#### **REVIEW**



# Deep learning: systematic review, models, challenges, and research directions

Tala Talaei Khoei<sup>1</sup> • Hadjar Ould Slimane<sup>1</sup> • Naima Kaabouch<sup>1</sup>

Received: 31 May 2023 / Accepted: 15 August 2023 © The Author(s) 2023

#### **Abstract**

The current development in deep learning is witnessing an exponential transition into automation applications. This automation transition can provide a promising framework for higher performance and lower complexity. This ongoing transition undergoes several rapid changes, resulting in the processing of the data by several studies, while it may lead to time-consuming and costly models. Thus, to address these challenges, several studies have been conducted to investigate deep learning techniques; however, they mostly focused on specific learning approaches, such as supervised deep learning. In addition, these studies did not comprehensively investigate other deep learning techniques, such as deep unsupervised and deep reinforcement learning techniques. Moreover, the majority of these studies neglect to discuss some main methodologies in deep learning, such as transfer learning, federated learning, and online learning. Therefore, motivated by the limitations of the existing studies, this study summarizes the deep learning techniques into supervised, unsupervised, reinforcement, and hybrid learning-based models. In addition to address each category, a brief description of these categories and their models is provided. Some of the critical topics in deep learning, namely, transfer, federated, and online learning models, are explored and discussed in detail. Finally, challenges and future directions are outlined to provide wider outlooks for future researchers.

**Keywords** Artificial intelligence · Neural networks · Deep learning · Supervised learning · Unsupervised learning · Reinforcement learning · Online learning · Federated learning · Transfer learning

#### 1 Introduction

The main concept of artificial neural networks (ANN) was proposed and introduced as a mathematical model of an artificial neuron in 1943 [1–3]. In 2006, the concept of deep learning (DL) was proposed as an ANN model with several layers, which has significant learning capacity. In recent years, DL models have seen tremendous progress in addressing and solving challenges, such as anomaly detection, object detection, disease diagnosis, semantic segmentation, social network analysis, and video recommendations [4–7].

Several studies have been conducted to discuss and investigate the importance of the DL models in different

Published online: 07 September 2023

applications, as illustrated in Table 1. For instance, the authors of [8] reviewed supervised, unsupervised, and reinforcement DL-based models. In [9], the authors outlined DL-based models, platforms, applications, and future directions. Another survey [10] provided a comprehensive review of the existing models in the literature in different applications, such as natural processing, social network analysis, and audio. In this study, the authors provided a recent advancement in DL applications and elaborated on some of the existing challenges faced by these applications. In [11], the authors highlighted different DL-based models, such as deep neural networks, convolutional neural networks, recurrent neural networks, and auto-encoders. They also covered their frameworks, benchmarks, and software development requirements. In [12], the authors discussed the main concepts of deep learning and neural networks. They also provided several applications of DL in a variety of areas.



<sup>☐</sup> Tala Talaei Khoei tala.talaeikhoei@und.edu

School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, ND 58202, USA

Other studies covered particular challenges of DL models. For instance, the authors of [13] explored the importance of class imbalanced dataset on the performance of the DL models as well as the strengths and weaknesses of the methods proposed in the literature for solving class imbalanced data. Another study [14] explored the challenges that DL faces in the case of data mining, big data, and information processing due to huge volume of data, velocity, and variety. In [15], the authors analyzed the complexity of DL-based models and provided a review of the existing studies on this topic. In [16], the authors focused on the activation functions of DL. They introduced these functions as a strategy in DL to transfer nonlinearly separable input into the more linearly separable data by applying a hierarchy of layers, whereas they provided the most common activation functions and their characteristics.

In [17], the authors outlined the applications of DL in cybersecurity. They provided a comprehensive literature review of DL models in this field and discussed different types of DL models, such as convolutional neural networks, auto-encoders, and generative adversarial networks. They also covered the applications of different attack categories, such as malware, spam, insider threats, network intrusions, false data injection, and malicious in DL. In another study [18], the authors focused on detecting tiny objects using DL. They analyzed the performance of different DL in detecting these objects. In [19], the authors reviewed DL models in the building and construction industry-based applications while they discussed several important key factors of using DL models in manufacturing and construction, such as progress monitoring and automation systems. Another study [20] focused on using different strategies in the domain of artificial intelligence (AI), including DL in smart grids. In such a study, the authors introduced the main AI applications in smart grids while exploring different DL models in depth. In [7], the authors discussed the current progress of DL in medical areas and gave clear definitions of DL models and their theoretical concepts and architectures. In [21], the authors analyzed the DL applications in biology, medicine, and engineering domains. They also provided an overview of this field of study and major DL applications and illustrated the main characteristics of several frameworks, including molecular shuttles.

Despite the existing surveys in the field of DL focusing on a comprehensive overview of these techniques in different domains, the increasing amount of these applications and the existing limitations in the current studies motivated us to investigate this topic in depth. In general, the recent studies in the literature mostly discussed specific learning strategies, such as supervised models, while they did not cover different learning strategies and compare them with each other. In addition, the majority of the existing surveys

excluded new strategies, such as online learning or federated learning, from their studies. Moreover, these surveys mostly explored specific applications in DL, such as the Internet of Things, smart grid, or constructions; however, this field of study requires formulation and generalization in different applications. In fact, limited information, discussions, and investigations in this domain may lead to prevent any development and progress in DL-based applications. To fill these gaps, this paper provides a comprehensive survey on four types of DL models, namely, supervised, unsupervised, reinforcement, and hybrid learning. It also provides the major DL models in each category and describes the main learning strategies, such as online, transfer, and federated learning. Finally, a detailed discussion of future direction and challenges is provided to support future studies. In short, the main contributions of this paper are as follows:

- Classifications and in-depth descriptions of supervised, unsupervised, enforcement, and hybrid models.
   Description and discussion of learning strategies, such as online, federated, and transfer learning,
- Comparison of different classes of learning strategies, their advantages, and disadvantages,
- Current challenges and future directions in the domain of deep learning.

The remainder of this paper is organized as follows: Sect. 2 provides descriptions of the supervised, unsupervised, reinforcement, and hybrid learning models, along with a brief description of the models in each category. Section 3 highlights the main learning approaches that are used in deep learning. Section 4 discusses the challenges and future directions in the field of deep learning. The conclusion is summarized in Sect. 5.

# 2 Categories of deep learning models

DL models can be classified into four categories, namely, deep supervised, unsupervised, reinforcement learning, and hybrid models. Figure 1 depicts the main categories of DL along with examples of models in each category. In the following, short descriptions of these categories are provided. In addition, Table 2 provides the most common techniques in every category.

#### 2.1 Deep supervised learning

Deep supervised learning-based models are one of the main categories of deep learning models that use a labeled training dataset to be trained. These models measure the accuracy through a function, loss function, and adjust the weights till the error has been minimized sufficiently.



Table 1 Summary of related works

References	Topics	Concepts covered	Concepts not covered
[8]	General DL	Studies different DL categories, namely, supervised, unsupervised, and reinforcement learning	Different models in DL categories, Applications of these DL models
[9]	General DL	Reviews of supervised, unsupervised, and reinforcement learning models, Detailed discussions of DL applications and future directions	Lack of comprehensive analysis of different DL models
[10] G	General DL	Studies DL algorithms, applications, and relevant techniques	Limited investigation on unsupervised and reinforcement models.
			Lack of investigation on the different architecture of DL models
[11]	General DL	A short review of supervised, unsupervised, and reinforcement learning models, Comprehensive analysis of current studies on DL architecture	Lack of discussion on analysis and different DL models in different categories
[12]	General DL	Compares the differences between DL, classical ML, and other conventional learning approaches,  Discusses different applications of DL	No discussion on supervised, unsupervised, and reinforcement learning models
[13]	Class balancing	Investigates DL techniques in domain of class balancing	Limited discussions in different DL models,
			Lack of discussions of DL in the presence of class balancing
[14]	Big data	Analyzes the emerging research directions in the field of big data, Discusses the challenges in big data and future directions	Limited discussions of different DL models
[15]	Model complexity	Discusses the complexity of DL models	No analysis of supervised, unsupervised, and reinforcement learning models,
			No discussion of the future directions of different DL models,
			No investigations of different DL applications
[16]	Activation function	Explores of different activation functions in DL models	Lack of discussions of different DL models,
			No investigations into the DL models' architecture or different applications
[17]	Cybersecurity	Investigates different DL techniques in the domain of cybersecurity	No discussion of DL in other domains,
			No discussion of reinforcement or unsupervised models,
F103	m: 1: .		No discussion of different features in DL
[18]	Tiny objects	Investigates tiny object detection techniques in the field of DL,  Discusses the 12 popular datasets for tiny objects and evaluates the current techniques	Limited discussion of other possible DL techniques in aspects of tiny objects
[19]	Building and construction		Not focusing only on DL techniques,
			Limited discussions of various DL models,
			Limited investigations on different functions of DL techniques
[20]	Smart grid	forecasting, power grid stability, and fault detection.	Not detailed descriptions of DL techniques in domain of smart grid,
		Future direction in domain of smart grid applying AI techniques	Limited focuses on DL models and different architectures
[7]	Medicine	Investigating DL models along with the literature review in medicine, In-depth analysis of DL models and their literature review	Lack of investigations of DL models in other fields of study,
			Limited descriptions of different DL models



Table 1 (continued)

References	Topics	Concepts covered	Concepts not covered
[21]	Medicine	Provides emerging technology in the field of DL models in medicine.  Presents literature review of DL techniques in medicine	Limited discussions of reinforcement or unsupervised learning.  Lack of descriptions of any DL models

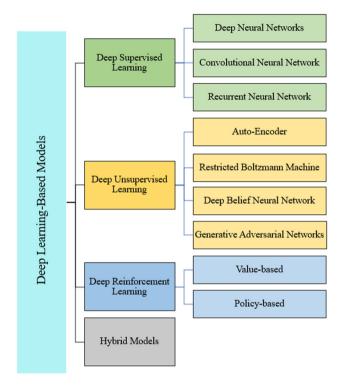
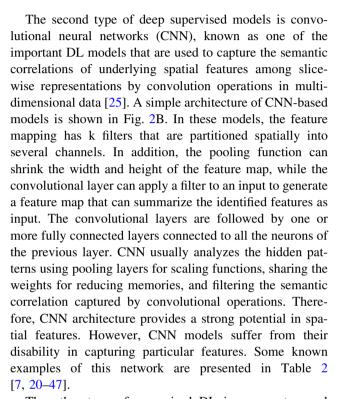


Fig. 1 Schematic review of the models in deep learning

Among the supervised deep learning category, three important models are identified, namely, deep neural networks, convolutional neural networks, and recurrent neural network-based models, as illustrated in Fig. 2. Artificial neural networks (ANN), known as neural networks or neural nets, are one of the computing systems, which are inspired by biological neural networks. ANN models are a collection of connected nodes (artificial neurons) that model the neurons in a biological brain. One of the simple ANN models is known as a deep neural network (DNN) [22–29]. DNN models consist of a hierarchical architecture with input, output, and hidden layers, each of which has a nonlinear information processing unit, as illustrated in Fig. 2A. DNN, using the architecture of neural networks, consists of functions with higher complexity when the number of layers and units in a layer is increased. Some known instances of DNN models, as highlighted in Table 2, are multi-layer perceptron, shallow neural network, operational neural network, self-operational neural network, and iterative residual blocks neural network.



