Deep Learning for Privacy Preservation in Autonomous Moving Platforms Enhanced 5G Heterogeneous Networks

Yulei Wu, *Senior Member, IEEE,* Yuxiang Ma, Hong-Ning Dai, *Senior Member, IEEE,* and Hao Wang, *Member, IEEE*

***Abstract*—5G heterogeneous networks have become a promising platform to connect a growing number of Internet-of-Things (IoT) devices and accommodate a wide variety of vertical services. IoT has not been limited to traditional sensing systems since the introduction of 5G, but also includes a range of autonomous moving platforms, e.g., autonomous flying vehicles, autonomous underwater vehicles, autonomous surface vehicles as well as autonomous land vehicles. These platforms can be used as an effective means to connect air, space, ground, and sea mobile networks for providing a wider diversity of Internet services. Deep learning has been widely used to extract useful information from network big data for enhancing network quality-of-service and user quality-of-experience. Privacy preservation for user and network data is a burning concern in 5G heterogeneous networks due to various attacks in this environment. In this paper, we conduct an in-depth investigation on how deep learning can cope with privacy preservation issues in 5G heterogeneous networks, in terms of heterogeneous radio access networks (RANs), beyond-RAN networks, and end-to-end network slices, followed by a set of key research challenges and open issues that aim to guide future research.**

***Index Terms*—Deep learning, 5G, Heterogeneous networks, Privacy Preservation, Network slicing.**

I. Introduction

According to a Statista report, by 2025, the number of connected Internet-of-Things (IoT) devices would be approximately 75.44 billion[1]. The IoT devices will be used to provide a wide variety of vertical services in the sectors of e.g., automotive, transportation, energy, city management, agriculture, and manufacturing [1], [2], [3]. Therefore, these devices have various connection demands e.g., in terms of different radio technologies [4]. These vertical services also have diversified Quality-of-Service (QoS) requirements, ranging from ultra-low latency to ultra-dense connectivity [5]. The fifth-generation (5G) mobile communication system has been widely recognised as a promising platform to connect IoT devices by using bandwidth spectrum of heterogeneous networks (HetNets) and provide accommodation to the vertical services [6].

Since the introduction of 5G, IoT has not been limited to traditional sensing systems, but also includes a wide variety of autonomous moving platforms (AMP), including autonomous flying vehicles (AFV), autonomous underwater vehicles (AUV), autonomous surface vehicles (ASV) as well as autonomous land vehicles (ALV) [7]. These AMPs are usually designed for specific tasks. For example, some AFVs are designed to deliver goods, while some are designed for monitoring [8]. AUVs and ASVs are robotic vehicles that are particularly designed for performing tasks under the sea and on the sea surface, respectively. ALVs have been designed to undertake tasks, ranging from mining and agriculture to bushfire fighting and defence. Different from before, the fast development of 5G can enable the communication between different types of AMPs, creating the so-called 5G-enabled AMPs. This in turn catalyses a wider range of emerging services that span over a unification of air, space, ground, and sea mobile networks, and can therefore further reshape the sectors of automotive, transportation, energy, city management, agriculture, and manufacturing.

The heterogeneity of the 5G infrastructure, in terms of heterogeneous radio access networks (RANs), heterogeneous beyond-RAN networks[2], such as cross-domain environment and heterogeneous connectivity technologies, and heterogeneous network slices, provides an advanced solution for fulfilling various QoS and Quality-of-Experience (QoE) requirements of many emerging services [9]. The growing volume of data generated by the huge amount of connected IoT devices over air, space, ground, and sea mobile networks, results in an extra burden on the 5G infrastructure to maintain QoS and QoE requirements. Deep learning (DL) has been widely used to extract useful information from network big data to enhance network QoS and user QoE [10]. Due to the heterogeneous nature of 5G infrastructure, various network providers along with different parts of networks, and different owners of diversified IoT devices, as well as the related privacy preservation concerns, network and service data are not always fully available for network management and business operations [11]. The network and service would be better managed

This work was partially supported by the Engineering and Physical Sciences Research Council of United Kingdom under Grant No. EP/R030863/1

Y. Wu is with the College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter, EX4 4QF, UK e-mail: y.l.wu@exeter.ac.uk

Y. Ma is with the School of Computer and Information Engineering, Henan University, Kaifeng, 475004, China. e-mail: yma@henu.edu.cn.

H.-N. Dai is with the Faculty of Information Technology, Macau University of Science and Technology, Macau. email: hndai@ieee.org

H. Wang is with the Department of Computer Science, Norwegian University of Science and Technology, Gjøvik, Norway email: hawa@ntnu.no

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] The network initiates from the point where a packet leaves the RAN, until the point where the packet reaches the destination. Beyond-RAN may include core networks, industrial networks, private networks, and so on.

TABLE I
POTENTIAL EXAMPLES / ALIAS OF DIFFERENT TYPES OF AUTONOMOUS MOVING PLATFORMS

Types of AMPs	Potential examples / alias
Autonomous flying vehicles	Unmanned aerial vehicles, self-flying cars, autonomous flying taxi, autonomous flying vehicles transporting commuters
Autonomous underwater vehicles	Unmanned underwater vehicles, underwater gliders, bionic autonomous underwater vehicles
Autonomous surface vehicles	Automated ships, drone ships, wave gliders, autonomous boat, autonomous cargo ship, saildrone
Autonomous land vehicles	Self-driving cars, unmanned ground vehicle, agricultural robot

if more data could be available by using effective techniques for protecting privacy.

Privacy preservation is a burning issue in 5G HetNets since many services are expected to be running on top of them [12], [13], [14], [15]. The main concerns, in 5G heterogeneous RANs, include privacy leakage in radio spectrum sharing, in-network access, and in edge computing. In beyond-RAN networks, privacy concerns are more about privacy preservation in shared resource infrastructure, under cross-domain environment, and for heterogeneous connectivity technologies. Network slicing is a unique feature of 5G networks, consisting of heterogeneous shared resources from underlying physical infrastructure. The key privacy concerns for network slicing include privacy leakage of resource scheduling in slices, slice orchestration, and communication between devices and network slices. In addition to the traditional IoTs that cause the above privacy issues, 5G-enabled AMP, while providing benefits to a number of related businesses, have produced growing privacy concerns [16], [17], [18].

In this paper, we first give a systematic introduction of 5G-enabled AMPs in Section II, along with how they amplify the privacy issues in 5G HetNets. After that, in Sections III - V we elaborate on how DL can cope with privacy preservation issues in 5G HetNets. Then, we outline a set of challenging and open issues for future research in this area in Section VI. Finally, Section VII concludes this work.

II. 5G-ENABLED AUTONOMOUS MOVING PLATFORMS

The AMP has gained significant attention since the introduction of 5G [7]. It includes AFVs, AUVs, ASVs, and ALVs. They are essentially self-propelled, unmanned, untethered robots that are capable of carrying out activities and performing tasks with little or no human supervision. Recall that AUVs usually operate under the sea, e.g., unmanned underwater vehicles, while ASVs work on the sea surface, such as automated ships. ALVs usually run on the ground, where self-driving cars are typical examples. AFVs operate in the air or space, such as unmanned aerial vehicles and unmanned spacecraft. Table I shows a list of typical examples for each type of AMPs.

Before the era of 5G, each type of AMPs essentially works in isolation. For example, an unmanned underwater vehicle may not be able to communicate with an unmanned aerial vehicle to work on a task in a collaborative manner. 5G and B5G/6G provide a heterogeneous infrastructure over the air, space, ground, and sea mobile networks, to provide not only true ubiquitous communications, but also the support of a wide variety of services over this infrastructure [19]. To enable the ubiquitous communications, AMPs are now equipped with 5G-capable modules, creating 5G-enabled AMPs[3]. The introduction of 5G and B5G/6G, together with the advances in artificial intelligence (e.g., DL) and computing paradigms (e.g., edge computing), revolutionises the way how an AMP works. One type of 5G-enabled AMPs can readily work with another to complete a task in a collaborative way. This in turn enables a wide spectrum of services for the air, space, ground, and sea mobile networks, under the support of 5G/B5G and 6G HetNets.

There are two roles of 5G-enabled AMPs. One is serving as part of the infrastructure of 5G HetNets. For example, an unmanned aerial vehicle can be mounted with a lightweight base station to become a moving 5G base station. This can be used in certain areas and circumstances, e.g., rural areas and bushfire scenes, to quickly establish a communication environment. The other role is acting as 5G users. For example, a self-driving car equipped with 5G modules, can communicate with other devices through 5G HetNet infrastructure. This includes offloading computation tasks to edge computing nodes, exchanging data with roadside vehicle-to-infrastructure facilities, etc.

Fig. 1 shows typical example services in this horizon. In this example, there are self-driving cars operating on the roads, self-driving firefighting vehicles working on bushfire fighting, unmanned underwater vehicles and unmanned surface vehicles carrying out their duties on deep-sea exploration, unmanned aerial vehicles providing necessary computing and communications facilities and carrying goods, and satellites providing communication facilitates. Let us consider a rural area, if a bushfire occurs around the road connecting villages, self-driving cars ought to be alerted, through satellite communications, and alternative routes shall be calculated with the help of edge computing provided by unmanned aerial vehicles. Unmanned surface vehicles can be communicated by self-driving firefighting vehicles, through satellite communications, for requesting water to fight the bushfire in emergencies. Unmanned surface vehicles can decide whether to accept the request considering their on-going deep-sea exploration jobs, through local computing or nearby edge computing provided by unmanned aerial vehicles. If they decide to accept the request, unmanned aerial vehicles that have been designed for that purpose, can be used to deliver seawater to help fight bushfire.

Different from ordinary mobile devices, AMPs have some characteristics that need to be considered when we design and

[3]With the evolution of mobile communication systems, 6G-enabled AMPs would be present in the future.

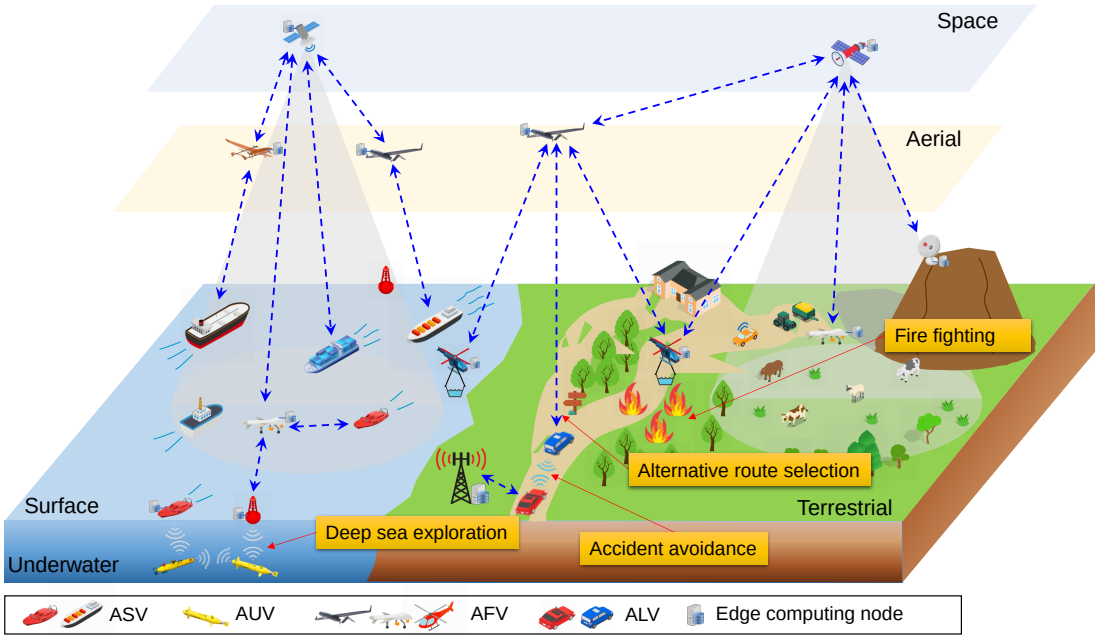

Fig. 1. The 5G-enabled autonomous moving platforms.

deploy them. Specifically, AMPs should have the ability to make decisions independently, and perform a series of actions including route planning, target detection, obstacle avoidance, etc [7]. More importantly, AMPs need to move autonomously. Therefore, compared to ordinary mobile devices (e.g., mobile phones, laptops), AMPs would consume more energy and have higher requirements for continuous energy supply. The use of solar energy to provide energy for AMPs requires certain weather conditions. The use of fuel to provide power and electricity requires timely refueling. In recent years, more devices use batteries to provide energy. No matter which energy supply method is used, AMPs need to save as much energy as possible while they are working.

