. 23, no. 10, pp. 9678–9691, 2024, doi: 10.1109/tmc.2024.3366928.
[340] X. Wang, Y. Gao, G. Zhang, M. Guo, and K. Xu, "Security performance analysis for cell-free massive multiple-input multiple-output system with multi-antenna access points deployment in presence of active eavesdropping," *International Journal of Distributed Sensor Networks*, vol. 18, no. 8, 2022, doi: 10.1177/15501329221114535.
[341] J. Xu, X. Wang, P. Zhu, and X. You, "Privacy-preserving channel estimation in cell-free hybrid massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 20, no. 6, pp. 3815–3830, 2021, doi: 10.1109/TWC.2021.3053770.
[342] X. Costa-Pérez, V. Sciancalepore, L. Zanzi, and A. Albanese, *Blockchain for Mobile Networks*, 2024, pp. 185–213, doi: 10.1002/9781119781042.ch7.
[343] A. M. Hilal, J. S. Alzahrani, I. Abunadi, N. Nemri, F. N. Al-Wesabi, A. Motwakel, I. Yaseen, and A. S. Zamani, "Intelligent deep learning model for privacy preserving iiot on 6g environment," *Computers, Materials and Continua*, vol. 72, no. 1, pp. 333–348, 2022, doi: 10.32604/cmc.2022.024794.
[344] S. K.M., S. Nicolazzo, M. Arazzi, A. Nocera, R. R. K.A., V. P., and M. Conti, "Privacy-preserving in blockchain-based federated learning systems," *Computer Communications*, vol. 222, pp. 38–67, 2024, doi: 10.1016/j.comcom.2024.04.024.
[345] S. Muralidhara and B. A. Usha, "Review of blockchain security and privacy," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, 2021, doi: 10.1109/ICCMC51019.2021.9418424.
[346] S. Bharati and P. Podder, "Machine and deep learning for IoT security and privacy: Applications, challenges, and future directions," *Security and Communication Networks*, vol. 2022, no. 1, article no. 8951961, 2022, doi: 10.1155/2022/8951961.

Mostafa M. Fouda (Senior Member, IEEE) received the B.S. degree and the M.S. degree in Electrical Engineering from Benha University, Egypt, in 2002 and 2007, respectively, and the Ph.D. degree in Information Sciences from Tohoku University, Japan, in 2011. He is an Associate Professor with the Department of Electrical and Computer Engineering at Idaho State University, ID, USA. He also holds the position of a Full Professor at Benha University. He has (co)authored more than 280 technical publications. His current research focuses on cybersecurity, communication networks, signal processing, wireless mobile communications, smart healthcare, smart grids, AI, and IoT. He serves on the editorial board of IEEE Transactions on Vehicular Technology (TVT), IEEE Internet of Things Journal (IoT-J), and IEEE Access. He has received several research grants, including NSF Japan-U.S. Network Opportunity 3 (JUNO3).

Zubair Md Fadlullah (Senior Member, IEEE) is currently an Associate Professor in the Department of Computer Science at the University of Western Ontario. He was previously an Associate Professor at Lakehead University, Canada, and Tohoku University, Japan. He also held the position of Smart Health Technology Research Chair at the Thunder Bay Regional Health Research Institute (TBRHRI) from 2019 to 2022. His research spans data collection, beyond 5G communication networks, and computing for cyber-physical systems, with a focus on performance quality, reliability, security, and privacy. He has a particular interest in designing lightweight AI-driven solutions for resource-constrained communication nodes, such as Internet of Things devices. He received several best paper awards and several research awards for his excellent research contributions in networking areas. He was recognized as a Highly Cited Researcher in Computer Science in 2021 and 2022.

Mohamed I. Ibrahem (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering (electronics and communications) from Benha University, Cairo, Egypt, in 2014 and 2018, respectively, and the Ph.D. degree in electrical and computer engineering from Tennessee Technological University, USA, in 2021. He is currently an Assistant Professor with the School of Computer and Cyber Sciences, Augusta University, USA. He also holds the position of Assistant Professor at Benha University. His research interests include machine learning, cryptography and network security, and privacy-preserving schemes for Cyber-Physical Systems and Internet of Things. He received the Eminence Award for the Doctor of Philosophy Best Paper from Tennessee Technological University, USA.

Nei Kato (Fellow, IEEE) is a Full Professor and the Dean with the Graduate School of Information Sciences. He has published more than 400 papers in prestigious peer-reviewed journals and conferences. He has been engaged in research on computer networking, wireless mobile communications, satellite communications, ad hoc and sensor and mesh networks, UAV networks, smart grid, AI, IoT, big data, and pattern recognition. He has been acclaimed with many best paper awards and a long list of other awards and recognition. He was the Vice-President (Member and Global Activities) of IEEE Communications Society from 2018 to 2021, the Editor-in-Chief of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2017 to 2021 and IEEE Network Magazine from 2015 to 2017. He is a Fellow of The Engineering Academy of Japan and IEICE.