The other type of supervised DL is recurrent neural network (RNN) models, which are designed for sequential time-series data where the output is returned to the input, as shown in Fig. 2C [27]. RNN-based models are widely used to memorize the previous inputs and handle the sequential data and existing inputs [42]. In RNN models, the recursive process has hidden layers with loops that indicate effective information about the previous states. In traditional neural networks, the given inputs and outputs are totally independent of one another, whereas the recurrent layers of RNN have a memory that remembers the whole data about what is exactly calculated [48]. In fact, in RNN, similar parameters for every input are applied to construct the neural network and estimate the outputs. The critical principle of RNN-based models is to model time collection samples; hence, specific patterns can be estimated to be dependent on previous ones [48-64]. Table 2 provides the instances of RNN-based models as simple recurrent neural network, long short-term memory, gated recurrent unit neural network, bidirectional gated recurrent unit neural



**Table 2** Summary of deep learning models [22–74]

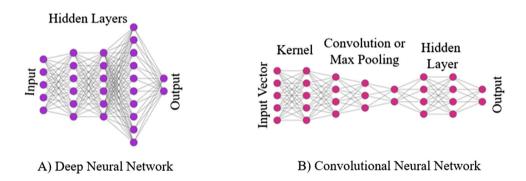
Learning methodology	Category	Model
Supervised learning	Deep neural networks	Multi-layer perceptron
		Shallow neural network
		Operational neural network
		Self-operational neural network
		Iterative residual blocks neural network
	Convolutional neural networks	Simple convolutional neural network
		Faster R convolutional neural network
		Alex neural network
		Residual neural network
		Densely connected neural network
		Le neural network
		Google neural network
		Inception neural network
		Visual geometry neural network
		Efficient neural network
	Recurrent neural networks	Simple recurrent neural network
		Long short-term memory
		Gated recurrent unit neural network
		Bidirectional gated recurrent unit neural network
		Bidirectional long short-term memory
		Residual gated recurrent neural network
Unsupervised learning	Auto-encoders	Stacked auto-encoder
		Variational auto-encoder
		Convolutional auto-encoder
	Restricted Boltzmann machine	Shallow restricted Boltzmann machine
		Convolutional restricted Boltzmann machine
	Deep belief neural networks	Simple deep belief neural networks
		Conditional deep belief neural networks
	Generative adversarial networks	Generative adversarial networks
		Signal augmented self-taught learning
		Wasserstein generative adversarial networks
Reinforcement learning	Value-based	Deep Q learning
		Double deep Q learning
		Duel deep Q learning
	Policy gradient-based	Deep deterministic policy gradient
		Asynchronous advantage actor critic
	Model-based	Imagination-augmented agents
		Model-based priors for model-free
		Model-based value expansion
Hybrid learning	DRL	Convolutional neural network-deep Q-learning
, ,		Long short-term memory-deep reinforcement learning
		Policy dynamics-based win
		Deep Q-learning-PG
	Unsupervised DL	Auto-encoder-long short-term memory
		Gated recurrent neural network-convolutional neural network
		C Long short-term memory-auto-encoder
		ACWGAN-GP

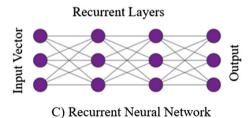


		/	11
Ian	י בו	(continu	1001

Learning methodology	Category	Model C-hybrid-generative adversarial networks
		Joint latent-variational auto-encoder
	Supervised DL	dLASSO-multi-layer perceptron
		Convolutional neural network-deep neural network
		Convolutional neural network-long short-term memory
		Convolutional neural network-constrained naive
		WaferSegClassNet
		Spiking-auto-encoder
		Deep belief neural networks-bidirectional-recurrent neural network
		SES-convolutional neural network
		Recurrent neural network-long short-term memory
		Convolutional neural network-recurrent neural network
		GoogleNet-AlexNet

Fig. 2 Inner architecture of deep supervised models





network, bidirectional long short-term memory, and residual gated recurrent neural network [64–66]. Table 3 shows the advantages and disadvantages of supervised DL models.

# 3 Deep unsupervised learning

Deep unsupervised models have gained significant interest as a mainstream of viable deep learning models. These models are widely used to generate systems that can be trained with few numbers of unlabeled samples [24]. The models can be classified into auto-encoders, restricted

Boltzmann machine, deep belief neural networks, and generative adversarial networks. An auto-encoder (AE) is a type of auto-associative feed-forward neural network that can learn effective representations from the given input in an unsupervised manner [29]. Figure 3A provides a basic architecture of AE. As it can be seen, there are three elements in AE, encoder, latent space, and decoder. Initially, the corresponding input passes through the encoder. The encoder is mostly a fully connected ANN that is able to generate the code. In contrast, the decoder generates the outputs using the codes and has an architecture similar to ANN. The aim of having an encoder and decoder is to present an identical output with the given input. It is



Table 3 Advantages and disadvantages of deep supervised learning techniques

Learning methodology	Category	Advantage	Disadvantage
Deep supervised learning	Deep neural networks	Tendency to high nonlinear relationships, Easy to develop	Slow learning, Hard for parameter tuning,
			Insufficient for high- dimensional input space
	Convolutional neural network	Ability to capture spatial correlations, high potentiality at generalization	Difficult parameter tuning, High computational cost
	Recurrent neural network	Sometimes fast converge with minimum parameters, improve the vanishing gradient issues	Difficult parameter tuning, Poor spatial feature representations

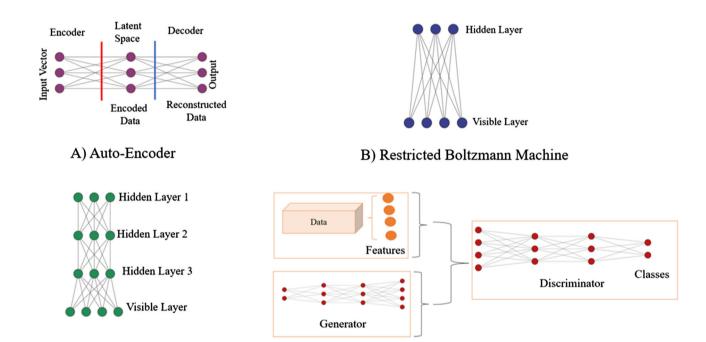


Fig. 3 Inner architecture of deep unsupervised models

C) Deep Belief Neural Network

notable that the dimensionality of the input and output has to be similar. Additionally, real-world data usually suffer from redundancy and high dimensionality, resulting in lower computational efficiency and hindering the modeling of the representation. Thus, a latent space can address this issue by representing compressed data and learning the features of the data, and facilitating data representations to find patterns. As shown in Table 2, AE consists of several known models, namely, stacked, variational, and convolutional AEs [30, 43]. The advantages and disadvantages of these models are presented in Table 4.

The restricted Boltzmann machine (RBM) model, known as Gibbs distribution, is a network of neurons that are connected to each other, as shown in Fig. 3B. In RBM,

the network consists of two layers, namely, the input or visible layer and the hidden layer. There is no output layer in RBM, while the Boltzmann machines are random and generative neural networks that can solve combinative problems. Some common RBM are presented in Table 2 as shallow restricted Boltzmann machines and convolutional restricted Boltzmann machines. The deep belief network (DBN) is another unsupervised deep neural network that performs in a similar way as the deep feed-forward neural network with inputs and multiple computational layers, known as hidden layers, as illustrated in Fig. 3C. In DBM, there are two main phases that are necessary to be performed, pre-train and fine-tuning phases. The pre-train phase consists of several hidden layers; however, fine-

D) Generative Adversarial Network



Table 4 Advantages and disadvantages of deep unsupervised learning techniques

Learning methodology	Category	Advantages	Disadvantages
Deep unsupervised	Auto-encoder	processes,	Difficult to tune parameters,
learning			Long processing time,
			Training can suffer from vanishing the errors
	Restricted Boltzmann	Learn complicated probability distributions,	Low robustness for noisy data,
	machine	Strong representation capability	Limited applications due to binary units
	Deep belief neural network	High efficiency for feature extractions, Unsupervised training	Unable to process multi-dimensional data,
			Slow and inefficient training
	Generative adversarial	Trains only using backpropagations,	Density estimation,
	network	Operates with small supervisions,	Unstable training process,
		Computational efficiency	Non-convergence

tuning phase only is considered a feed-forward neural network to train and classify the data. In addition, DBN has multiple layers with values, while there is a relation between layers but not with the values [31]. Table 2 reviews some of the known DBN models, namely, shallow deep belief neural networks and conditional deep belief neural networks [44, 45].