Thanks to the low latency and high bandwidth features of 5G networks, AMPs can appropriately reduce the allocation of computing and storage resources [20], [21], [22]. Part of the computing and storage requirements of AMPs can be completed in edge computing and/or remote data centers, and AMPs perform corresponding operations based on the returned results. This working mode helps reduce the weight of AMPs and reduce energy consumption [23].

5G-enabled AMPs cause rapid growth of data pouring into the 5G HetNet infrastructure. Recall that before 5G, each type of AMPs is working in isolation, i.e., the data generated by a type of AMPs, e.g., AFV, stay in the system of that type of AMPs, or more accurately in the system of applications carried out by that type of AMPs. Since the introduction of 5G, different types of AMPs can communicate and exchange data with each other. On the one hand, this can inevitably enhance the QoS provided by each type of AMPs. On the other hand, this enables orders of magnitude more data traversing over 5G HetNets. Although causing additional burdens on network infrastructure, the significant growth of data can enable better service provisions. Whilst the fast development of machine learning, especially DL, can help with extracting useful information from massive data [24], [25], [26], privacy preservation has become a burning issue [27], [28]. In what follows, we will elaborate on how to overcome this issue in 5G HetNets.

III. Privacy Preservation in 5G Heterogeneous Radio Access Networks

As an important component in 5G HetNets, 5G RAN consists of a wide diversity of evolved NodeBs (eNBs or base stations), AMPs, user equipment (UE), and IoT devices, which generate massive wireless data. Data analytics on 5G RAN data can extract valuable information, which is beneficial for mobile network operators (MNOs) to identify the performance bottleneck, detect malicious behaviours, improve user QoE, optimise network operation, and reduce the operational cost [29], [30]. However, the benefits brought by 5G RAN data are also accompanied by privacy and security vulnerabilities as illustrated in the following aspects (as shown in Fig. 2):

- *Privacy leakage in radio spectrum sharing.* Radio spectrum is becoming a precious resource especially in 5G RAN which requires a large portion of the radio spectrum to fulfill the increased throughput demands. It is a necessity to enforce efficient spectrum sharing and management in 5G RAN. However, the widely-adopted approaches including either cooperative spectrum sensing [31] or database-driven spectrum access [32] inevitably lead to potential privacy exposure of legitimate primary users (PUs) and secondary users (SUs) during the spectrum data sharing process [33].
- *Privacy leakage in network access.* Due to the openness of wireless media, network complexity, and the diversity of UEs, 5G RAN is susceptible to various malicious attacks such as eavesdropping [34], identification (ID)

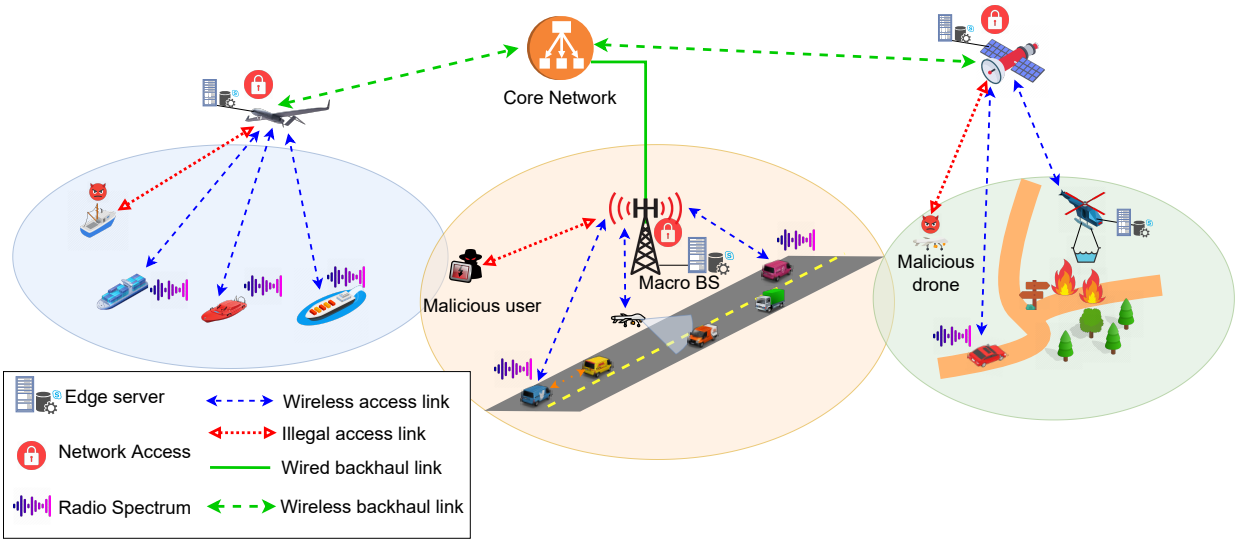

Fig. 2. Privacy preservation in 5G heterogeneous RAN.

spoofing [35], distributed denial-of-service (DDoS) [36], and system intrusion [37]. Following these malicious attacks, user privacy-sensitive data can be stolen, misused, sold, and even falsified.

- *Privacy leakage in edge computing.* The integration of 5G HetNets with cloud computing and mobile edge computing (MEC) is serving as an enabling technology to cater for the growing demands of both communications and computations. MEC that serves as a complement for cloud computing, can potentially overcome the weakness of cloud computing by offloading computation-intensive tasks to edge servers (or nodes) which are usually deployed at eNBs, base stations, access points, and IoT gateways. However, data stored at MEC servers is also vulnerable to privacy leakage due to illegal access or malicious attacks [38], [39].

Thanks to the latest advances in DL, the above privacy and security vulnerabilities can be tackled. We next show how DL approaches can solve the above challenges in 5G heterogeneous RAN in the following aspects.

A. Deep learning approaches in privacy preservation in radio spectrum sharing

DL approaches can be used to protect the privacy of both PUs and SUs during the radio spectrum sharing process, where PUs and SUs can be any AMPs, UEs, or IoT devices. In particular, DL approaches can analyse footprints (i.e., records or clues) left by malicious users, consequently identifying malicious behaviours and making the corresponding countermeasures. For example, when malicious users spy upon the spectrum sharing of legitimate users (in database-driven radio spectrum access), they may leave query reports attached with timestamps in the spectrum database. However, it is challenging for conventional analytical methods based on either manual operations or statistics analysis to extract key information from massive query data. DL approaches including recurrent neural networks (RNNs) and its alternatives, such as long short-term memory (LSTM) and gated recurrent units (GRU) can be used to extract the key information from the time-series data and identify the malicious behaviors since DL approaches are beneficial to analyse massive data. Consequently, countermeasures (e.g., warning or banning malicious users) can be made.

Regarding cooperative spectrum sensing, spectrum bidding has often been leveraged to achieve dynamic spectrum sharing while both spectrum buyers and sellers are also facing potential privacy exposure during the spectrum auction procedure [40]. Therefore, sophisticated cryptographic mechanisms have been typically used to *anonymise* both spectrum buyers and sellers [41] while also posing the challenges in data analytics. The recent work [42] that can fasten the training process of deep neural networks on encrypted data is a potentially good solution to data analytics on encrypted spectrum data. Moreover, [43] presents an RNN approach to analyse the encrypted data.

Meanwhile, malicious users may send the falsified spectrum data to the central entity (a.k.a. the fusion centre), so as to confuse the fusion centre and interfere with the decision-making process [44]. For example, malicious users sending wrong spectrum availability information (i.e., absence or presence) to the fusion centre can lead to the poor spectrum usage [45]. DL approaches have the potential to address this emerging issue through analysing the activities of malicious users. No matter what kind of malicious behaviors, malicious users will inevitably leave some *footprints*, such as channel state information (CSI), locations, and received signal strength indicator (RSSI). The work [46] presents an end-to-end DL framework to collect, preprocess, and analyse spectrum data, as shown in Fig. 3. In addition, this article also shows that a CNN-based model can effectively analyse spectrum data with high accuracy. Moreover, the work [47] collected radio signals via the software-defined radio (SDR) devices. GRU neural networks were then used to analyse radio signals and demonstrated a high classification accuracy (more than 90% accuracy).

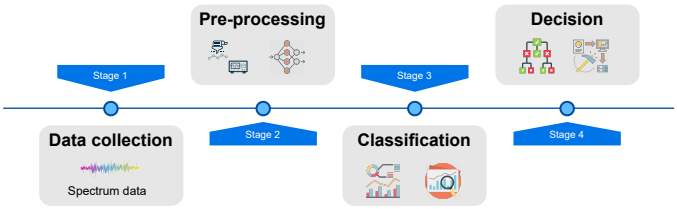

Fig. 3. Spectrum data processing pipeline.

The joint analysis of these footprints with falsified spectrum reports together can help us detect and identify malicious behaviors while it may require advanced DL methods to process the data from multiple sources. Multi-modal DL approaches [48] may be beneficial to address this issue. In particular, multi-modal DL algorithms need to learn from multi-modal data sources via deep auto-encoder as well as other techniques. Although multi-modal DL approaches demonstrate their effectiveness in analysing video, audio, and sensor data [48], [49], there are few studies on multi-modal spectrum data (including spectrum footprints and reports).

B. Deep learning approaches in privacy preservation in network access management

Regarding privacy preservation in network access management, DL approaches can be adopted to detect and identify malicious attacks through collecting and analysing the user activity data. Due to the network complexity and the device diversity (e.g., diverse AMPs, UEs, and IoT devices), conventional attack detection methods, e.g., machine learning (ML) methods like k-nearest neighbor (k-NN) have low detection accuracy and high false-alarm rate in detecting malicious attacks, especially for those unidentified attacks [61]. In contrast to conventional ML methods, DL methods have the advantages in higher detection accuracy while requiring no (or less) domain knowledge when processing and analysing user activity data [50]. In addition, the advances in unsupervised or semi-supervised DL methods are also helpful to detect and identify unknown attacks [51], [52].

The HetNets bring the challenges in network access management in 5G RAN. Take data roaming across different networks as an example, in which an AMP that is intended to access another guest network must first transfer the authentication of its host network to the guest network. However, the transmission of the authentication as well as the AMP's ID can cause the network latency across multiple networks and can also bring the privacy leakage risk since the confidential information can be wiretapped by malicious users [62], [63]. The convergence of blockchains and deep reinforcement learning (DRL) may potentially overcome this disadvantage. In particular, a blockchain is essentially a chain of data records, which have kept growing with the increment of the committed transactions. Thanks to the built-in mechanisms with distributed consensus, cryptographic schemes, peer-to-peer network, and smart contracts, blockchains can ensure traceability, immutability, and non-repudiation of blockchain data [64]. For example, smart contracts running on top of blockchain can automate the authentication in network roaming, whereas blockchain can essentially preserve the privacy of users [53]. During this process, DRL can help to establish dynamic network access rules across different networks as well as flexible data sharing services [54], [65].

DL approaches can also cope with issues in the network authorisation management. The appropriate network authorisation can protect the security and privacy of user data while facilitating the data sharing and accessing across different 5G RANs as well as diverse AMPs, UEs, and IoT devices [66]. The access control schemes such as attribute-based encryption (ABE) can achieve the fine-grained permissions for multiple authorities across different networks [67]. However, it is challenging for ML/DL approaches to analysing the encrypted data. The recent advancement in learning partially-encrypted data [55], deep neural networks (DNN) on encrypted data [56], a classifier based on DNN on encrypted data [57] can address this challenge.

C. Deep learning approaches in privacy preservation in edge computing

Edge servers are vulnerable to privacy leakage risks. On the one hand, the privacy leakage risks exist when raw data collected from AMPs, UEs, or IoT devices is sent to untrustworthy edge servers, which can be hijacked or misused by malicious users. Consequently, data stored at edge servers can be stolen or misused. Recent advances in differential privacy, homomorphic encryption, and federated deep learning (FDL) bring opportunities in offering privacy protection in edge computing. The main idea of differential privacy mechanisms is to either annex additive noise to the collected data or obscure sensitive metadata so that other parties obtaining the data cannot restore the original data [68]. Homomorphic encryption schemes encrypt the data while computing on cybertexts is still permitted [69]. In contrast to differential privacy and homomorphic encryption, FDL [70] is more suitable for edge computing since it allows training a DL model at each edge server locally without the necessity of uploading the data to the central servers. In this way, data privacy can be preserved.