The generative adversarial network (GAN) is an another type of unsupervised deep learning model that uses a generator network (GN) and discriminator network (DN) to generate synthetic data to follow similar distribution from the original data, as presented in Fig. 3D. In this context, the GN mimics the distribution of the given data using noise vectors to exhaust the DN to classify between fake and real samples. The DN can be trained to differentiate between fake and real samples by the GN from the original samples. In general, the GN learns to create plausible data, whereas the DN can learn to identify the generator's fake data from the real ones. Additionally, the discriminator can penalize the generator for generating implausible data [32, 54]. The known types of GAN are presented in Table 2 as generative adversarial networks, signal augmented selftaught learning, and Wasserstein generative adversarial networks. As a result of this discussion, Table 4 provides the main advantages and disadvantages of the unsupervised DL categories [56].

# 3.1 Deep reinforcement learning

Reinforcement learning (RL) is the science of making decisions with learning the optimal behavior in an environment to achieve maximum reward. The optimal behavior is achieved through interactions with the environment. In RL, an agent can make decisions, monitor the

results, and adjust its technique to provide optimal policy [75, 76]. In particular, RL is applied to assist an agent in learning the optimal policy when the agent has no information about the surrounding environments. Initially, the agent monitors the current state, takes action, and receives its reward with its new state. In this context, the immediate reward and new state can adjust the agent's policy; This process is repeated till the agent's policy is getting close to the optimal policy. To be precise, RL does not need any detailed mathematical model for the system to guarantee optimal control [77]; however, the agent considers the target system as the environment and optimizes the control policy by communicating with it. The agent performs specific steps. During every step, the agent selects an action based on its existing policy, and the environment feeds back a reward and goes to the next state [78-80]. This process is learned by the agent to adjust its policy by referencing the relationships during the state, action, and rewards. The RL agent also can determine an optimal policy related to the maximum cumulative reward. In addition, an RL agent can be modeled as Markov decision process (MDP) [78]. In MDP, when the states and action spaces are finite, the process is known as finite. As it is clear, the RL learning approach may take a huge amount of time to achieve the best policy and discover the knowledge of a whole system; hence, RL is inappropriate for largescale networks [81].

In the past few years, deep reinforcement learning (DRL) was proposed as an advanced model of RL in which DL is applied as an effective tool to enhance the learning rate for RL models. The achieved experiences are stored during the real-time learning process, whereas the generated data for training and validating neural networks are applied [82]. In this context, the trained neural network has



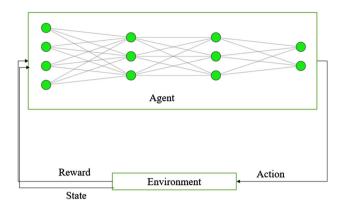


Fig. 4 Inner architecture of deep reinforcement learning

to be used to assist the agent in making optimal decisions in real-time scenarios. DRL overcomes the main shortcomings of RL, such as long processing time to achieve optimal policy, thus opening a new horizon to embrace the DRL [83]. In general, as shown in Fig. 4, DRL uses the deep neural networks' characteristics to train the learning process, resulting in increasing the speed and improving the algorithms' performance. In DRL, within the environment or agent interactions, the deep neural networks keep the internal policy of the agent, which indicates the next action according to the current state of the environment.

DRL can be divided into three methods, value-based, policy-based, and model-based methods. Value-based DRL mainly represents and finds the value functions and their optimal ones. In such methods, the agent learns the state or state-action value and behaves based on the best action in the state. One necessary step of these methods is to explore the environment. Some known instances of value-based DRL are deep Q-learning, double deep Q-learning, and duel deep Q-learning [83–85]. On the contrary, policy-based DRL finds an optimal policy, stochastic or deterministic, to better convergence on high-dimensional or continuous action space. These methods are mainly optimization techniques in which the maximum policy of function can be found. Some examples of policy-based

DRL are deep deterministic policy gradient and asynchronous advantage actor critic [86]. The third category of DRL, model-based methods, aims at learning the functionality of the environment and its dynamics from its previous observations, while these methods attempt a solution using the specific model. For these methods, in the case of having a model, they find the best policy to be efficient, while the process may fail when the state space is huge. In model-based DRL, the model is often updated, and the process is replanned. Instances of model-based DRL are imagination-augmented agents, model-based priors for model-free, and model-based value expansion. Table 5 illustrates the important advantages and disadvantages of these categories [87–89].

# 3.2 Hybrid deep learning

Deep learning models have weaknesses and strengths in terms of hyperparameter tuning settings and data explorations [45]. Therefore, the highlighted weakness of these models can hinder them from being strong techniques in different applications. Every DL model also has characteristics that make it efficient for specific applications; hence, to overcome these shortcomings, hybrid DL models have been proposed based on individual DL models to tackle the shortcomings of specific applications [79–89]. Figure 5 indicates the popular hybrid DL models that are used in the literature. It is observed that convolutional neural networks and recurrent neural networks are widely used in existing studies and have high applicability and potentiality compared to other developed DL models.

#### 4 Evaluation metrics

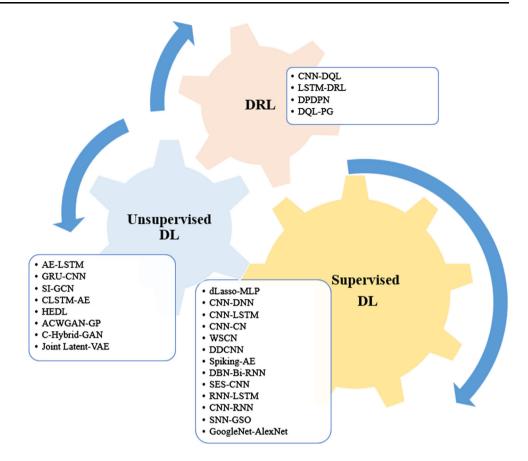
In any classification tasks, the metrics are required to evaluate the DL models. It is worth mentioning that various metrics can be used in different fields of studies. It means that the metrics which are used in medical analysis are

Table 5 Advantage and disadvantages of deep reinforcement learning techniques

Category	Used models	Advantage	Disadvantage
Deep reinforcement learning	Value- based	Less computational cost Relatively fast Learns directly the optimal policy	High variance per-sample  Not efficient for offline learning
	Policy- based	Able to find the best stochastic policy Efficient for high-dimensional dataset	High variance Slow convergence
	Model- based	Number of the interactions between the agent and the environment	Model accuracy has a huge impact on learning tasks High dependence on the transitional models



**Fig. 5** Review of popular hybrid models



mostly different with other domains, such as cybersecurity or computer visions. For this reason, we provide a short descriptions and a mathematical equations of the most common metrics in different domains, as following:

Accuracy: It is mainly used in classification problems to indicate the correct predictions made by a DL model. This metric is calculated, as shown in Eq. (1), where T<sub>P</sub> is the true positive, T<sub>N</sub> is true negative, F<sub>P</sub> is the false positive, and F<sub>N</sub> is the false negative.

$$Accuracy = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \times 100 \tag{1}$$

 Precision: It refers to the number of the true positives divided by the total number of the positive predictions, including true positive and false positive. This metric can be measured as following:

$$Precision = \frac{T_{P}}{T_{P} + F_{P}} \times 100 \tag{2}$$

• *Recall* (detection rate): It measures the number of the positive samples that are classified correctly to the total number of the positive samples. This metric, as measuring in Eq. (3), can indicate the model's ability to classify positive samples among other samples.

$$Recall = \frac{T_{P}}{T_{P} + F_{N}} \times 100 \tag{3}$$

• *F1-Score*: It is calculated from the precision and recall of the test, where the precision is defined as Eq. (2), and recall is presented in Eq. (3). This metric is calculated as shown in Eq. (4):

F1 - Score = 
$$\frac{2T_{\rm P}}{2T_{\rm P} + F_{\rm p} + F_{\rm N}} \times 100$$
 (4)

• Area under the receiver operating characteristics curve (AUC): AUC is one of the important metrics in classification problems. Receiver operating characteristic (ROC) helps to visualize the tradeoff between sensitivity and specificity in DL models. The AUC curve is a plot of true-positive rate (TPR) to false-positive rate (FPR). A good DL model has an AUC value near to 1. This metric is measured, as shown in Eq. (5), where x is the varying AUC parameter.

Area Under Curve 
$$= \int_{x=0}^{1} \frac{T_{P}}{T_{P} + F_{N}} \left( \left( \frac{F_{P}}{F_{P} + T_{N}} \right)^{-1} (x) \right) dx$$
(5)

 False Alarm Rate: This metric is also known as falsepositive rate, which is the probability of a false alarm



will be raised. It means, a positive result will be given when a true value is negative. This metric can be measured as shown in Eq. (6):

• Misdetection Rate: It is a metric that shows the percentage of misclassified samples. This metric can be defined as the percentage of the samples that are not detected. It is also measured, as shown in Eq. (7):

$$\text{Misdetection Rate} = \frac{F_{\text{N}}}{T_{\text{P}} + F_{\text{N}}} \times 100 \tag{7}$$

# 5 Learning classification in deep learning models

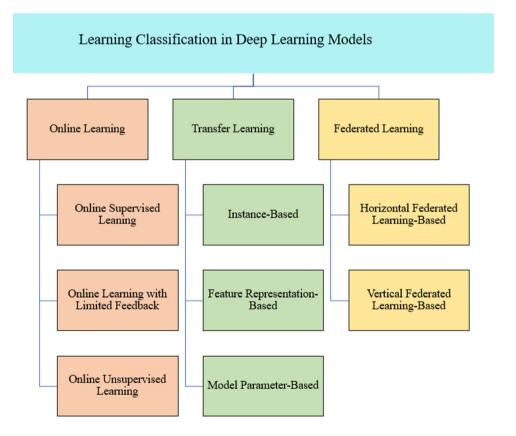
Learning strategies, as shown in Fig. 6, include online learning, transfer learning, and federated learning. In this section, these learning strategies are discussed in brief.

#### 5.1 Online learning

Conventional machine learning models mostly employ batch learning methods, in which a collection of training data is provided in advance to the model. This learning method requires the whole training dataset to be made accessible ahead to the training, which lead to high memory usage and poor scalability. On the other hand, online learning is a machine learning category where data are processed in sequential order, and the model is updated accordingly [90]. The purpose of online learning is to maximize the accuracy of the prediction model using the ground truth of previous predictions [91]. Unlike batch or offline machine learning approaches, which require the complete training dataset to be available to be trained on [92], online learning models use sequential stream of data to update their parameters after each data instance. Online learning is mainly optimal when the entire dataset is unavailable or the environment is dynamically changing [92–96]. On the other hand, batch learning is easier to maintain and less complex; it requires all the data to be available to be trained on it and does not update its model. Table 6 shows the advantages and disadvantages of batch learning and online learning.

An online model aims to learn a hypothesis  $\mathcal{H}: X \to Y$  Where X is the input space, and Y is the output space. At each time stept, a new data instance  $x_t \in X$  is received, and an output or prediction  $\hat{y}_t$  is generated using the mapping function  $\mathcal{H}(x_t, w_t) = \hat{y}_t$ , where  $w_t$  is the weights' vector of the online model at the time stept. The true class label  $y_t$  is then utilized to calculate the loss and update the weights of the model  $w_{t+1}$ , which is illustrated in Fig. 7 [97].

**Fig. 6** Review of learning classification in deep learning models





**Table 6** Advantages and disadvantages of batch learning and online learning

Learning technique	Advantage	Disadvantage
Batch learning	Low-cost learning,	Requires data availability,
	Easier to maintain,	High memory,
	Less complex	Poor scalability
Online learning	More efficient.	High training cost,
	Better scalability.	Previously acquired knowledge can be forgotten
	Adapts to data changes,	Difficult to maintain,
		More complex

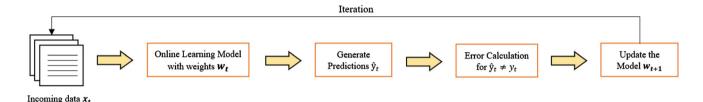


Fig. 7 Online machine learning process

The number of mistakes committed by the online model across T time steps is defined as  $M_T$  for  $\hat{y_t} \neq y_t$  [55]. The goal of an online learning model is to minimize the total loss of the online model performance compared to the best model in hindsight, which is defined as [35]

$$R_T = \sum_{t=1}^{T} l_t(\mathbf{w}_t) - \min_{\mathbf{w}} \sum_{t=1}^{T} l_t(\mathbf{w})$$
 (8)

where the first term is the sum of the loss function at time step t, and the second term is the loss function of the best model after seeing all the instances [98, 99]. While training the online model, different approaches can be adopted regarding data that the model has already trained on; full memory, in which the model preserves all training data instances; partial memory, where the model retains only some of the training data instances; and no memory, in which it remembers none. Two main techniques are utilized to remove training data instances: passive forgetting and active forgetting [107–109]

- Passive forgetting only considers the amount of time that has passed since the training data instances were received by the model, which implies that the significance of data diminishes over time.
- Active forgetting, on the other hand, requires additional information from the utilized training data in order to determine which objects to remove. The density-based forgetting and error-based forgetting are two active forgetting techniques.

Online learning techniques can be classified into three categories: online learning with full feedback, online learning with partial feedback, and online learning with no feedback. Online learning with full feedback is when all

training data instances x have a corresponding true label y which is always disclosed to the model at the end of each online learning round. Online learning with partial feedback is when only partial feedback information is received that shows if the prediction is correct or not, rather than the corresponding true label explicitly. In this category, the online learning model is required to make online updates by seeking to maintain a balance between the exploitation of revealed knowledge and the exploration of unknown information with the environment [2]. On the other hand, online learning with no feedback is when only the training data are fed to the model without the ground truth or feedback. This category includes online clustering and dimension reduction [99–111].

# 5.2 Deep transfer learning

Training deep learning models from scratch needs extensive computational and memory resources and large amounts of labeled datasets. However, for some types of scenarios, huge, annotated datasets are not always available. Additionally, developing such datasets requires a great deal of time and is a costly operation. Transfer learning (TL) has been proposed as an alternative for training deep learning models [112]. In TL, the obtained knowledge from another domain can be easily transferred to target another classification problem. TL saves computing resources and increases efficiency in training new deep learning models. TL can also help train deep learning models on available annotated datasets before validating them on unlabeled data [113, 114]. Figure 8 illustrates a simple visualization of the deep transfer learning, which



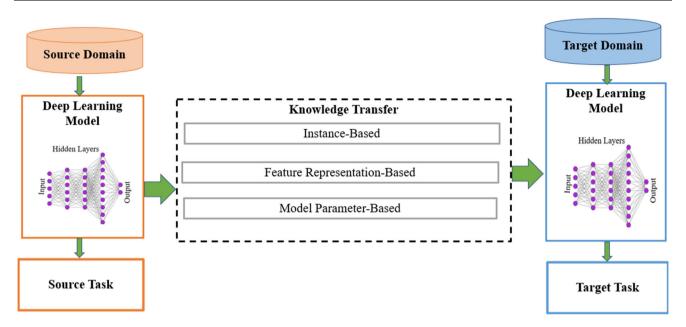
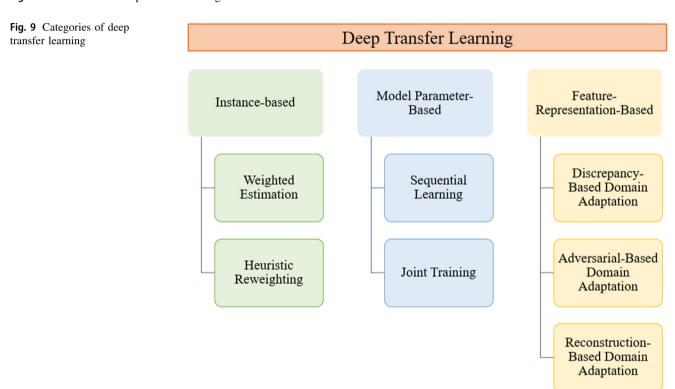


Fig. 8 Visualization of deep transfer learning



can transfer valuable knowledge by further using the learning ability of neural networks.

In this survey, the deep transfer learning techniques are classified based on the generalization viewpoints between deep learning models and domains into four categories, namely, instance, feature representation, model parameter, and relational knowledge-based techniques. In the

following, we briefly discuss these categories with their categorizations, as illustrated in Fig. 9.

# 5.2.1 Instance-based

Instance-based TL techniques are performed based on the selected instance or on selecting different weights for instances. In such techniques, the TL aims at training a



more accurate model under a transfer scenario, in which the difference between a source and a target comes from the different marginal probability distributions or conditional probability distributions [62]. Instance-based TL presents the labeled samples that are only limited to training a classification model in the target domain. This technique can directly margin the source data into the target data, resulting in decreasing the target model performance and a negative transfer during training [109–111]. The main goal of instance-based TL is to single out the instances in the source domains. Such a process can have positive impact on the training of the models in target as well as augmenting the target data through particular weighting techniques. In this context, a viable solution is to learn the weights of the source domains' instances automatically in an objective function. The objective function is given by:

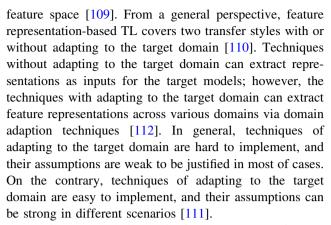
$$\vartheta = \frac{1}{C^s} \sum_{i=1}^{N^s} W_i R^s(f(x_i^s, y_i^s) + \vartheta^*(f(X), Y)$$
(9)

where  $W_i$  is the weighting coefficient of the given source instance,  $C^s$  represents the risks function of the selected source instance, and  $\vartheta^*$  is the second risk function related to the target task or the parameter regularization.

The weighting coefficient of the given source instance can be computed as the ratio of the marginal probability distribution between source and target domains. Instancebased TL can be categorized into two subcategories, weight estimation and heuristic re-weighting-based techniques [63]. A weight estimation method can focus on scenarios in which there are limited labeled instances in the target domain, converting the instance transfer problem into the weight estimation problem using kernel embedding techniques. In contrast, a heuristic re-weighting technique is more effective for developing deep TL tasks that have labeled instances and are available in the target domains [64]. This technique aims at detecting negative source instances by applying instance re-weighting approaches in a heuristic manner. One of the known instance re-weighting approaches is the transfer adaptive boosting algorithm, in which the weights of the source and target instances are updated via several iterations [116].

# 5.2.2 Feature representation-based

Feature representation-based TL models can share or learn a common feature representation between a target and a source domain. This category uses models with the ability to transfer knowledge by learning similar representations at the feature space level. Its main aim is to learn the mapping function as a bridge to transfer raw data in source and target domains from various feature spaces to a latent



One important challenge in feature representation TL with domain adaptation is the estimation of representing invariance between source and target domains. There are three techniques to build representation invariance, leveraging discrepancy-based, adversarial-based, and reconstruction-based. Leveraging discrepancy-based improve the learning transferable ability representations and decrease the discrepancy based on distance metrics between a given source and target, while the adversarialbased is inspired by GANs and provides the neural network with the ability to learn domain-invariant representations. In construction-based, the auto-encoder neural networks with specific task classifiers are combined to optimize the encoder architecture, which takes domain-specific representations and shares an encoder that learns representations between different domains [113].