On the other hand, edge servers, due to their limited computing and storage capabilities, are vulnerable to malicious attacks. First, computation-complicated cryptographic algorithms that have been well adopted in cloud servers cannot be directly employed at edge servers. Second, it is also difficult to deploy DDoS countermeasures such as quarantining (or isolating) at edge servers due to their limited computing and storage resources inferior to cloud servers [71]. Data stored at edge servers therefore can be compromised (i.e., tampered and accessed illegally) to privacy breaches. In this regard, DL approaches can help to identify these malicious attacks by analysing the activity reports and suggest relevant countermeasures [72]. For example, Tian et al. [58] showed that DL approaches can be used to detect web attacks at edge nodes by analysing URL data. Moreover, an unsupervised DL approach is adopted to detect unknown malicious attacks [59]. In addition, a DL approach based on the stacked autoencoder has been proposed in [60] for cyber-attack detection. Experi-

TABLE II
SUMMARY OF DEEP LEARNING APPROACHES FOR PRIVACY PRESERVATION IN 5G HETEROGENEOUS RAN NETWORKS

Issues	Potential Solutions	Representative Works	Main Contributions
Privacy leakage in radio spectrum sharing	DL approaches to analyse encrypted spectrum data	Lou et al. [42]	Propose a deep neural network based on the shift-accumulation-based leveled-homomorphic encryption
		Podschwadt et al. [43]	Propose an integrated method to combine RNNs and homomorphic encryption
	DL to analyse footprints from radio spectrum data	Kulin et al. [46]	Develop a CNN-based deep model to analyse spectrum data
		Utrilla et al. [47]	Design a GRU neural network to analyse radio signals
Privacy leakage in network access	Supervised, unsupervised and semi-supervised DL approaches	Elmasry et al. [50]	Design a double particle swarm optimization to optimise the selection of features and parameters for DL approaches
		Choi et al. [51]	Propose an unsupervised DL approach based on autoencoders
		Ran et al. [52]	Propose an semi-supervised DL approach based on the ladder network
	Blockchain and deep reinforcement learning	Refaey et al. [53]	Propose a blockchain-based roaming policy in RAN
		Yin et al. [54]	Design a FDL framework
	DL approaches on encrypted data for network access management	Ryffel et al. [55]	Design a DL approach based on functional encryption to analyse partially-encrypted data
		Nandakumar et al. [56]	Propose a stochastic gradient descent-based deep neural network
		Hesamifard et al. [57]	Develop a DNN-based classifier for encrypted data
Privacy leakage in edge computing	DL approaches to identify malicious attacks at edge nodes	Tian et al. [58]	Develop a DL approach to detect web attacks at edge nodes through analysing URL data
		Chen et al. [59]	Propose a unsupervised DL approach to detect unknown attacks
		Abeshu et al. [60]	Design a DL approach based on the stacked autoencoder to detect cyber-attacks

mental results demonstrated higher accuracy and lower false-alarm rate than shallow learning approaches.

Table II summarises the above three challenges, potential solutions, preventative studies as well as their major contributions.

IV. PRIVACY PRESERVATION IN 5G HETEROGENEOUS BEYOND-RAN NETWORKS

5G-enabled AMPs may experience beyond-RAN networks to communicate with each other if they are not staying in the coverage of the same RAN. Since AMPs may work in different application fields, beyond-RAN may include various types of networks including private networks (e.g., formed by a certain type of AMPs such as a swarm of unmanned aerial vehicles or unmanned surface vehicles) and public networks (e.g., public data centres). It may also involve multiple network domains (e.g., AMPs may be operated by different network operators and thus form different network domains) and diversified connectivity technologies (e.g., various private connectivity technologies within private networks and the Ethernet in public networks).

It has been a trend to leverage virtualisation technologies to enable various resources of beyond-RAN networks virtualised, in order to allow flexible resource provision. Emerging IT technologies, e.g., network virtualisation [73], software-defined networking (SDN) [74], [75] and network functions virtualisation (NFV) [76], [77], have been fast developed in recent years. Heterogeneous computing, networking, and storage resources can now be virtualised, creating a pool of shared resources for use in multiple vertical services, as shown in Fig. 4. These emerging IT technologies bring flexibility and efficiency for 5G and B5G/6G networks, while challenging its security architecture in the following ways:

- *Privacy preservation in shared resource infrastructure.* In the shared resource infrastructure, user privacy will be more easily compromised due to the unauthorised user data access attacks, e.g., exploitation of bugs in the hypervisor and distributed DDoS attacks. In the presence of 5G-enabled AMPs, the user privacy issues across multiple applications may get even worse as AMPs may provide services to many applications on the fly.
- *Privacy preservation under cross-domain environment.* For a certain range of applications enabled by diverse AMPs collaboratively, the data generated by an AMP may need to traverse multiple network domains, since AMPs may belong to different network operators. In addition, for some applications where the requested data needs to be retrieved from a data centre, the communication in 5G networks usually needs to traverse multiple network domains to reach the data centre. Protecting the privacy of each network domain in a cross-domain environment

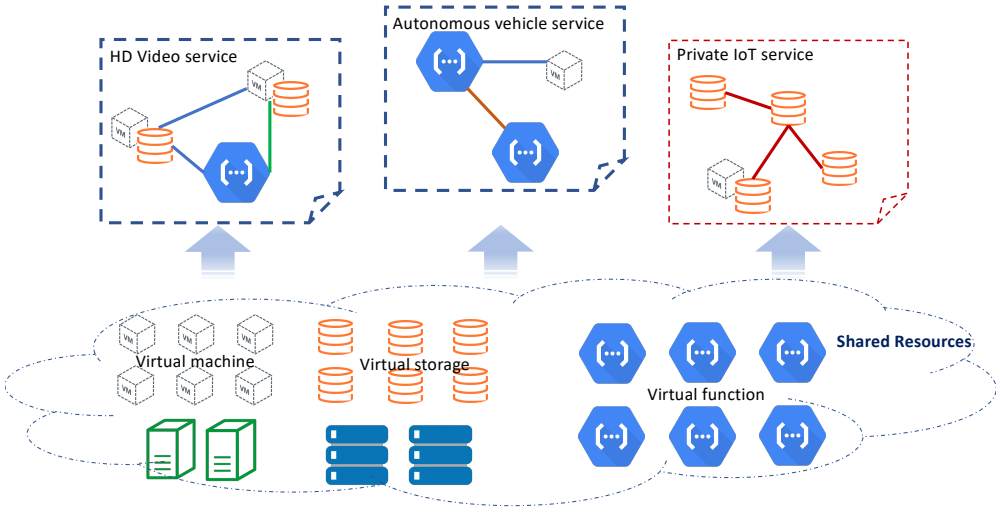

Fig. 4. Shared heterogeneous resources for vertical services.

is an important concern.

- *Privacy preservation under heterogeneous connectivity technologies.* For certain applications such as Industrial Internet of Things (a.k.a. Industrial Internet), 5G networks mixed with a large number of legacy connectivity technologies, e.g., the Industrial Ethernet, are being used to support the communication. In addition, AMPs may easily form private networks with private connectivity technologies, and thus the communication between AMPs may experience heterogeneous connectivity technologies. Ensuring the privacy preservation across multiple connectivity technologies is of paramount importance for the success of the applications running over them.

In what follows, we will discuss the emerging DL techniques that can be applied to cope with the privacy issues in the above three aspects of 5G HetNets. Tables III and IV summarise the relevant DL approaches for privacy preservation in 5G beyond-RAN. The privacy-preserving DL models developed for shared resource infrastructure can also be modified and adapted in a cross-domain environment and heterogeneous connectivity technologies. The DL models developed for either cross-domain environment or heterogeneous connectivity technologies in Table IV can essentially be leveraged to tackle each other's issues since these two issues share common features.

A. Privacy preservation in shared resource infrastructure

One strand of research in this direction is to employ DL approaches to efficiently detect unauthorised user data access attacks in the shared resource infrastructure. In the presence of AMPs, virtualised resources may be used to serve a wider range of users. For example, an unmanned aerial vehicle acting as a kind of AFVs, can be equipped with a lightweight computing device which can then be virtualised to provide services to the users coupled with different applications if the unmanned aerial vehicle is scheduled to perform tasks between those applications. An intrusion detection system (IDS) is an important tool to prevent and mitigate unauthorised access to the user data over network virtualisation, computing virtualisation, storage virtualisation, and even function virtualisation. Numerous DL models that have been developed for flow-based anomaly detection, spatial-temporal traffic analysis, and so on, can be readily adapted for unauthorised access detection. These DL models include RNN [78], [92], convolutional neural network (CNN) [79], [93], bidirectional long short-term memory [80], contractive autoencoder (CAE) [81], gated recurrent unit with attention [82], meta-learning [83], deep belief network [84], as well as a combination of multiple DL models.

Another strand of research for privacy preservation in shared resource infrastructure is to modify the original DL models to make them work in a privacy preservation environment. In other words, the modified DL models should be able to be trained using the encrypted data [90], since applications require the traffic data to be encrypted for privacy preservation. In this strand, the modification of DL models usually needs to consider the methods of traditional privacy preservation technologies such as homomorphic encryption [94], secure multi-party computation [95], and differential privacy [96]. A number of modified DL models have been developed, e.g., E2DM [85] and Gazelle [86] for the cases under homomorphic encryption, DeepSecure [87] and ABY3 [88] for secure multi-party computation, and PATE [89] for differential privacy based scenarios. Further, Ma et al. [90] proposed a privacy-preserving learning model that applied DL over encrypted data with multiple keys. In addition, many emerging privacy-preserving learning frameworks, e.g., federated learning, can be adopted to develop privacy-preserving DL models [91].

B. Privacy preservation under cross-domain environment

Recall that 5G-enabled AMPs contain various types of platforms, e.g., AFVs, AUVs, ASVs, and ALVs. Each type of AMPs is usually designed for a specific task, and different AMPs may work in different application areas. In addition, the AMPs working on a task are usually operated by a network/service provider, forming a private network domain.

TABLE III
SUMMARY OF DEEP LEARNING APPROACHES FOR PRIVACY PRESERVATION FOR SHARED RESOURCE INFRASTRUCTURE IN 5G BEYOND-RAN NETWORKS

Issues	Potential Solutions	Representative Works	Main Contributions
Privacy leakage in shared resource infrastructure	Use DL based IDS to detect unauthorised data access	Yin et al. [78]	Develop an RNN based IDS
		Wang et al. [79]	Develop a hierarchical spatial-temporal features based IDS, using CNN to learn low-level spatial features of network traffic and long short-term memory network to learn temporal features
		Alkadi et al. [80]	Propose an IDS that employs bidirectional long short-term memory DL algorithm to deal with sequential network data
		Wang et al. [81]	Develop an IDS that uses a stacked contractive autoencoder method for unsupervised feature extraction and then adopts support vector machine classification algorithms for intrusion detection
		Liu et al. [82]	Develop a bidirectional gated recurrent unit (GRU) based IDS with hierarchical attention mechanism
		Xu et al. [83]	A meta-learning framework is proposed for few-shot detection of some intrusion scenarios like zero-day attacks
		Zhang et al. [84]	An IDS with two parts: 1) a real-time detection algorithm based on flow calculations and frequent patterns, and 2) a classification algorithm based on the deep belief network and support vector machine
	Develop privacy preserving DL models that consider homomorphic encryption, multi-party computation and differential privacy	Jiang et al. [85]	Propose an encrypted data and encrypted model (E2DM) to handle homomorphic encrypted data for DL models. E2DM provides a practical solution to encrypt a matrix homomorphically and perform arithmetic operations on encrypted matrices
		Juvekar et al. [86]	Design GAZELLE, a scalable and low-latency system for secure neural network inference, considering a combination of homomorphic encryption and traditional two-party computation techniques
		Rouhani et al. [87]	Propose a framework called DeepSecure that enables scalable execution of DL models in privacy-preservation settings.
		Mohassel et al. [88]	Design a general framework called ABY3 for privacy-preservation machine learning, and used it to obtain new solutions for training linear regression, logistic regression and neural network models. ABY3 can be applicable for multi-party computation scenarios.
		Papernot et al. [89]	Propose an approach that can provide strong privacy guarantees for training data of DL: Private Aggregation of Teacher Ensembles (PATE)
		Ma et al. [90]	Propose a privacy-preserving learning model, called PDLM, to apply DL over the multi-key encrypted data.
		Liu et al. [91]	Propose a privacy-preserving machine learning technique named federated learning and developed a Federated Learning-based Gated Recurrent Unit neural network

From a global point of view, AMP enhanced 5G HetNets are naturally a cross-domain environment, which hinders data sharing between domains.