# 5.2.3 Model parameter-based

Model parameter-based TL can share the neural network architecture and parameters between target and source domains. This category can convey the assumptions that can share in common between the source and target domains. In such a technique, transferable knowledge is embedded into the pre-trained source model. This pretrained source model has a particular architecture with some parameters in the target model [99]. The aim of this process is to use a section of the pre-trained model in the source domain, which can improve the learning process in the target domain. These techniques are performed based on the assumption that labeled instances in the target domain are available during the training of the target model [99–103]. Model parameter-based TL is divided into two categories, sequential and joint training. In sequential training, the target deep model can be established by pretraining a model on an auxiliary domain. However, joint training focuses on developing the source and target tasks at the same time. There are two methods to perform joint training [104]. The first method is hard parameter sharing, which shares the hidden layers directly while maintaining



Table 7 Advantage and disadvantage of instance-, feature representation-, and model parameter-based techniques

Category	Advantage	Disadvantage
Instance-based	Works based on the selection of instances or re-weight techniques, applications using this technique are found in probabilistic forecasting, which increases the accuracy in the target domain	Selection of instances may not be proper
Feature representation- based	Shares or even learns the common feature representation between the target and source domains	Common feature representation must be chosen correctly
Model parameter- based	Shares the neural network architecture and parameters between target and source domains	Sharing neural network architecture can be tricky

the task-specific layers independently [99–118]. The second method is soft parameter sharing which changes the weight coefficient of the source and target tasks and adds regularization to the risk function. Table 7 shows the advantages and disadvantages of the three categories, instance-based, future representation-based, and model parameter-based.

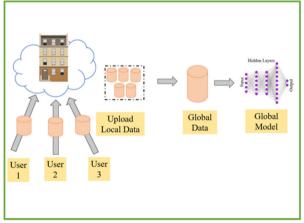
#### 5.3 Deep federated learning

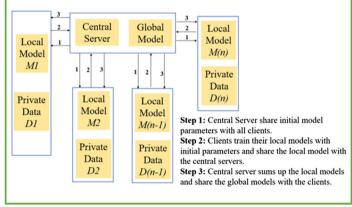
In traditional centralized DL, the collected data have to be stored on local devices, such as personal computers [74–87]. In general, traditional centralized DL can store the user data on the central server and apply it for training and testing purposes, as illustrated in Fig. 10A, while this process may deal with several shortcomings, such as high computational power, low security, and privacy. In such models, the efficiency and accuracy of the models heavily depend on the computational power and training process of the given data on a centralized server. As a result, centralized DL models not only provide low privacy and high risks of data leakage but also indicate the high demands on

storage and computing capacities of the several machines which train the models in parallel. Therefore, federated learning (FL) was proposed as an emerging technology to address such challenges [104–119].

FL provides solutions to keep the users' privacy by decentralizing data from the corresponding central server to devices and enabling artificial intelligence (AI) methods to discipline the data. Figure 10B summarizes the main process in an FL model. In particular, the unavailability of sufficient data, high computational power, and a limited level of privacy using local data are three major benefits of FL AI over centralized AI [115–119]. For this purpose, FL models aim at training a global model which can be trained on data distributed on several devices while they can protect the data. In this context, FL finds an optimal global model, known as  $\theta$ , can minimize the aggregated local loss function,  $f_k(\theta^k)$ , as shown in Eq. (10).

$$f_{(k)}(\theta^k) = \frac{1}{n_k} \sum_{i=1}^{n_k} l(x_i, y_i, \theta^k)$$
(10)





A) Centralized Learning

Fig. 10 Centralized and federated learning process flow

B) Federated Learning



$$\min_{\theta} f(\theta) = \sum_{k=1}^{C*k} \frac{n_k}{n} f_k(\theta^k)$$
 (11)

where X denotes the data feature, y is the data label,  $n_k$  is the local data size, C is the ratio in which the local clients do not participate in every round of the models' updates, C is the loss function, C is the client index, and C is shows the total number of sample pairs. FL can be classified based on the characteristics of the data distribution among the clients into two types, namely, vertical and horizontal FL models, as discussed in the following:

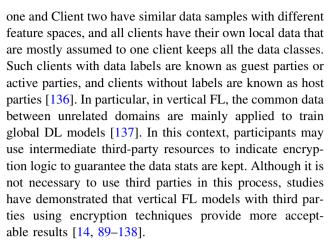
#### 5.3.1 Horizontal federated learning

Horizontal FL, homogeneous FL, shows the cases in which the given training data of the participating clients share a similar feature space; however, these corresponding data have various sample spaces [76]. Client one and Client two have several data rows with similar features, whereas each row shows specific data for a unique client. A typical common algorithm, namely, federated averaging (FedAvg), is usually used as a horizontal FL algorithm. FedAvg is one of the most efficient algorithms for distributing training data with multiple clients. In such an algorithm, clients keep the data local for protecting their privacy, while central parameters are applied to communicate between different clients [69–122].

In addition, horizontal FL provides efficient solutions to avoid leaking private local data. This can happen since the global and local model parameters are only permitted to communicate between the servers and clients, whereas all the given training data are stored on the client devices without being accessed by any other parties [14, 119–133]. Despite such advantages, constant downloading and uploading in horizontal FL may consume huge amounts of communication resources. In deep learning models, the situation is getting worse due to the needing huge amounts of computation and memory resources. To address such issues, several studies have been performed to decrease the computational efficiency of horizontal FL models [134]. These studies proposed methods to reduce communication costs using multi-objective evolutionary algorithms, model quantization, and sub-sampling techniques. In these studies, however, no private data can be accessed directly by any third party, the uploaded model parameters or gradients may still leak the data for every client [135].

#### 5.3.2 Vertical federated learning

Vertical FL, heterogeneous FL, is one of the types of FL in which users' training data can share the same sample space while they have multiple different feature spaces. Client



In contrast with horizontal FL, training parametric models in vertical FL has two benefits. Firstly, trained models in vertical FL have a similar performance as centralized models. As a matter of fact, the computed loss function in vertical FL is the same as the loss function in centralized models. Secondly, vertical FL often consumes fewer communication resources compared to horizontal FL [138]. Vertical FL only consumes more communication resources than horizontal FL if and only if the data size is huge. In vertical FL, privacy preservation is the main challenge. For this purpose, several studies have been conducted to investigate privacy preservation in vertical FL, using identity resolution schemes, protocols, and vertical decision learning schemes. Although these approaches improve the vertical FL models, there are still some main slight differences between horizontal and vertical FL [100-143].

Horizontal FL includes a server for aggregation of the global models. In contrast, the vertical FL does not have a central server and global model [14, 122–130]. As a result, the output of the local model's aggregation is done based on the guest client to build a proper loss function. Another difference is the model parameters or gradients between servers and clients in horizontal FL. Local model parameters in vertical FL depend on the local data feature spaces, while the guest client receives model outputs from the connected host clients [143]. In this process, the intermediate gradient values are sent back for updating local models [105]. Ultimately, the server and the clients communicate with one another once in a communication round in horizontal FL; however, the guest and host clients have to send and receive data several times in a communication round in vertical FL [14, 106-128]. Table 8 summarizes the main advantages and disadvantages of vertical and horizontal FL and compares these FL learning categories with central learning.



Table 8 Advantages and disadvantages of vertical and horizontal federated and centralized learning [77-143]

Learning technique		Advantage	Disadvantage
Central learning		High accuracy	Data leakage
Federated Horizontal learning		Avoiding data leakage	Consume a huge amount of communication and memory resources
	Vertical	High performance, like centralized learning, consuming less communication resources compared to horizontal federated learning	No server or global model

# 6 Challenges and future directions

Deep learning models, while powerful and versatile, face several significant challenges. Addressing these challenges requires a multidisciplinary approach involving data collection and preprocessing techniques, algorithmic enhancements, fairness-aware model training, interpretability methods, safe learning, robust models to adversarial attacks, and collaboration with domain experts and affected communities to push the boundaries of deep learning and realize its full potential. A brief description of each of these challenges is given below.

#### 6.1 Data availability and quality

Deep learning models require large amounts of labeled training data to learn effectively. However, obtaining sufficient and high-quality labeled data can be expensive, time-consuming, or challenging, particularly in specialized domains or when dealing with sensitive data such cybersecurity. Although there are several approaches, such as data augmentation, to generate high amounts of data, it can sometimes be cumbersome to generate enough training data and satisfy the requirements of DL models. In addition, having a small dataset may lead to overfitting issues where DL models perform well on the training data but fail to generalize to unseen data. Balancing model complexity and regularization techniques to avoid overfitting while achieving good generalization is a challenge in deep learning. In addition, exploring techniques to improve data efficiency, such as few-shot learning, active learning, or semi-supervised learning, remains an active area of research.

#### 6.2 Ethics and fairness

The challenge of ethics and fairness in deep learning underscores the critical need to address biases, discrimination, and social implications embedded within these models. Deep learning systems learn patterns from vast and potentially biased datasets, which can perpetuate and

amplify societal prejudices, leading to unfair or unjust outcomes. The ethical dilemma lies in the potential for these models to unintentionally marginalize certain groups or reinforce systemic disparities. As deep learning is increasingly integrated into decision-making processes across domains such as hiring, lending, and criminal justice, ensuring fairness and transparency becomes paramount. Striving for ethical deep learning involves not only detecting and mitigating biases but also establishing guidelines and standards that prioritize equitable treatment, encompassing a multidisciplinary effort to foster responsible AI innovation for the betterment of society.

#### 6.3 Interpretability and explainability

Interpretability and explainability of deep learning pose significant challenges in understanding the inner workings of complex models. As deep neural networks become more intricate, with numerous layers and parameters, their decision-making processes often resemble "black boxes," making it difficult to discern how and why specific predictions are made. This lack of transparency hinders the trust and adoption of these models, especially in high-stakes applications like health care and finance. Striking a balance between model performance and comprehensibility is crucial to ensure that stakeholders, including researchers, regulators, and end-users, can gain meaningful insights into the model's reasoning, enabling informed decisions and accountability while navigating the intricate landscape of modern deep learning.

#### 6.4 Robustness to adversarial attacks

Deep learning models are susceptible to adversarial attacks, a concerning vulnerability that highlights the fragility of their decision boundaries. Adversarial attacks involve making small, carefully crafted perturbations to input data, often imperceptible to humans, which can lead to misclassification or erroneous outputs from the model. These attacks exploit the model's sensitivity to subtle changes in its input space, revealing a lack of robustness in real-world



scenarios. Adversarial attacks not only challenge the reliability of deep learning systems in critical applications such as autonomous vehicles and security systems but also underscore the need for developing advanced defense mechanisms and more resilient models that can withstand these intentional manipulations. Therefore, developing robust models that can withstand such attacks and maintaining model security and data is of high importance.

# 6.5 Catastrophic forgetting

Catastrophic forgetting, or catastrophic interference, is a phenomenon that can occur in online deep learning, where a model forgets or loses previously learned information when it learns new information. This can lead to a degradation in performance on tasks that were previously well-learned as the model adjusts to new data. This catastrophic forgetting is particularly problematic because deep neural networks often have a large number of parameters and complex representations. When a neural network is trained on new data, the optimization process may adjust the weights and connections in a way that erases the knowledge the network had about previous tasks. Therefore, there is a need for models that address this phenomenon.

#### 6.6 Safe learning

Safe deep learning models are designed and trained with a focus on ensuring safety, reliability, and robustness. These models are built to minimize risks associated with uncertainty, hazards, errors, and other potential failures that can arise in the deployment and operation of artificial intelligence systems. DL models without safety and risks considerations in ground or aerial robots can lead to unsafe outcomes, serious damage, and even casualties. The safety properties include estimating risks, dealing with uncertainty in data, and detecting abnormal system behaviors and unforeseen events to ensure safety and avoid catastrophic failures and hazards. The research in this area is still at a very early stage.

# 6.7 Transfer learning and adaptation

Transfer learning and adaptation present complex challenges in the realm of deep learning. While pretraining models on large datasets can capture valuable features and representations, effectively transferring this knowledge to new tasks or domains requires overcoming hurdles related to differences in data distributions, semantic gaps, and contextual variations. Adapting pre-trained models to specific target tasks demands careful fine-tuning, domain adaptation, or designing novel architectures that can accommodate varying input modalities and semantics. The

challenge lies in striking a balance between leveraging the knowledge gained from pretraining and tailoring the model to extract meaningful insights from the new data, ensuring that the transferred representations are both relevant and accurate. Successfully addressing the intricacies of transfer learning and adaptation in deep learning holds the key to unlocking the full potential of AI across diverse applications and domains.

#### 7 Conclusions

In recent years, deep learning has emerged as a prominent data-driven approach across diverse fields. Its significance lies in its capacity to reshape entire industries and tackle complex problems that were once challenging or insurmountable. While numerous surveys have been published on deep learning, its models, and applications, a notable proportion of these surveys has predominantly focused on supervised techniques and their potential use cases. In contrast, there has been a relative lack of emphasis on deep unsupervised and deep reinforcement learning methods. Motivated by these gaps, this survey offers a comprehensive exploration of key learning paradigms, encompassing supervised, unsupervised, reinforcement, and hybrid learning, while also describing prominent models within each category. Furthermore, it delves into cutting-edge facets of deep learning, including transfer learning, online learning, and federated learning. The survey finishes by outlining critical challenges and charting prospective pathways, thereby illuminating forthcoming research trends across diverse domains.

**Acknowledgements** The authors acknowledge the support of the National Science Foundation (NSF), Award Number 2006674.

Data availability Not applicable.

#### **Declarations**

Conflict of interest The authors declare no conflicts of interest relevant to this article

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.



#### References

- Tan C, Sun F, Kong T, Zhang W, Yang C, Liu C (2018) A survey on deep transfer learning. In: International conference on artificial neural networks, Springer, Berlin; p 270–279
- Tang B, Chen Z, Hefferman G, Pei S, Wei T, He H, Yang Q (2017) Incorporating intelligence in fog computing for big data analysis in smart cities. IEEE Trans Ind Informatics 13:2140–2150
- Khoei TT, Aissou G, Al Shamaileh K, Devabhaktuni VK, Kaabouch N (2023) Supervised deep learning models for detecting GPS spoofing attacks on unmanned aerial vehicles. In: 2023 IEEE international conference on electro information technology (eIT), Romeoville, IL, USA, pp 340–346. https://doi. org/10.1109/eIT57321.2023.10187274
- Nguyen TT, Nguyen QVH, Nguyen DT, Nguyen DT, Huynh-The T, Nahavandi S, Nguyen TT, Pham QV, Nguyen CM (2022) Deep learning for deepfakes creation and detection: a survey. Comput Vis Image Underst 223:103525
- Dong S, Wang P, Abbas K (2021) A survey on deep learning and its applications. Comput Scie Rev 40:100379
- Ni J, Young T, Pandelea V, Xue F, Cambria E (2022) Recent advances in deep learning based dialogue systems: a systematic survey. Artif Intell Rev 56:1–101
- Piccialli F, Di Somma V, Giampaolo F, Cuomo S, Fortino G (2021) A survey on deep learning in medicine: why, how and when? Inf Fus 66:111–137
- 8. Schmidhuber J (2015) Deep learning in neural networks: an overview. Neural Netw 61:85–117
- Hatcher WG, Yu W (2018) A survey of deep learning: platforms, applications and emerging research trends. IEEE Access 6:24411–24432. https://doi.org/10.1109/ACCESS.2018. 2830661
- Pouyanfar S, Sadiq S, Yan Y, Tian H, Tao Y, Reyes MP, Shyu ML, Chen SC, Iyengar SS (2018) A survey on deep learning: algorithms, techniques, and applications. ACM Comput Surv (CSUR) 51(5):1–36
- Alom MZ et al (2019) A state-of-the-art survey on deep learning theory and architectures. Electronics 8(3):292. https://doi.org/ 10.3390/electronics8030292
- 12. Dargan S, Kumar M, Ayyagari MR, Kumar G (2020) A survey of deep learning and its applications: a new paradigm to machine learning. Arch of Computat Methods Eng 27(4):1071–1092
- Johnson JM, Khoshgoftaar TM (2019) Survey on deep learning with class imbalance. J Big Data 6(1):1–54
- Zhang Q, Yang LT, Chen Z, Li P (2018) A survey on deep learning for big data. Inf Fus 42:146–157
- Hu X, Chu L, Pei J, Liu W, Bian J (2021) Model complexity of deep learning: a survey. Knowl Inf Syst 63(10):2585–2619
- Dubey SR, Singh SK, Chaudhuri BB (2022) Activation functions in deep learning: a comprehensive survey and benchmark. Neurocomputing 503:92–108
- Berman D, Buczak A, Chavis J, Corbett C (2019) A survey of deep learning methods for cyber security. Information 10(4):122. https://doi.org/10.3390/info10040122
- Tong K, Wu Y (2022) Deep learning-based detection from the perspective of small or tiny objects: a survey. Image Vis Comput 123:104471
- Baduge SK, Thilakarathna S, Perera JS, Arashpour M, Sharafi P, Teodosio B, Shringi A, Mendis P (2022) Artificial intelligence and smart vision for building and construction 4.0: machine and deep learning methods and applications. Autom Constr 141:104440

- Omitaomu OA, Niu H (2021) Artificial intelligence techniques in smart grid: a survey. Smart Cities 4(2):548–568. https://doi. org/10.3390/smartcities4020029
- Akay A, Hess H (2019) Deep learning: current and emerging applications in medicine and technology. IEEE J Biomed Health Inform 23(3):906–920. https://doi.org/10.1109/JBHI.2019. 2894713
- Liu W, Wang Z, Liu X, Zeng N, Liu Y, Alsaadi FE (2017) A survey of deep neural network architectures and their applications. Neurocomputing 234:11–26
- Srinidhi CL, Ciga O, Martel AL (2021) Deep neural network models for computational histopathology: a survey. Med Image Anal 67:101813
- Kattenborn T, Leitloff J, Schiefer F, Hinz S (2021) Review on convolutional neural networks (CNN) in vegetation remote sensing. ISPRS J Photogramm Remote Sens 173:24

  49
- Tugrul B, Elfatimi E, Eryigit R (2022) Convolutional neural networks in detection of plant leaf diseases: a review. Agriculture 12(8):1192
- Yadav SP, Zaidi S, Mishra A, Yadav V (2022) Survey on machine learning in speech emotion recognition and vision systems using a recurrent neural network (RNN). Arch Computat Methods Eng 29(3):1753–1770
- Mai HT, Lieu QX, Kang J, Lee J (2022) A novel deep unsupervised learning-based framework for optimization of truss structures. Eng Comput 39:1–24
- Jiang H, Peng M, Zhong Y, Xie H, Hao Z, Lin J, Ma X, Hu X (2022) A survey on deep learning-based change detection from high-resolution remote sensing images. Remote Sens 14(7):1552
- 29. Mousavi SM, Beroza GC (2022) Deep-learning seismology. Science 377(6607):eabm4470
- Song X, Li J, Cai T, Yang S, Yang T, Liu C (2022) A survey on deep learning based knowledge tracing. Knowl-Based Syst 258:110036
- 31. Wang J, Biljecki F (2022) Unsupervised machine learning in urban studies: a systematic review of applications. Cities 129:103925
- Li Y (2022) Research and application of deep learning in image recognition. In: 2022 IEEE 2nd international conference on power, electronics and computer applications (ICPECA), p 994–999
- 33. Borowiec ML, Dikow RB, Frandsen PB, McKeeken A, Valentini G, White AE (2022) Deep learning as a tool for ecology and evolution. Methods Ecol Evol 13(8):1640–1660
- Wang X et al (2022) Deep reinforcement learning: a survey.
   IEEE Trans on Neural Netw Learn Syst. https://doi.org/10.1109/ TNNLS.2022.3207346
- 35. Pateria S, Subagdja B, Tan AH, Quek C (2021) Hierarchical reinforcement learning: A comprehensive survey. ACM Comput Surv (CSUR) 54(5):1–35
- Amroune M (2019) Machine learning techniques applied to online voltage stability assessment: a review. Arch Comput Methods Eng 28:273–287
- 37. Liu S, Shi R, Huang Y, Li X, Li Z, Wang L, Mao D, Liu L, Liao S, Zhang M et al (2021) A data-driven and data-based framework for online voltage stability assessment using partial mutual information and iterated random forest. Energies 14:715
- Ahmad A, Saraswat D, El Gamal A (2023) A survey on using deep learning techniques for plant disease diagnosis and recommendations for development of appropriate tools. Smart Agric Technol 3:100083
- Khan A, Khan SH, Saif M, Batool A, Sohail A, Waleed Khan M (2023) A survey of deep learning techniques for the analysis of COVID-19 and their usability for detecting omicron. J Exp Theor Artif Intell. https://doi.org/10.1080/0952813X.2023. 2165724