The modification of DL models in the second strand of the above section is also applicable to the privacy preservation under a cross-domain environment, since traditional privacy preservation technologies are still being widely used in this environment. Besides, due to the performance issues of applying the classic privacy preservation technologies in a cross-domain environment, several other privacy preservation technologies like PYCRO [97] have been proposed. The modification of DL models also needs to consider these new technologies for more efficient privacy preservation in a cross-domain environment.

The main trend of research is shifting towards using the data of each network domain to train DL models so that the data does not need to be transferred outside of the domain in which it originates. The models that are separately trained in each domain are then jointly optimised for a cross-domain purpose. This is a fairly intuitive way to achieve the privacy preservation in a multi-domain environment without sharing the data between domains. There are a number of research results dedicated in this area, e.g., the well-known federated learning [98] and the privacy preserving DL technique proposed by Shokri and Shmatikov [99]. In the event that the model training

TABLE IV
SUMMARY OF DEEP LEARNING APPROACHES FOR PRIVACY PRESERVATION FOR CROSS-DOMAIN ENVIRONMENT AND HETEROGENEOUS CONNECTIVITY TECHNOLOGIES IN 5G BEYOND-RAN NETWORKS

Issues	Potential Solutions	Representative Works	Main Contributions
Privacy leakage in cross-domain environment	Develop privacy preserved DL models	Chen et al. [97]	Propose a cryptographic protocol, named PYCRO, that is specifically designed for privacy-preserving cross-domain routing optimisation in Software Defined Networking (SDN) environments
	Use local data to train the DL model	Aledhari et al. [98]	A comprehensive introduction of federated learning that allows the use of local data to train a DL model locally
		Shokri et al. [99]	Develop a practical system that enables multiple parties to jointly learn an accurate neural-network model for a given objective without sharing their input dataset
		Ramakrishnan et al. [100]	Develop a solution to provide interpretable explanations for transfer learning in sequential tasks
Privacy leakage in heterogeneous connectivity technologies	Consider diverse trust degrees of different connectivity technologies	Wang et al. [101]	Propose a two-phase framework that computes the average value while preserving heterogeneous privacy for nodes' private data that may happen in heterogeneous connectivity technologies environment

has to be performed sequentially across multiple domains, i.e., the output of a model trained in one network domain is the input for the model to be trained in another network domain, the transfer learning paradigm has been proposed for this purpose. With the use of transfer learning, the trustworthiness of the model output needs to be considered [100]. Many studies have been devoted to improving the reliability of DL, but this is out of the scope of this paper.

C. Privacy preservation under heterogeneous connectivity technologies

Given the fact that AMPs have been used in various applications for many years, although 5G-enabled AMPs are being widely used, there are a fair amount of legacy connectivity technologies in those applications. For example, the backhaul connecting RAN and core networks have a number of choices for the connectivity technologies, including copper-line, fibre-optic, microwave, and even satellite backhaul and WiFi backhaul links. In addition, many private networks established by AMPs may use private connectivity technologies. The heterogeneity of connectivity technologies has caused significant challenges on privacy preservation.

The key issue for privacy preservation with heterogeneous connectivity technologies is that different connectivity technologies may adopt different privacy preservation paradigms. The training of DL models needs to consider diverse trust degrees of different connectivity technologies. This actually creates the noisy label issue of machine learning. This issue may also apply for the model training in a cross-domain environment when the degrees of the fidelity of collected data at each domain are different. Wang et al. [101] proposed a two-phase framework that is able to calculate the average trust degree while preserving heterogeneous privacy for the collected data with different trust degrees. In addition, based on the definition of Kullback–Leibler (KL) privacy [102], they derived the analytical expressions of the privacy preservation degree and quantify the relation between different privacy preservation degrees. The modification of DL models needs to take privacy preservation degrees into account in order to develop a unified model for privacy preservation across heterogeneous connectivity technologies.

V. PRIVACY PRESERVATION FOR END-TO-END NETWORK SLICING IN 5G

With the increase in the number of AMPs and the emergence of various new scenarios, it is expected that user demands for communications and services will increase dramatically in the future, in terms of scale and variability. This requires wireless networks (e.g., 5G networks) to become more agile to meet the changing needs of users. However, there are various proprietary hardware devices in the current network, which increases the investment cost of network operators and is not conducive to the introduction of new services in the Internet. Therefore, new technologies are needed to reduce investment in infrastructure and management.

5G networks are designed with these factors in mind. The emergence of various new technologies is expected to technically ensure that operators are able to provide diverse 5G services in a flexible, economical, and sustainable manner. Among them, network slicing is considered as a promising direction and has become a key technology for meeting the various requirements of different use cases [103], [104], [105].

Network slicing aims to divide (slice) the physical network in the network infrastructure into isolated and independently managed resource pools, and to create the concept of end-to-end (E2E) logically virtual networks [106]. Each virtual network can be customised and optimised for different users or specific types of applications. In a slice-based 5G network, resources in infrastructures belonging to different domains can be efficiently allocated to multiple slices according to users needs. In other words, network slicing allows multiple network operators to share a network infrastructure, so that each network operator can provide its own unique functions and services to users [107]. In addition, network slicing should not

only have the bespoke functions required by the corresponding services, but also the ability to adapt to changing needs. By using virtualisation technologies, physical network resources can be dynamically and efficiently scheduled to logical network slices based on changing user needs [108], [109]. It should be pointed out that providing a virtualised end-to-end environment that is open to third parties is one of the key functions to distinguish network slicing and network sharing. Through network slicing technologies, 5G networks can support users' diverse needs and a wide range of services in a sustainable and flexible manner. However, this also complicates the situation in the network. How to protect the privacy of network users when deploying and running heterogeneous end-to-end slicing is a challenge [110], [111]. In particular, a network slice may span different parts of 5G networks such as RANs, core networks, and carrying networks. Therefore, when proposing solutions for privacy preservation in network slicing, it is necessary to consider the heterogeneous components across the entire network.

When discussing which information of AMPs face a higher risk of privacy leakage when they use network slicing, we analyze the two roles that AMPs may play separately. One is as a user who uses network slicing, and the other is to play the role of a service provider with data forwarding functions and can provide slicing services. As users, AMPs may leak their identities, locations, behaviors, plans, and even transmitted data when using end-to-end network slicing. When AMPs act as service providers, malicious users may obtain information about the node's resource scale, capabilities, and resource usage, and even steal the AMP's valuable algorithms and execution strategies.

Before discussing potential solutions, let us analyse the existing privacy issues from the perspectives of resource scheduling, orchestration of slices, communication between device and slice, and communication between slices.

- *Privacy leakage in resource scheduling in slices.* User demands for resources (in slices) may cause privacy leakage. This is because users have different requirements for the resources in the network slices that are used to accommodate different applications or services [110]. User's requirements for specific functions will reflect the scale of deployment of corresponding resources in a slice, which may leak information on user behaviours. For such problems, we should explore the allocation of resources in a way that does not reveal privacy, and at the same time, without affecting users' needs.
- *Privacy leakage in slice orchestration.* The process of orchestrating and managing network slices is complex. For example, from the perspective of system security, the order in which network traffic passes through network functions will affect where to deploy security mechanisms and security policies. Consequently, resource orchestration in slices based on user needs will determine network topology and specific services. So similar to resource scheduling in a slice, orchestration of network slices may also be used to infer user behaviours [112], [113]. Therefore, 5G systems need to provide adequate security guarantees during the orchestration process, including reducing user privacy concerns, and the relevance and consistency of resources shared between services need to be efficiently guaranteed. In addition, network slices need to be effectively isolated between each other. Otherwise, sensitive data processed or managed in one network slice may be obtained by applications running in another.
- *Privacy leakage in communication between device and network slice.* 5G networks need to support the access to a large number of devices, so the management of device access is an important issue. Considering that delay in 5G networks should be ultra low for certain services, the process of device accessing slices needs to be completed efficiently and without introducing security issues. The communication between the device and the network slice includes a lot of information, such as signaling and data sent by the user, which may involve user privacy. However, such communications may be tampered with, causing the user to select the wrong network slice and enter an untrusted and insecure network slice [114]. In addition, if the device's access to the network slice lacks effective authentication measures, unauthorised communication may enter the slice. Such behaviors will occupy and consume the resources of network slices and affect the rights and interests of legitimate users. What is more serious is that the user's privacy information may be intercepted in the slice.
- *Privacy leakage in communication between slices.* An attacker can attack from one slice to another. Therefore, even in the same Internet service provider (ISP) or the same network infrastructure, effective access control approaches should be implemented between different slices [115]. Unauthorised access should be blocked to prevent internal attacks from the same network domain.

Fig. 5 shows the processes that a data packet passes through when users use end-to-end network slices. It shows user privacy may be leaked in the communication between device and slice, and in the interaction between slices. Therefore, effective isolation measures and other new technologies (including those based on DL) are needed to strengthen the privacy protection of users. The same challenge also exists when data packets are transmitted across the network infrastructure before or after they reach different network functions. Privacy protection measures should cover the entire process of users using end-to-end network slices [106], [116].

Based on the above analysis of the processes that may cause the leakage of user privacy, we can consider solving such problems from the following aspects.

A. Privacy preservation in accessing slices

The security of accessing slices can be analysed from two perspectives: network slices and users. From the perspective of network slices, in 5G networks, effective authentication mechanisms are needed to prevent users from illegally accessing slices [117], [118], [119].

When users access slices, DL techniques can be used in access control and identity authentication. Attribute based access control (ABAC) [120], [121] is an important access

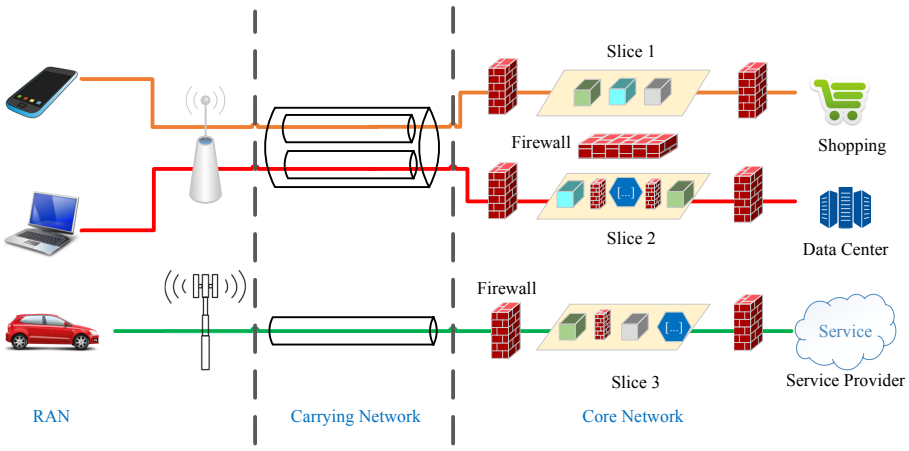

Fig. 5. An overview of the isolation between end-to-end network slicing.

control mechanism. According to an estimate, 70% of enterprises will use ABAC mechanisms in 2020 [122]. However, in ABAC, the policy authoring task requires a lot of overhead and is a limiting factor. In the recent work [122], the authors proposed a method using DL to automatically convert the natural language access control policy (NLACP) in ABAC to a machine-readable form. This work is beneficial to the efficient implementation of ABAC strategies in 5G HetNets.

Identity authentication is an important technology for access control. In a recent study [123], the authors proposed a privacy preservation scheme in the Internet of Vehicles (IoVs), which is a typical application scenario of AMPs. Large-scale IoV networks are usually divided into different fogs [124]. Each fog has its own fog head, which is similar to the central processing unit in the fog that can centrally manage members in the fog. This structure effectively reduces the latency and position awareness in the vehicle communication. The process of joining the fog naturally requires identity authentication. Based on this background, a two-way authentication and security monitoring method using the random forest algorithm of a DL scheme, named FBIA, was proposed to protect system security and user privacy in IoV. The evaluation results showed that the FBIA scheme has higher authentication accuracy and better adaptability to the high-speed mobile network environment. In addition, in recent years, some traditional authentication methods for access control have also begun to use DL techniques [125], [126]. Effective and reliable authentication methods help improve the service provider's access control capabilities.

From the user's perspective, it is also necessary to ensure that the device is accessing or is about to access the correct and trusted slice, instead of a fake network slice or service [127]. DL techniques can be used to find anomalies in slices. Users can use the exception as a clue to further determine whether a correct slice is accessed. Efficient access control mechanisms and anomaly detection mechanisms with the help of DL technologies are expected to improve the security of 5G networks and prevent the leakage of user privacy. In addition, users should have the right and opportunity to use suitable slices. DL approaches can be used to help ISPs select a suitable set of slices for a user. Research on this field can refer to a series of personalised recommendation algorithms based on DL technologies [128].

Whether an AMP is a service provider that provides network slicing or a user who uses slices, they all expect to cooperate with trusted objects. Trust management can be used by the slice provider to confirm that the user is not malicious for the sake of system security. For users, they can also select slices from trusted service providers through trust management technology to ensure that their private information is properly handled. The traditional trust management mechanism is insufficient for AMPs [129]. DL technology can help improve the efficiency and effectiveness of trust management mechanisms. In [130], Raya et al. evaluated several techniques, including Bayesian inference and the Dempster-Shafer Theory. Then, the authors used them for trust computation. In [131], the authors proposed a RESTful message exchanging architecture, and a trust model based on the solution of a multi-class classification problem using machine learning techniques. In [132], a DL based driver classification and trust computation (DL-DCTC) scheme was proposed. The authors developed a sequential deep neural network model to calculate reward points based on the behavior of equipment (e.g., vehicles), and classify fraudulent and non-fraudulent messages.

B. Privacy preservation for applications in slices

In addition to strengthening access control to prevent malicious users from entering a slice to obtain information about other users and to prevent users from entering fake slices to cause privacy leakage, the security of the slice itself should also be considered. In particular, a network slice may contain a series of services or network functions. These network functions can be considered as different applications. We should therefore focus on the security of these services and functions as we do in our end devices. This is because if an application in the slice is malicious, it will easily obtain the user's information and abuse it, causing the leakage of user privacy. With excellent feature extraction capabilities, DL approaches can be used to perform anomaly detection, network intrusion detection, and malware detection [133],

[134], [135], [136]. Schultz et al. [137] first applied machine learning methods to malware detection. Since then, more and more studies have tried to use various artificial intelligence techniques to detect malware. Among them, methods based on DL can improve detection accuracy within a range of sample sizes and traffic anomaly types [138].

In a recent study [133], the authors represented malware as opcode sequences and detected it using a deep belief network (DBN). In the field of malware detection, it usually takes a lot of manpower to determine whether an executable is a malware. Therefore, it is difficult for researchers to build a data set that contains a sufficient number of data samples for training. Considering this factor, the authors proposed a DBN-based malware detection model in this paper, which can learn from unlabeled data. In [139], Hardy et al. proposed a DL architecture using a stacked AutoEncoders (SAEs) model for intelligent malware detection. Its input is based on Windows Application Programming Interface (API) calls extracted from a portable executable (PE). The SAEs model uses a greedy layerwise training operation for unsupervised feature learning, followed by supervised fine-tuning of parameters such as weights and offset vectors. Different network functions in the slice can be regarded as different software programs. Using similar methods of SAEs can effectively detect malicious network functions in slices, thereby reducing the risk of user privacy leakage.

In [140], the authors discussed the problems faced by existing intrusion detection technologies. In this regard, they proposed a new DL technology for intrusion detection, with nonsymmetric deep autoencoder (NDAE) for unsupervised feature learning. Furthermore, they proposed a novel DL classification model constructed using stacked NDAEs. In [78], the authors explored how to model an IDS based on DL, and proposed a DL method for intrusion detection using recurrent neural networks (RNN-IDS). In addition, the authors studied the performance of the proposed model in binary classification and multiclass classification, as well as the influence of the number of neurons and different learning rates on the performance of the proposed model.

End-to-end slicing requires the support of SDN technology [141], [75]. Some studies have proposed DL methods specifically for intrusion detection in SDN [142], [143], [144], [145], [146]. In [145], the authors proposed a DDoS detection system in SDN. The authors implemented the system as a network application in the SDN controller. DL methods are used for feature extractors and traffic classification. In [146], the authors proposed a lightweight DDoS flooding attack detection solution, using an intelligent mechanism based on self organising maps (SOM) [147], which is a kind of unsupervised artificial neural networks trained by the features of the traffic flow. The authors used SOM to classify network traffic as normal traffic or abnormal traffic, and used traffic statistics as parameters for the SOM computation.

C. Privacy preservation in slice resource management

In 5G networks, slice resources need to be allocated according to user needs. In addition, the user's demand for the resources of a network slice is dynamically changing. Especially with the increase in the number of AMPs and the continuous diversification of AMP requirements, it is necessary to use machines for automated management instead of manual operations to manually allocate resources [148]. DL can play an important role in the allocation and scheduling of slice resources, and it can also strengthen the privacy protection of users in this process [149], [150], [151].

In view of the fact that the service provider needs to periodically obtain some data belonging to the user, such as the user's needs, in order to adjust the resources allocated to the slice [110]. Data-sharing methods need to be carefully designed in order to protect the privacy of users. Differential privacy is a method for data publishing and sharing. Using differential privacy technology can effectively protect users' privacy when they provide information to ISPs or service providers (SPs). The effect of differential privacy can also be enhanced with DL technologies [152], [153]. In [154], the authors proposed a new method for learning and a refined analysis of privacy costs within the framework of differential privacy. The proposed method can effectively address the user's concerns about the leakage of private information during the training of models.

Besides differential privacy protection methods, DL approaches can be used to achieve data sharing with privacy protection. Wang et al. [155] proposed a mechanism for sharing user information using DL approaches. To protect sensitive information, the authors introduced a lightweight privacy protection mechanism, which consists of arbitrary invalid data and random noise to provide a strong privacy guarantee. However, the added interference to the original data will inevitably have a negative impact on the effectiveness of further inference in the cloud. To mitigate this adverse effect, the authors proposed a noise training method to enhance the robustness of the cloud-side network to the interfered data. This mechanism can solve the problem of privacy leakage when transmitting data from the device to the ISPs and SPs.

D. Privacy protection in data transmission

There are some interesting research topics on how to ensure the confidentiality of data during transmission. As we know, encryption is an important means to protect users' private information. In 2016, Google Brain devised a method to apply DL to encryption technology [156]. In the proposed method, the authors assumed that a system consists of neural networks named Alice and Bob, and the goal is to limit what a third neural network named Eve learns by eavesdropping on the communication between Alice and Bob. In the learning process, there is no need to prescribe a particular set of cryptographic algorithms, nor to indicate ways of applying these algorithms Such research showed us the broad application prospects of DL in the field of privacy preservation.

E. Other privacy preservation considerations

End-to-end slicing spans various network infrastructures, including RAN, carrying networks, and core networks. In this section, we show which areas in an end-to-end network slice

TABLE V
DIFFERENT ROLES THAT NEED TO CONSIDER PRIVACY IN AN END-TO-END NETWORK SLICE

Region \ Roles	Regulators (government)	ISP	User Data	User Equipment (UE)	IT Company	Network Function or Virtual Network Function
RAN	√	√	√	√	×	√
Carrying Network	√	√	√	×	√	×
Core Network	√	√	√	×	×	√

TABLE VI
DIFFERENT EVENTS THAT NEED TO CONSIDER PRIVACY IN AN END-TO-END NETWORK SLICE

Region \ Events	Access Control	Resource Request	Resource Management (Scheduling)	Data Transmission
RAN	√	√	√	√
Carrying Network	×	×	√	√
Core Network	√	√	√	√

need to consider privacy protection from two perspectives: different roles and different events. Specifically, Table V shows whether different roles need to implement privacy protection measures in different areas of the network. Table VI lists several common behaviors in 5G networks and describes whether it is necessary to take measures to protect user privacy. From these tables, we can clearly observe that privacy protection needs to be considered in various processes in 5G HetNets. New technologies (including DL) are therefore expected to bring higher efficiency and better results in terms of privacy protection. Table VII summarises the relevant DL approaches for privacy preservation in 5G end-to-end network slicing.

VI. RESEARCH CHALLENGES AND OPEN ISSUES

Although DL approaches have been used to ensure privacy preservation in 5G HetNets, there are still many on-going challenges and open issues that need to be considered in future research. In this section, we discuss a set of issues in 5G heterogeneous RANs, beyond-RAN networks, and also end-to-end network slices.

A. Privacy preservation in 5G heterogeneous RANs

- Heterogeneous data in 5G RAN has different privacy-preservation requirements. It is a challenge to preserve the privacy at different levels of requirements from different AMPs, UEs, and IoT devices. For example, healthy data from body sensor networks may have higher privacy-preservation requirements than vehicular network data, which is mainly used for traffic management and intelligent transportation system (ITS). Future DL models should take different privacy-preservation requirements into account. Moreover, multi-authority attribute-based encryption schemes should be integrated with DL models to meet this emerging demand.
- Edge servers are often resource-limited whereas most of the incumbent DL models have stringent requirements on computing capabilities (e.g., using GPUs to fasten the training process) and storage capacity (e.g., DNNs often have large models). In addition, federated DL models also require homomorphic encryptions, which are often computationally intensive. Compacted DNNs technologies include network pruning, knowledge distillation, and network structure modifying while the feasibility of these technologies in AMPs is still worth investigating. It is expected to design portable privacy-preservation DL models being suitable for edge servers in the future.
- DL models are also vulnerable to malicious attacks, e.g., small perturbations can essentially paralyse the whole CNN model. Moreover, some malicious users may intentionally add adversarial data samples to contaminate the training dataset so as to poison the entire DL models. How to prevent DL models from adversary attacks is an open question that is worthwhile for further investigation in the future. For example, the integration of DL models with blockchain has the potential to overcome this issue due to the traceability of blockchain, which can trace newly-added data and identify potential threats.

B. Privacy preservation in 5G beyond-RAN networks

- In the shared 5G core resource infrastructure, more types of resources will be virtualised to support diversified requirements of services. It is a challenging issue to ensure the consistency of privacy preservation requirements that have been enforced by each resource, e.g., computing, networking, storage, and function, when data are collected across resources for DL model training. In addition, virtualised resources carried by 5G-enabled AMPs can be used to provide services in different application fields. Given the fact that different application fields may have different privacy preservation requirements, the above consistency issue will become more challenging.
- With the emergence of a growing number of AMPs involved in 5G HetNets, the privacy protection of data is becoming more significant. The performance of DL models usually degrades when encrypted data are collected for the model training. How to mitigate the impact of encrypted data e.g. by homomorphic encryption, on the performance of DL model training is an important

TABLE VII
SUMMARY OF DEEP LEARNING APPROACHES FOR PRIVACY PRESERVATION IN 5G END-TO-END NETWORK SLICING

Issues	Potential Solutions	Representative Works	Main Contributions
Privacy leakage in accessing slices	DL approaches for access control	Alohaly et al. [122]	Propose a method using DL to automatically convert the natural language access control policy (NLACP) in ABAC to a machine-readable form
		Song et al. [123]	Design a two-way authentication and security monitoring method using the random forest algorithm of a DL scheme, named FBIA, to protect system security and user privacy in IoV
		Zou et al. [126]	Design DL techniques to learn and model the biometrics to obtain good person identification and authentication performance
	DL approaches for trust management	Refaey et al. [130]	Proposed an architecture using DL for trust computation
		Tangade et al. [132]	Design a DL based driver classification and trust computation (DL-DCTC) scheme
Privacy leakage by malicious applications in slices	DL approaches in malware detection	Ding et al. [133]	Represent malware as opcode sequences and detected it using a deep belief network (DBN)
		Hardy et al. [139]	Proposed a DL architecture using a stacked AutoEncoders (SAEs) model for intelligent malware detection
	DL approaches in intrusion detection	Shone et al. [140]	Propose a DL technique for intrusion detection with nonsymmetric deep autoencoder (NDAE) for unsupervised feature learning
		Yin et al. [78]	Propose a DL method for intrusion detection using recurrent neural networks (RNN-IDS)
	DL approaches attack in detection	Niyaz et al. [55]	Proposed a DDoS detection system using DL methods for feature extractors and traffic classification
Privacy leakage in slice resource management	DL approaches in resource management	Abadi et al. [154]	Propose a new method for learning and a refined analysis of privacy costs within the framework of differential privacy
		Wang et al. [155]	Propose a mechanism for sharing user information using DL approaches
	Encryption	Abadi et al. [156]	Propose a method to apply DL to encryption technology

future research direction. It is becoming more challenging if DL models consider the data that are encrypted by heterogeneous encryption technologies.