- Wang C, Gong L, Wang A, Li X, Hung PCK, Xuehai Z (2017)
   SOLAR: services-oriented deep learning architectures. IEEE Trans Services Comput 14(1):262–273
- Moshayedi AJ, Roy AS, Kolahdooz A, Shuxin Y (2022) Deep learning application pros and cons over algorithm deep learning application pros and cons over algorithm. EAI Endorsed Trans AI Robotics 1(1):1–13
- 42. Huang L, Luo R, Liu X, Hao X (2022) Spectral imaging with deep learning. Light: Sci Appl 11(1):61
- Bhangale KB, Kothandaraman M (2022) Survey of deep learning paradigms for speech processing. Wireless Pers Commun 125(2):1913–1949
- Khojaste-Sarakhsi M, Haghighi SS, Ghomi SF, Marchiori E (2022) Deep learning for Alzheimer's disease diagnosis: a survey. Artif Intell Med 130:102332
- Fu G, Jin Y, Sun S, Yuan Z, Butler D (2022) The role of deep learning in urban water management: a critical review. Water Res 223:118973
- Kim L-W (2018) DeepX: deep learning accelerator for restricted Boltzmann machine artificial neural networks. IEEE Trans Neural Netw Learn Syst 29(5):1441–1453
- 47. Wang C, Gong L, Yu Q, Li X, Xie Y, Zhou X (2017) DLAU: a scalable deep learning accelerator unit on FPGA. IEEE Trans Comput-Aided Design Integr Circuits Syst 36(3):513–517
- 48. Dundar A, Jin J, Martini B, Culurciello E (2017) Embedded streaming deep neural networks accelerator with applications. IEEE Trans Neural Netw Learn Syst 28(7):1572–1583
- De Mauro A, Greco M, Grimaldi M, Nobili G (2016) Beyond data scientists: a review of big data skills and job families. In: Proceedings of IFKAD, p 1844–1857
- 50. Lin S-B (2019) Generalization and expressivity for deep nets. IEEE Trans Neural Netw Learn Syst 30(5):1392–1406
- Gopinath M, Sethuraman SC (2023) A comprehensive survey on deep learning based malware detection techniques. Comp Sci Rev 47:100529
- Khalifa NE, Loey M, Mirjalili S (2022) A comprehensive survey of recent trends in deep learning for digital images augmentation. Artif Intell Rev 55:1–27
- Peng S, Cao L, Zhou Y, Ouyang Z, Yang A, Li X, Jia W, Yu S (2022) A survey on deep learning for textual emotion analysis in social networks. Digital Commun Netw 8(5):745–762
- Tao X, Gong X, Zhang X, Yan S, Adak C (2022) Deep learning for unsupervised anomaly localization in industrial images: a survey. IEEE Trans Instrum Meas 71:1–21. https://doi.org/10. 1109/TIM.2022.3196436
- Sharifani K, Amini M (2023) Machine learning and deep learning: a review of methods and applications. World Inf Technol Eng J 10(07):3897–3904
- Li Q, Peng H, Li J, Xia C, Yang R, Sun L, Yu PS, He L (2022) A survey on text classification: from traditional to deep learning. ACM Trans Intell Syst Technol (TIST) 13(2):1–41
- 57. Zhou Z, Xiang Y, Hao Xu, Yi Z, Shi Di, Wang Z (2021) A novel transfer learning-based intelligent nonintrusive loadmonitoring with limited measurements. IEEE Trans Instrum Meas 70:1–8
- Akram MW, Li G, Jin Y, Chen X, Zhu C, Ahmad A (2020) Automatic detection of photovoltaic module defects in infrared images with isolated and develop-model transfer deep learning. Sol Energy 198:175–186
- 59. Karimipour H, Dehghantanha A, Parizi RM, Choo K-KR, Leung H (2019) A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. IEEE Access 7:80778–80788
- Moonesar IA, Dass R (2021) Artificial intelligence in health policy—a global perspective. Global J Comput Sci Technol 1:1–7

- 61. Mo Y, Wu Y, Yang X, Liu F, Liao Y (2022) Review the state-of-the-art technologies of semantic segmentation based on deep learning. Neurocomputing 493:626–646
- Subramanian N, Elharrouss O, Al-Maadeed S, Chowdhury M (2022) A review of deep learning-based detection methods for COVID-19. Comput Biol Med 143:105233
- 63. Tsuneki M (2022) Deep learning models in medical image analysis. J Oral Biosci 64(3):312–320
- 64. Pan X, Lin X, Cao D, Zeng X, Yu PS, He L, Nussinov R, Cheng F (2022) Deep learning for drug repurposing: Methods, databases, and applications. Wiley Interdiscip Rev: Computat Mol Sci 12(4):e1597
- Novakovsky G, Dexter N, Libbrecht MW, Wasserman WW, Mostafavi S (2023) Obtaining genetics insights from deep learning via explainable artificial intelligence. Nat Rev Genet 24(2):125–137
- 66. Fan Y, Tao B, Zheng Y, Jang S-S (2020) A data-driven soft sensor based on multilayer perceptron neural network with a double LASSO approach. IEEE Trans Instrum Meas 69(7):3972–3979
- Menghani G (2023) Efficient deep learning: a survey on making deep learning models smaller, faster, and better. ACM Comput Surv 55(12):1–37
- 68. Mehrish A, Majumder N, Bharadwaj R, Mihalcea R, Poria S (2023) A review of deep learning techniques for speech processing. Inf Fus 99:101869
- Mohammed A, Kora R (2023) A comprehensive review on ensemble deep learning: opportunities and challenges. J King Saud Univ-Comput Inf Sci 35:757–774
- 70. Alzubaidi L, Bai J, Al-Sabaawi A, Santamaría J, Albahri AS, Al-dabbagh BSN, Fadhel MA, Manoufali M, Zhang J, Al-Timemy AH, Duan Y (2023) A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications. J Big Data 10(1):46
- Katsogiannis-Meimarakis G, Koutrika G (2023) A survey on deep learning approaches for text-to-SQL. The VLDB J. https:// doi.org/10.1007/s00778-022-00776-8
- Soori M, Arezoo B, Dastres R (2023) Artificial intelligence, machine learning and deep learning in advanced robotics a review. Cognitive Robotics 3:57–70
- Mijwil M, Salem IE, Ismaeel MM (2023) The significance of machine learning and deep learning techniques in cybersecurity: a comprehensive review. Iraqi J Comput Sci Math 4(1):87–101
- 74. de Oliveira RA, Bollen MH (2023) Deep learning for power quality. Electr Power Syst Res 214:108887
- Yin L, Gao Qi, Zhao L, Zhang B, Wang T, Li S, Liu H (2020) A review of machine learning for new generation smart dispatch in power systems. Eng Appl Artif Intell 88:103372
- Luong NC et al. (2019) Applications of deep reinforcement learning in communications and networking: a survey. In: IEEE communications surveys & tutorials, vol 21, no 4, p 3133–3174, https://doi.org/10.1109/COMST.2019.2916583
- Kiran BR et al (2022) Deep reinforcement learning for autonomous driving: a survey. IEEE Trans Intell Transp Syst 23(6):4909–4926. https://doi.org/10.1109/TITS.2021.3054625
- Arulkumaran K, Deisenroth MP, Brundage M, Bharath AA (2017) Deep Reinforcement Learning: A Brief Survey. IEEE Signal Process Mag 34(6):26–38. https://doi.org/10.1109/MSP. 2017.2743240
- Levine S, Kumar A, Tucker G, Fu J (2020) Offline reinforcement learning: Tutorial, review, and perspectives on open problems. arXiv preprint arXiv:2005.01643
- Vinuesa R, Azizpour H, Leite I, Balaam M, Dignum V, Domisch S, Felländer A, Langhans SD, Tegmark M, Nerini FF (2020) The role of artificial intelligence in achieving the