- Many 5G vertical services such as Industrial Internet of Things (IIoT) ask for stringent requirements, e.g., ultra-high reliability and ultra-low latency. 5G-enabled AMPs are in place to assure such stringent requirements. For example, 5G-enabled unmanned aerial vehicles equipped with edge computing devices are widely used to reduce computation delay for nearby IIoT devices. Balancing the accuracy of privacy preservation DL models with a number of other service requirements is an open issue that needs to keep a watchful eye on it.
- Given the nature of heterogeneous connectivity technologies and cross-domain infrastructure of 5G networks, the scalability issue will become a bottleneck that hinders the efficient and online training of privacy preservation DL models. How to build scalable DL models in this context with HetNets, heterogeneous connectivity technologies, heterogeneous encryption technologies, heterogeneous vertical services, heterogeneous service requirements, and heterogeneous 5G-enabled AMPs, is still a challenging issue.

C. Privacy preservation for end-to-end network slicing in 5G

- In a 5G HetNet, it is a challenge to maintain the policy consistency of the various parts involved in the communication process. Because this involves the collaboration of different components (e.g., different network functions) in the network. DL techniques are expected to make better and timely decisions for communication systems (including network functions that traffic needs to pass through), but they still faces efficiency issues. Especially, the low latency required by 5G networks puts forward higher requirements on the design of the mechanism. Therefore, the update and synchronization mechanisms (without losing user privacy) suitable for 5G HetNets need further research.
- In 5G networks, there are HetNets composed of different types of networks. Therefore, the establishment of trust relationships between different network architectures and different network domains is more complicated. For network domains or network slices that have not interacted with each other and may belong to different ISPs, how to accurately establish a trust relationship is a challenging problem. The establishment of the relationship between

slices, as well as between users (devices) and slices, can refer to the research of social networks. This is because, to some extent, the relationship in the network is an extension of the relationship in reality. DL approaches have been applied to social networks and achieved ideal results. Therefore, the study of social networks combined with DL technologies may be applied to build trust relationships in 5G HetNets. In this way, it is expected to establish a trust relationship without directly obtaining the information of a specific user, which will help protect the privacy of users.

- SDN and NFV are key technologies in implementing network slicing. Among them, SDN is a suitable technology for configuring and controlling the resource forwarding plane. The NFV technology can manage the lifecycle of network slices and orchestrate virtual network functions (VNF) effectively. Therefore, when solving privacy protection issues (or other security issues) caused by communication through end-to-end network slicing, it is necessary to consider improving SDN and NVF technologies that have been applied to 5G.

Through the investigation and analysis in this paper, we can find that similar work may be involved in different communication processes given that 5G networks are HetNets. Authentication is a typical example. In a 5G network, the system needs to identify and verify the user's identity and manage user behavior in multiple processes. However, in a heterogeneous 5G network, Internet service providers and network function providers may come from different organizations or companies. Therefore, the pursuit of unified and efficient identity verification faces challenges in 5G HetNets. If the user's performance in multiple processes during communication cannot be judged together, we may miss the opportunity to find malicious users. For the work that requires similar data sets as the basis for judgment in 5G networks, we can refer to the idea of distributed machine learning [157], [158], [159], [160] and use technologies such as federated learning [70] and shared machine learning [161], [162] to design mechanisms based on 5G HetNets.

In recent years, federated learning has attracted attention as an emerging artificial intelligence technology [70], [163], [164], [165]. Its design goal is to develop efficient machine learning approaches between multiple participants or multiple computing nodes on the premise of ensuring information security during data exchange and protecting user data security and user privacy [91], [166]. In the future, we can consider relying on the concept of federated learning to return the results to the data center after training in each network domain (or slice). The data can then be further analysed using DL techniques. The user's data will not leave the slice during this process. We still take identity authorization as an example. The ideal goal is that different parts of the 5G network can continuously learn and train separately, and discover potential security risks through collaboration, and then improve the results of identity authorization.

When using distributed machine learning technologies, it is inevitable to face a series of problems such as policy consistency and communication efficiency in distributed systems. However, with the low latency requirements of 5G networks, designing such a reliable and efficient solution is a challenging problem. In addition, the differences in the standards and methods of identity authentication in different processes may also become challenges. Despite the need for further research, this case shows that DL has a good prospect in promoting collaboration between different parts of the 5G HetNets.

VII. Conclusion

This article has investigated the use of DL to handle privacy preservation issues in 5G HetNets, targeting at heterogeneous RANs, beyond-RAN networks, and end-to-end networks slice. In particular, the effects of 5G-enabled AMPs on privacy issues in 5G HetNets have been thoroughly investigated. A set of relevant research challenges and open issues has been outlined to guide future research. We hope this article provides useful insights and summary that can help the development of AMPs in the era of 5G/B5G and 6G.

References

[1] Y. Wu, "Cloud-edge orchestration for the internet-of-things: Architecture and ai-powered data processing," *IEEE Internet of Things Journal*, pp. 1–1, doi: 10.1109/JIOT.2020.3014845, 2020.

[2] Y. Wu, H. N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable iiot critical infrastructures in industry 4.0," *IEEE Internet of Things Journal*, pp. 1–1, 10.1109/JIOT.2020.3025916, 2020.

[3] Y. Wu, H. Huang, C. Wang, and Y. Pan, *5G-Enabled Internet of Things*. Boca Raton: CRC Press, 2019.

[4] D. S. Sabareesh, G. V. P. Reddy, S. Jaiswal, J. M. Ppallan, K. Arunachalam, and Y. Wu, "Redundant tcp connector (rtc) for improving the performance of mobile devices," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 10.1109/WCNC.2019.8885889, 2019, pp. 1–7.

[5] X. Cheng, Y. Wu, G. Min, A. Y. Zomaya, and X. Fang, "Safeguard network slicing in 5g: A learning augmented optimization approach," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1600–1613, 2020.

[6] B. Qian, H. Zhou, T. Ma, K. Yu, Q. Yu, and X. Shen, "Multi-operator spectrum sharing for massive iot coexisting in 5g/b5g wireless networks," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 10.1109/JSAC.2020.3018803, 2020.

[7] J. Yang, N. Guizani, L. Hu, A. Ghoneim, M. Alrashoud, and M. S. Hossain, "Smart autonomous moving platforms," *IEEE Network*, vol. 34, no. 3, pp. 116–123, 2020.

[8] X. Zhou, W. Liang, K. I. Wang, H. Wang, L. T. Yang, and Q. Jin, "Deep-learning-enhanced human activity recognition for internet of healthcare things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6429–6438, 2020.

[9] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[10] Z. Yan, J. Ge, Y. Wu, L. Li, and T. Li, "Automatic virtual network embedding: A deep reinforcement learning approach with graph convolutional networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1040–1057, 2020.

[11] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6g: A survey," *IEEE Communications Surveys Tutorials*, pp. 1–1, 10.1109/COMST.2020.3011561, 2020.

[12] Q. Kong, R. Lu, F. Yin, and S. Cui, "Privacy-preserving continuous data collection for predictive maintenance in vehicular fog-cloud," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 10.1109/TITS.2020.3011931, 2020.

[13] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," *IEEE Network*, vol. 34, no. 2, pp. 37–45, 2020.

[14] Y. Ma, Y. Wu, J. Li, and J. Ge, "APCN: A scalable architecture for balancing accountability and privacy in large-scale content-based networks," *Information Sciences*, vol. 527, pp. 511 – 532, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025519300659

[15] Z. Yao, J. Ge, Y. Wu, and L. Jian, "A privacy preserved and credible network protocol," *Journal of Parallel and Distributed Computing*, vol. 132, pp. 150 – 159, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731518308323

[16] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, "An efficient collaboration and incentive mechanism for internet of vehicles (iov) with secured information exchange based on blockchains," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1582–1593, 2020.

[17] B. Brik, A. Ksentini, and M. Bouaziz, "Federated learning for uavs-enabled wireless networks: Use cases, challenges, and open problems," *IEEE Access*, vol. 8, pp. 53 841–53 849, 2020.

[18] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, "Blockchain-based privacy preservation for 5g-enabled drone communications," *IEEE Network*, 2020.

[19] B. Wu and Z. Xu, "Research on integrated space-air-ground tt c and communication network based on space tracking ship," in *2017 16th International Conference on Optical Communications and Networks (ICOCN)*, 2017, pp. 1–3.

[20] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5g network edge cloud architecture and orchestration," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017.

[21] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative mobile edge computing in 5g networks: New paradigms, scenarios, and challenges," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 54–61, 2017.

[22] Z. Ning, J. Huang, X. Wang, J. J. Rodrigues, and L. Guo, "Mobile edge computing-enabled internet of vehicles: Toward energy-efficient scheduling," *IEEE Network*, vol. 33, no. 5, pp. 198–205, 2019.

[23] J. Zhang, Y. Wu, G. Min, F. Hao, and L. Cui, "Balancing energy consumption and reputation gain of uav scheduling in edge computing," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 10.1109/TCCN.2020.3004592, 2020.

[24] Y. Zuo, Y. Wu, G. Min, C. Huang, and K. Pei, "An intelligent anomaly detection scheme for micro-services architectures with temporal and spatial data analysis," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 548–561, 2020.

[25] Y. Wu, F. Hu, G. Min, and A. Zomaya, *Big Data and Computational Intelligence in Networking*. CRC Press, 2017.

[26] Y. Wu, "Robust learning enabled intelligence for the internet-of-things: A survey from the perspectives of noisy data and adversarial examples," *IEEE Internet of Things Journal*, pp. 1–1, 10.1109/JIOT.2020.3018691, 2020.

[27] R. Zhou, X. Zhang, X. Wang, G. Yang, H. Wang, and Y. Wu, "Privacy-preserving data search with fine-grained dynamic search right management in fog-assisted internet of things," *Information Sciences*, vol. 491, pp. 251 – 264, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025519302968

[28] Y. Ma, Y. Wu, and J. Ge, *Accountability and Privacy in Network Security*. Springer, 2020. [Online]. Available: https://doi.org/10.1007/978-981-15-6575-5

[29] H.-N. Dai, R. C.-W. Wong, H. Wang, Z. Zheng, and A. V. Vasilakos, "Big data analytics for large-scale wireless networks: Challenges and opportunities," *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, pp. 1–36, 2019.

[30] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Computer Communications*, vol. 155, pp. 66 – 83, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419318754

[31] H. He and H. Jiang, "Deep learning based energy efficiency optimization for distributed cooperative spectrum sensing," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 32–39, 2019.

[32] Y. Ma, X. Zhang, and Y. Gao, "Joint Sub-Nyquist Spectrum Sensing Scheme With Geolocation Database Over TV White Space," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3998–4007, 2018.

[33] M. Grissa, B. Hamdaoui, and A. A. Yavuz, "Location privacy in cognitive radio networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1726–1760, thirdquarter 2017.

[34] X. Li, J. Xu, H.-N. Dai, Q. Zhao, C. F. Cheang, and Q. Wang, "On modeling eavesdropping attacks in wireless networks," *Journal of Computational Science*, vol. 11, pp. 196–204, 2015.

[35] Z. Jiang, K. Zhao, R. Li, J. Zhao, and J. Du, "PHYAlert: identity spoofing attack detection and prevention for a wireless edge network," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–13, 2020.

[36] R. Ghannam, F. Sharevski, and A. Chung, "User-targeted Denial-of-Service Attacks in LTE Mobile Networks," in *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2018, pp. 1–8.

[37] X. An, X. Lü, L. Yang, X. Zhou, and F. Lin, "Node state monitoring scheme in fog radio access networks for intrusion detection," *IEEE Access*, vol. 7, pp. 21 879–21 888, 2019.

[38] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.

[39] 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, pp. 2512–2520.

[40] Y. Chen, Z. Ma, Q. Wang, J. Huang, X. Tian, and Q. Zhang, "Privacy-preserving spectrum auction design: Challenges, solutions, and research directions," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 142–150, October 2019.

[41] M. Pan, X. Zhu, and Y. Fang, "Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer," *Wireless Networks*, vol. 18, no. 2, pp. 113–128, 2012.

[42] Q. Lou and L. Jiang, "SHE: A fast and accurate deep neural network for encrypted data," in *Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019, NeurIPS 2019, 8-14 December 2019, Vancouver, BC, Canada*, 2019, pp. 10 035–10 043.

[43] R. Podschwadt and D. Takabi, "Classification of encrypted word embeddings using recurrent neural networks." in *PrivateNLP*, 2020, pp. 27–31.

[44] R. Rajkumari and N. Marchang, "Mitigating spectrum sensing data falsification attack in ad hoc cognitive radio networks," *International Journal of Communication Systems*, vol. 32, no. 2, p. e3852, 2019.

[45] A. A. Sharifi and M. J. Musevi Niya, "Defense against ssdf attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," *IEEE Communications Letters*, vol. 20, no. 1, pp. 93–96, 2016.

[46] M. Kulin, T. Kazaz, I. Moerman, and E. De Poorter, "End-to-End Learning From Spectrum Data: A Deep Learning Approach for Wireless Signal Identification in Spectrum Monitoring Applications," *IEEE Access*, vol. 6, pp. 18 484–18 501, 2018.

[47] R. Utrilla, E. Fonseca, A. Araujo, and L. A. Dasilva, "Gated recurrent unit neural networks for automatic modulation classification with resource-constrained end-devices," *IEEE Access*, vol. 8, pp. 112 783–112 794, 2020.

[48] J. Ngiam, A. Khosla, M. Kim, J. Nam, H. Lee, and A. Y. Ng, "Multimodal deep learning," in *Proceedings of the 28th International Conference on International Conference on Machine Learning (ICML)*, 2011, pp. 689–696.

[49] V. Radu, C. Tong, S. Bhattacharya, N. D. Lane, C. Mascolo, M. K. Marina, and F. Kawsar, "Multimodal deep learning for activity and context recognition," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 4, pp. 1–27, 2018.

[50] W. Elmasry, A. Akbulut, and A. H. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic," *Computer Networks*, vol. 168, p. 107042, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861930800X

[51] H. Choi, M. Kim, G. Lee, and W. Kim, "Unsupervised learning approach for network intrusion detection system using autoencoders," *The Journal of Supercomputing*, vol. 75, no. 9, pp. 5597–5621, 2019.

[52] J. Ran, Y. Ji, and B. Tang, "A semi-supervised learning approach to ieee 802.11 network anomaly detection," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1–5.

[53] A. Refaey, K. Hammad, S. Magierowski, and E. Hossain, "A blockchain policy and charging control framework for roaming in cellular networks," *IEEE Network*, vol. 34, no. 3, pp. 170–177, 2020.

[54] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "FDC: A Secure Federated Deep Learning Mechanism for Data Collaborations in the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6348–6359, 2020.

[55] T. Ryffel, D. Pointcheval, F. Bach, E. Dufour-Sans, and R. Gay, "Partially encrypted deep learning using functional

encryption," in *Advances in Neural Information Processing Systems 32*. Curran Associates, Inc., 2019, pp. 4517–4528. [Online]. Available: http://papers.nips.cc/paper/8701-partially-encrypted-deep-learning-using-functional-encryption.pdf

[56] K. Nandakumar, N. Ratha, S. Pankanti, and S. Halevi, "Towards deep neural network training on encrypted data," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, June 2019.

[57] E. Hesamifard, H. Takabi, and M. Ghasemi, "Deep neural networks classification over encrypted data," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 97–108. [Online]. Available: https://doi.org/10.1145/3292006.3300044

[58] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1963–1971, 2020.

[59] Y. Chen, Y. Zhang, S. Maharjan, M. Alam, and T. Wu, "Deep learning for secure mobile edge computing in cyber-physical transportation systems," *IEEE Network*, vol. 33, no. 4, pp. 36–41, 2019.

[60] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018.

[61] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Computer Networks*, vol. 148, pp. 164 – 175, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618303037

[62] Y. Zhou and L. Wang, "A lattice-based authentication scheme for roaming service in ubiquitous networks with anonymity," *Security and Communication Networks*, 10.1155/2020/2637916, 2020.

[63] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, "Securing internet of medical things with friendly-jamming schemes," *Computer Communications*, vol. 160, pp. 431 – 442, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366420310227

[64] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[65] Z. Ning, P. Dong, X. Wang, J. J. Rodrigues, and F. Xia, "Deep reinforcement learning for vehicular edge computing: An intelligent offloading system," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 6, pp. 1–24, 2019.

[66] K. Zhang, J. Long, X. Wang, H. Dai, K. Liang, and M. Imran, "Lightweight searchable encryption protocol for industrial internet of things," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 10.1109/TII.2020.3014168, 2020.

[67] V. K. Arthur Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, "Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage," *Journal of Network and Computer Applications*, vol. 129, pp. 25 – 36, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804519300037

[68] 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.

[69] N. J. Hernandez Marcano, M. Moller, S. Hansen, and R. H. Jacobsen, "On Fully Homomorphic Encryption for Privacy-Preserving Deep Learning," in *2019 IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.

[70] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, Jan. 2019. [Online]. Available: https://doi.org/10.1145/3298981

[71] C. Xu, H. Lin, Y. Wu, X. Guo, and W. Lin, "An SDNFV-Based DDoS Defense Technology for Smart Cities," *IEEE Access*, vol. 7, pp. 137 856–137 874, 2019.

[72] 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.

[73] H. Cao, A. Xiao, Y. Hu, P. Zhang, S. Wu, and L. Yang, "On virtual resource allocation of heterogeneous networks in virtualization environment: A service oriented perspective," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 10.1109/TNSE.2020.2972602, 2020.

[74] H. Huang, H. Yin, G. Min, H. Jiang, J. Zhang, and Y. Wu, "Data-driven information plane in software-defined networking," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 218–224, 2017.

[75] W. Miao, G. Min, Y. Wu, H. Wang, and J. Hu, "Performance modelling and analysis of software-defined networking under bursty multimedia traffic," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 12, no. 5s, Sep. 2016. [Online]. Available: https://doi.org/10.1145/2983637

[76] X. Cheng, Y. Wu, G. Min, and A. Y. Zomaya, "Network function virtualization in dynamic networks: A stochastic perspective," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2218–2232, 2018.

[77] W. Miao, G. Min, Y. Wu, H. Huang, Z. Zhao, H. Wang, and C. Luo, "Stochastic performance analysis of network function virtualization in future internet," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 613–626, 2019.

[78] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21 954–21 961, 2017.

[79] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, and M. Zhu, "Hast-ids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[80] O. Alkadi, N. Moustafa, B. Turnbull, and K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," *IEEE Internet of Things Journal*, pp. 1–1, 10.1109/JIOT.2020.2996590, 2020.

[81] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine," *IEEE Transactions on Cloud Computing*, pp. 1–1, 10.1109/TCC.2020.3001017, 2020.

[82] C. Liu, Y. Liu, Y. Yan, and J. Wang, "An intrusion detection model with hierarchical attention mechanism," *IEEE Access*, vol. 8, pp. 67 542–67 554, 2020.

[83] C. Xu, J. Shen, and X. Du, "A method of few-shot network intrusion detection based on meta-learning framework," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3540–3552, 2020.

[84] H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah, and T. Huang, "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 3, pp. 790–799, 2020.

[85] X. Jiang, M. Kim, K. Lauter, and Y. Song, "Secure outsourced matrix computation and application to neural networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1209–1222. [Online]. Available: https://doi.org/10.1145/3243734.3243837

[86] C. Juvekar, V. Vaikuntanathan, and A. Chandrakasan, "Gazelle: A low latency framework for secure neural network inference," in *Proceedings of the 27th USENIX Conference on Security Symposium*, ser. SEC'18. USA: USENIX Association, 2018, p. 1651–1668.

[87] B. D. Rouhani, M. S. Riazi, and F. Koushanfar, "Deepsecure: Scalable provably-secure deep learning," in *2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*, 2018, pp. 1–6.

[88] P. Mohassel and P. Rindal, "ABY^3: A mixed protocol framework for machine learning," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 35–52. [Online]. Available: https://doi.org/10.1145/3243734.3243760

[89] N. Papernot, M. Abadi, Ú. Erlingsson, I. J. Goodfellow, and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," in *5th International Conference on Learning Representations, ICLR 2017, Toulon, France, April 24-26, 2017, Conference Track Proceedings*, 2017. [Online]. Available: https://openreview.net/forum?id=HkwoSDPgg

[90] X. Ma, J. Ma, H. Li, Q. Jiang, and S. Gao, "Pdlm: Privacy-preserving deep learning model on cloud with multiple keys," *IEEE Transactions on Services Computing*, pp. 1–1, 2018.

[91] Y. Liu, J. J. Q. Yu, J. Kang, D. Niyato, and S. Zhang, "Privacy-preserving traffic flow prediction: A federated learning approach," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7751–7763, 2020.

[92] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational lstm enhanced anomaly detection for industrial big data," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 10.1109/TII.2020.3022432, 2020.

[93] X. Zhou, Y. Li, and W. Liang, "Cnn-rnn based intelligent recommendation for online medical pre-diagnosis support," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, pp. 1–1, 10.1109/TCBB.2020.2994780, 2020.

[94] H. Pang and B. Wang, "Privacy-preserving association rule mining using homomorphic encryption in a multikey environment," *IEEE Systems Journal*, pp. 1–11, 2020.

[95] M. Djatmiko, D. Schatzmann, X. Dimitropoulos, A. Friedman, and R. Boreli, "Collaborative network outage troubleshooting with secure multiparty computation," *IEEE Communications Magazine*, vol. 51, no. 11, pp. 78–84, 2013.

[96] W. Jung, S. Kwon, and K. Shim, "Tidy: Publishing a time interval dataset with differential privacy," *IEEE Transactions on Knowledge and Data Engineering*, pp. 1–1, 10.1109/TKDE.2019.2952351, 2019.

[97] Q. Chen, C. Qian, and S. Zhong, "Privacy-preserving cross-domain routing optimization - a cryptographic approach," in *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*, Nov 2015, pp. 356–365.

[98] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," *IEEE Access*, vol. 8, pp. 140 699–140 725, 2020.

[99] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 1310–1321. [Online]. Available: https://doi.org/10.1145/2810103.2813687

[100] R. Ramakrishnan and J. A. Shah, "Towards interpretable explanations for transfer learning in sequential tasks," in *2016 AAAI Spring Symposia, Stanford University, Palo Alto, California, USA, March 21-23, 2016*, 2016. [Online]. Available: http://www.aaai.org/ocs/index.php/SSS/SSS16/paper/view/12757

[101] X. Wang, J. He, P. Cheng, and J. Chen, "Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism," *IEEE Transactions on Signal Processing*, vol. 67, no. 1, pp. 221–233, Jan 2019.

[102] Z. Li, T. J. Oechtering, and D. Gündüz, "Privacy against a hypothesis testing adversary," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1567–1581, 2019.

[103] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5g: Survey and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, 2017.

[104] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. Leung, "Network slicing based 5g and future mobile networks: mobility, resource management, and challenges," *IEEE communications magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[105] S. Zhang, "An overview of network slicing for 5g," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019.

[106] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[107] P. Rost, A. Banchs, I. Berberana, M. Breitbach, M. Doll, H. Droste, C. Mannweiler, M. A. Puente, K. Samdanis, and B. Sayadi, "Mobile network architecture evolution toward 5g," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 84–91, 2016.