- sustainable development goals. Nature Commun. https://doi.org/10.1038/s41467-019-14108-y
- Khoei TT, Kaabouch N (2023) ACapsule Q-learning based reinforcement model for intrusion detection system on smart grid. In: 2023 IEEE international conference on electro information technology (eIT), Romeoville, IL, USA, pp 333–339. https://doi.org/10.1109/eIT57321.2023.10187374
- 82. Hoi SC, Sahoo D, Lu J, Zhao P (2021) Online learning: a comprehensive survey. Neurocomputing 459:249–289
- Celard P, Iglesias EL, Sorribes-Fdez JM, Romero R, Vieira AS, Borrajo L (2023) A survey on deep learning applied to medical images: from simple artificial neural networks to generative models. Neural Comput Appl 35(3):2291–2323
- 84. Mohammad-Rahimi H, Rokhshad R, Bencharit S, Krois J, Schwendicke F (2023) Deep learning: a primer for dentists and dental researchers. J Dent 130:104430
- Liu Z, Tong L, Chen L, Jiang Z, Zhou F, Zhang Q, Zhang X, Jin Y, Zhou H (2023) Deep learning based brain tumor segmentation: a survey. Complex Intell Syst 9(1):1001–1026
- 86. Zheng Y, Xu Z, Xiao A (2023) Deep learning in economics: a systematic and critical review. Artif Intell Rev 4:1–43
- 87. Jia T, Kapelan Z, de Vries R, Vriend P, Peereboom EC, Okkerman I, Taormina R (2023) Deep learning for detecting macroplastic litter in water bodies: a review. Water Res 231:119632
- 88. Newbury R, Gu M, Chumbley L, Mousavian A, Eppner C, Leitner J, Bohg J, Morales A, Asfour T, Kragic D, Fox D (2023) Deep learning approaches to grasp synthesis: a review. IEEE Trans Robotics. https://doi.org/10.1109/TRO.2023.3280597
- Shafay M, Ahmad RW, Salah K, Yaqoob I, Jayaraman R, Omar M (2023) Blockchain for deep learning: review and open challenges. Clust Comput 26(1):197–221
- Benczúr AA., Kocsis L, Pálovics R (2018) Online machine learning in big data streams. arXiv preprint arXiv:1802.05872
- 91. Shalev-Shwartz S (2011) Online learning and online convex optimization. Found Trends® Mach Learn 4(2):107–194
- Millán Giraldo M, Sánchez Garreta JS (2008) A comparative study of simple online learning strategies for streaming data. WSEAS Trans Circuits Syst 7(10):900–910
- Pinto G, Wang Z, Roy A, Hong T, Capozzoli A (2022) Transfer learning for smart buildings: a critical review of algorithms, applications, and future perspectives. Adv Appl Energy 5:100084
- Sayed AN, Himeur Y, Bensaali F (2022) Deep and transfer learning for building occupancy detection: a review and comparative analysis. Eng Appl Artif Intell 115:105254
- Li C, Zhang S, Qin Y, Estupinan E (2020) A systematic review of deep transfer learning for machinery fault diagnosis. Neurocomputing 407:121–135
- 96. Li W, Huang R, Li J, Liao Y, Chen Z, He G, Yan R, Gryllias K (2022) A perspective survey on deep transfer learning for fault diagnosis in industrial scenarios: theories, applications and challenges. Mech Syst Signal Process 167:108487
- 97. Wan Z, Yang R, Huang M, Zeng N, Liu X (2021) A review on transfer learning in EEG signal analysis. Neurocomputing 421:1–14
- Tan C, Sun F, Kong T (2018) A survey on deep transfer learning. In: Proceedings of international conference on artificial neural networks. p 270–279
- Qian F, Gao W, Yang Y, Yu D et al (2020) Potential analysis of the transfer learning model in short and medium-term forecasting of building HVAC energy consumption. Energy 193:116724
- 100. Weber M, Doblander C, Mandl P, (2020b). Towards the detection of building occupancy with synthetic environmental data. arXiv preprint arXiv:2010.04209

- Zhu H, Xu J, Liu S, Jin Y (2021) Federated learning on non-IID data: a survey. Neurocomputing 465:371–390
- Ouadrhiri AE, Abdelhadi A (2022) Differential privacy for deep and federated learning: a survey. IEEE Access 10:22359–22380. https://doi.org/10.1109/ACCESS.2022.3151670
- 103. Zhang C, Xie Y, Bai H, Yu B, Li W, Gao Y (2021) A survey on federated learning. Knowl-Based Syst 216:106775
- 104. Banabilah S, Aloqaily M, Alsayed E, Malik N, Jararweh Y (2022) Federated learning review: fundamentals, enabling technologies, and future applications. Inf Process Manag 59(6):103061
- 105. Mothukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G (2021) A survey on security and privacy of federated learning. Futur Gener Comput Syst 115:619–640
- 106. McMahan HB, Moore E, Ramage D, Hampson S, Arcas BA (2017) Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th international conference on artificial intelligence and statistics, AISTATS
- 107. Hardy S, Henecka W, Ivey-Law H, Nock R, Patrini G, Smith G, Thorne B (2017) Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. arXiv preprint arXiv:1711.10677
- 108. Chen T, He T, Benesty M, Khotilovich V, Tang Y, Cho H et al (2015) Xgboost: extreme gradient boosting. R Package Vers 1:4–2.
- Heng K, Fan T, Jin Y, Liu Y, Chen T, Yang Q (2019) Secureboost: a lossless federated learning framework. arXiv preprint arXiv:1901.08755
- 110. Konečný J, McMahan HB, Yu FX, Richtárik P, Suresh AT, Bacon D (2016) Federated learning: strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492
- 111. Hamedani L, Liu R, Atat J, Wu Y (2017) Reservoir computing meets smart grids: attack detection using delayed feedback networks. IEEE Trans Industr Inf 14(2):734–743
- 112. Yuan X, Xie L, Abouelenien M (2018) A regularized ensemble framework of deep learning for cancer detection from multiclass, imbalanced training data. Pattern Recogn 77:160–172
- 113. Xiao B, Xiong J, Shi Y (2016) Novel applications of deep learning hidden features for adaptive testing. In: Proceedings of the 21st Asia and South Pacifc design automation conference, p 743–748
- 114. Zhong SH, Li Y, Le B (2015) Query oriented unsupervised multi document summarization via deep learning. Expert Syst Appl 42:1–10
- 115. Vincent P et al (2010) Stacked denoising autoencoders: learning useful representations in a deep network with a local denoising criterion. J Mach Learn Res 11:3371–3408
- 116. Alom MZ et al. (2017) Object recognition using cellular simultaneous recurrent networks and convolutional neural network. In: Neural networks (IJCNN), international joint conference on IEEE
- 117. Quang W, Stokes JW (2016) MtNet: a multi-task neural network for dynamic malware classification. in: proceedings of the international conference detection of intrusions and malware, and vulnerability assessment, Donostia-San Sebastián, Spain, 7–8 July, p 399–418
- 118. Kamilaris A, Prenafeta-Boldú FX (2018) Deep learning in agriculture: a survey. Comput Electron Agric 147:70–90
- 119. Litjens G, Kooi T, Bejnordi BE, Setio AAA, Ciompi F, Ghafoorian M, Van Der Laak JA, Van Ginneken B, Sánchez CI (2017) A survey on deep learning in medical image analysis. Med Image Anal 42:60–88
- 120. Gheisari M, Ebrahimzadeh F, Rahimi M, Moazzamigodarzi M, Liu Y, Dutta Pramanik PK, Heravi MA, Mehbodniya A, Ghaderzadeh M, Feylizadeh MR, Kosari S (2023) Deep learning: applications, architectures, models, tools, and frameworks: a



- comprehensive survey. CAAI Trans Intell Technol. https://doi.org/10.1049/cit2.12180
- 121. Pichler M, Hartig F (2023) Machine learning and deep learning—a review for ecologists. Methods Ecol Evolut 14(4):994–1016
- 122. Wang N, Chen T, Liu S, Wang R, Karimi HR, Lin Y (2023) Deep learning-based visual detection of marine organisms: a survey. Neurocomputing 532:1–32
- 123. Lee M (2023) The geometry of feature space in deep learning models: a holistic perspective and comprehensive review. Mathematics 11(10):2375
- 124. Xu M, Yoon S, Fuentes A, Park DS (2023) A comprehensive survey of image augmentation techniques for deep learning. Pattern Recogn 137:109347
- 125. Minaee S, Abdolrashidi A, Su H, Bennamoun M, Zhang D (2023) Biometrics recognition using deep learning: a survey. Artif Intell Rev 56:1–49
- 126. Xiang H, Zou Q, Nawaz MA, Huang X, Zhang F, Yu H (2023) Deep learning for image inpainting: a survey. Pattern Recogn 134:109046
- 127. Chakraborty S, Mali K (2022) An overview of biomedical image analysis from the deep learning perspective. Research anthology on improving medical imaging techniques for analysis and intervention. IGI Global, Hershey, pp 43–59
- 128. Lestari, N.I., Hussain, W., Merigo, J.M. and Bekhit, M., 2023, January. A Survey of Trendy Financial Sector Applications of Machine and Deep Learning. In: Application of big data, blockchain, and internet of things for education informatization: second EAI international conference, BigIoT-EDU 2022, Virtual Event, July 29–31, 2022, Proceedings, Part III, Springer Nature, Cham, p. 619–633
- 129. Chaddad A, Peng J, Xu J, Bouridane A (2023) Survey of explainable AI techniques in healthcare. Sensors 23(2):634
- Grumiaux PA, Kitić S, Girin L, Guérin A (2022) A survey of sound source localization with deep learning methods. J Acoust Soc Am 152(1):107–151
- 131. Zaidi SSA, Ansari MS, Aslam A, Kanwal N, Asghar M, Lee B (2022) A survey of modern deep learning based object detection models. Digital Signal Process 126:103514

- 132. Dong J, Zhao M, Liu Y, Su Y, Zeng X (2022) Deep learning in retrosynthesis planning: datasets, models and tools. Brief Bioinf 23(1):391
- Zhan ZH, Li JY, Zhang J (2022) Evolutionary deep learning: a survey. Neurocomputing 483:42–58
- 134. Matsubara Y, Levorato M, Restuccia F (2022) Split computing and early exiting for deep learning applications: survey and research challenges. ACM Comput Surv 55(5):1–30
- 135. Zhang B, Rong Y, Yong R, Qin D, Li M, Zou G, Pan J (2022) Deep learning for air pollutant concentration prediction: a review. Atmos Environ 290:119347
- 136. Yu X, Zhou Q, Wang S, Zhang YD (2022) A systematic survey of deep learning in breast cancer. Int J Intell Syst 37(1):152–216
- Behrad F, Abadeh MS (2022) An overview of deep learning methods for multimodal medical data mining. Expert Syst Appl 200:117006
- 138. Mittal S, Srivastava S, Jayanth JP (2022) A survey of deep learning techniques for underwater image classification. IEEE Trans Neural Netw Learn Syst. https://doi.org/10.1109/TNNLS. 2022.3143887
- Tercan H, Meisen T (2022) Machine learning and deep learning based predictive quality in manufacturing: a systematic review.
   J Intell Manuf 33(7):1879–1905
- 140. Stefanini M, Cornia M, Baraldi L, Cascianelli S, Fiameni G, Cucchiara R (2022) From show to tell: a survey on deep learning-based image captioning. IEEE Trans Pattern Anal Mach Intell 45(1):539–559
- 141. Caldas S, Konečný J, McMahan HB, Talwalkar A (2018) Expanding the reach of federated learning by reducing client resource requirements. arXiv preprint arXiv:1812.07210
- 142. Chen Y, Sun X, Jin Y (2019) Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation. IEEE Trans Neural Netw Learn Syst 31:4229–4238
- 143. Zhu H, Jin Y (2019) Multi-objective evolutionary federated learning. IEEE Trans Neural Netw Learn Syst 31:1310–1322

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