[108] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega *et al.*, "Network slicing to enable scalability and flexibility in 5g mobile networks," *IEEE Communications magazine*, vol. 55, no. 5, pp. 72–79, 2017.

[109] N. M. K. Chowdhury and R. Boutaba, "A survey of network virtualization," *Computer Networks*, vol. 54, no. 5, pp. 862–876, 2010.

[110] H. Wang, Y. Wu, G. Min, J. Xu, and P. Tang, "Data-driven dynamic resource scheduling for network slicing: A deep reinforcement learning approach," *Information Sciences*, vol. 498, pp. 106–116, 2019.

[111] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5g network slicing using sdn and nfv: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, p. 106984, 2020.

[112] K. D. Joshi and K. Kataoka, "psmart: A lightweight, privacy-aware service function chain orchestration in multi-domain nfv/sdn," *Computer Networks*, p. 107295, 2020.

[113] G. Sun, Y. Li, H. Yu, A. V. Vasilakos, X. Du, and M. Guizani, "Energy-efficient and traffic-aware service function chaining orchestration in multi-domain networks," *Future Generation Computer Systems*, vol. 91, pp. 347–360, 2019.

[114] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5g vehicle-to-everything services: Gearing up for security and privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, 2019.

[115] S. Zhang, Y. Wang, and W. Zhou, "Towards secure 5g networks: A survey," *Computer Networks*, vol. 162, p. 106871, 2019.

[116] P. Schneider, C. Mannweiler, and S. Kerboeuf, "Providing strong 5g mobile network slice isolation for highly sensitive third-party services," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.

[117] D. Eckhoff, F. Dressler, and C. Sommer, "Smartrevoc: An efficient and privacy preserving revocation system using parked vehicles," in *38th Annual IEEE Conference on Local Computer Networks*. IEEE, 2013, pp. 827–834.

[118] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2016.

[119] G. Sun, S. Sun, J. Sun, H. Yu, X. Du, and M. Guizani, "Security and privacy preservation in fog-based crowd sensing on the internet of vehicles," *Journal of Network and Computer Applications*, vol. 134, pp. 89–99, 2019.

[120] D. Servos and S. L. Osborn, "Current research and open problems in attribute-based access control," *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, pp. 1–45, 2017.

[121] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[122] M. Alohaly, H. Takabi, and E. Blanco, "A deep learning approach for extracting attributes of abac policies," in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, 2018, pp. 137–148.

[123] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5403–5415, 2020.

[124] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627–2637, 2017.

[125] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Multibiometric secure system based on deep learning," in *2017 IEEE Global conference on signal and information processing (globalSIP)*. IEEE, 2017, pp. 298–302.

[126] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li, "Deep learning-based gait recognition using smartphones in the wild," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3197–3212, 2020.

[127] O. Gireesha, N. Somu, K. Krithivasan, and S. S. VS, "Iivifs-waspas: an integrated multi-criteria decision-making perspective for cloud service provider selection," *Future Generation Computer Systems*, vol. 103, pp. 91–110, 2020.

[128] S. Zhang, L. Yao, A. Sun, and Y. Tay, "Deep learning based recommender system: A survey and new perspectives," *ACM Comput. Surv.*, vol. 52, no. 1, Feb. 2019. [Online]. Available: https://doi.org/10.1145/3285029

[129] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[130] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 1238–1246.

[131] J. López and S. Maag, "Towards a generic trust management framework using a machine-learning-based trust model," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 1343–1348.

[132] S. Tangade, S. S. Manvi, and S. Hassan, "A deep learning based driver classification and trust computation in vanets," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–6.

[133] Y. Ding and S. Zhu, "Malware detection based on deep learning algorithm," *Neural Computing and Applications*, vol. 31, no. 2, pp. 461–472, 2019.

[134] H. Rathore, S. Agarwal, S. K. Sahay, and M. Sewak, "Malware detection using machine learning and deep learning," in *International Conference on Big Data Analytics*. Springer, 2018, pp. 402–411.

[135] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, and S. Venkatraman, "Robust intelligent malware detection using deep learning," *IEEE Access*, vol. 7, pp. 46 717–46 738, 2019.

[136] C. Huang, Y. Wu, Y. Zuo, K. Pei, and G. Min, "Towards experienced anomaly detector through reinforcement learning," in *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, (AAAI-18), the 30th innovative Applications of Artificial Intelligence (IAAI-18), and the 8th AAAI Symposium on Educational Advances in Artificial Intelligence (EAAI-18), New Orleans, Louisiana, USA, February 2-7, 2018*, S. A. McIlraith and K. Q. Weinberger, Eds. AAAI Press, 2018, pp. 8087–8088. [Online]. Available: https://www.aaai.org/ocs/index.php/AAAI/AAAI18/paper/view/16048

[137] M. G. Schultz, E. Eskin, F. Zadok, and S. J. Stolfo, "Data mining methods for detection of new malicious executables," in *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001*. IEEE, 2000, pp. 38–49.

[138] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*. IEEE, 2016, pp. 581–585.

[139] W. Hardy, L. Chen, S. Hou, Y. Ye, and X. Li, "DL4MD: A deep learning framework for intelligent malware detection," in *Proceedings of the International Conference on Data Mining (DMIN)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016, p. 61.

[140] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE transactions on emerging topics in computational intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[141] G. Wang, Y. Zhao, J. Huang, and Y. Wu, "An effective approach to controller placement in software defined wide area networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 344–355, 2018.

[142] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Multi-layered intrusion detection and prevention in the sdn/nfv enabled cloud of 5g networks using ai-based defense mechanisms," *Computer Networks*, vol. 179, p. 107364, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619310205

[143] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on sdn based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2019.

[144] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 2016, pp. 258–263.

[145] Q. Niyaz, W. Sun, and A. Y. Javaid, "A deep learning based ddos detection system in software-defined networking (sdn)," *EAI Endorsed Transactions on Security and Safety*, vol. 4, no. 12, 2017.

[146] R. Braga, E. Mota, and A. Passito, "Lightweight ddos flooding attack detection using nox/openflow," in *IEEE Local Computer Network Conference*. IEEE, 2010, pp. 408–415.

[147] T. Kohonen, "The self-organizing map," *Proceedings of the IEEE*, vol. 78, no. 9, pp. 1464–1480, 1990.

[148] H. Chergui and C. Verikoukis, "Big data for 5g intelligent network slicing management," *IEEE Network*, vol. 34, no. 4, pp. 56–61, 2020.

[149] V. P. Kafle, P. Martinez-Julia, and T. Miyazawa, "Automation of 5g network slice control functions with machine learning," *IEEE Communications Standards Magazine*, vol. 3, no. 3, pp. 54–62, 2019.

[150] R. Li, Z. Zhao, X. Zhou, G. Ding, Y. Chen, Z. Wang, and H. Zhang, "Intelligent 5g: When cellular networks meet artificial intelligence," *IEEE Wireless communications*, vol. 24, no. 5, pp. 175–183, 2017.

[151] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98–105, 2016.

[152] N. Phan, Y. Wang, X. Wu, and D. Dou, "Differential privacy preservation for deep auto-encoders: an application of human behavior prediction," in *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, 2016, pp. 1309–1316.

[153] 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.

[154] 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*, 2016, pp. 308–318.

[155] J. Wang, J. Zhang, W. Bao, X. Zhu, B. Cao, and P. S. Yu, "Not just privacy: Improving performance of private deep learning in mobile cloud," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2018, pp. 2407–2416.

[156] M. Abadi and D. G. Andersen, "Learning to protect communications with adversarial neural cryptography," *arXiv preprint arXiv:1610.06918*, 2016.

[157] E. P. Xing, Q. Ho, W. Dai, J. K. Kim, J. Wei, S. Lee, X. Zheng, P. Xie, A. Kumar, and Y. Yu, "Petuum: A new platform for distributed machine learning on big data," *IEEE Transactions on Big Data*, vol. 1, no. 2, pp. 49–67, 2015.

[158] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "When edge meets learning: Adaptive control for resource-constrained distributed machine learning," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2018, pp. 63–71.

[159] M. Li, D. G. Andersen, J. W. Park, A. J. Smola, A. Ahmed, V. Josifovski, J. Long, E. J. Shekita, and B.-Y. Su, "Scaling distributed machine learning with the parameter server," in *11th USENIX Symposium on Operating Systems Design and Implementation (OSDI 14)*. Broomfield, CO: USENIX Association, Oct. 2014, pp. 583–598. [Online]. Available: https://www.usenix.org/conference/osdi14/technical-sessions/presentation/li_mu

[160] X. Cai, X. Mo, J. Chen, and J. Xu, "D2d-enabled data sharing for distributed machine learning at wireless network edge," *IEEE Wireless Communications Letters*, vol. 9, no. 9, pp. 1457–1461, 2020.

[161] C. Chen, Z. Liu, P. Zhao, J. Zhou, and X. Li, "Privacy preserving point-of-interest recommendation using decentralized matrix factorization," 2020.

[162] C. Chen, J. Zhou, B. Wu, W. Fang, L. Wang, Y. Qi, and X. Zheng, "Practical privacy preserving poi recommendation," *ACM Trans. Intell. Syst. Technol.*, vol. 11, no. 5, Jul. 2020. [Online]. Available: https://doi.org/10.1145/3394138

[163] S. R. Pokhrel, "Towards efficient and reliable federated learning using blockchain for autonomous vehicles," *Computer Networks*, p. 107431, 2020.

[164] N. H. Tran, W. Bao, A. Zomaya, N. M. NH, and C. S. Hong, "Federated learning over wireless networks: Optimization model design and analysis," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 1387–1395.

[165] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," ser. Proceedings of Machine Learning Research, A. Singh and J. Zhu, Eds., vol. 54. Fort Lauderdale, FL, USA: PMLR, 20–22 Apr 2017, pp. 1273–1282. [Online]. Available: http://proceedings.mlr.press/v54/mcmahan17a.html

[166] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, 2020.

Yulei Wu is a Senior Lecturer with the Department of Computer Science, College of Engineering, Mathematics and Physical Sciences, University of Exeter, United Kingdom. He received the B.Sc. degree (First Class Honours) in Computer Science and the Ph.D. degree in Computing and Mathematics from the University of Bradford, United Kingdom, in 2006 and 2010, respectively. His expertise is on intelligent networking and his main research interests include computer networks, networked systems, software defined networks and systems, network management, and network security and privacy. He is an Editor of IEEE Transactions on Network and Service Management, IEEE Transactions on Network Science and Engineering, Computer Networks (Elsevier) and IEEE Access. He is a Senior Member of the IEEE, and a Fellow of the HEA (Higher Education Academy).

Yuxiang Ma is currently an Associate Professor in the School of Computer and Information Engineering at Henan University. He received the B.S. degree from Henan University in 2013, and the Ph.D. degree from the Computer Network Information Center, Chinese Academy of Sciences in 2019. His main research interests include future Internet architecture and technologies, network security, and privacy enhancement technologies.

Hong-Ning Dai is currently with Faculty of Information Technology at Macau University of Science and Technology as an Associate Professor. He obtained the Ph.D. degree in Computer Science and Engineering from Department of Computer Science and Engineering at the Chinese University of Hong Kong. His current research interests include Internet of Things, big data analytics and blockchain technology. He has served as associate editors/editors of IEEE Systems Journal, IEEE Access, Connection Science, and Ad Hoc Networks, guest editors for IEEE Transactions on Industrial Informatics, IEEE Transactions on Emerging Topics in Computing. He is a senior member of the IEEE and a senior member of ACM.

Hao Wang is an Associate Professor in the Department of Computer Science in Norwegian University of Science and Technology, Norway. He has a Ph.D. degree and a B.Eng. degree, both in computer science and engineering, from South China University of Technology. His research interests include big data analytics, industrial internet of things, high performance computing, and safety-critical systems. He served as a TPC co-chair for IEEE DataCom 2015, IEEE CIT 2017, ES 2017, and IEEE CPSCom 2020, a senior TPC member for CIKM 2019, and reviewers/TPC members for many journals and conferences. He is the Chair for Sub TC on Healthcare in IEEE IES Technical Committee on Industrial Informatics. He is a member of the IEEE and ACM.