Robust Learning Enabled Intelligence for the Internet-of-Things: A Survey From the Perspectives of Noisy Data and Adversarial Examples

Yulei Wu, *Senior Member, IEEE*

***Abstract*—The Internet-of-Things (IoT) has been widely adopted in a range of verticals, e.g., automation, health, energy and manufacturing. Many of the applications in these sectors, such as self-driving cars and remote surgery, are critical and high stakes applications, calling for advanced machine learning (ML) models for data analytics. Essentially, the training and testing data that are collected by massive IoT devices may contain noise (e.g., abnormal data, incorrect labels and incomplete information) and adversarial examples. This requires high robustness of ML models to make reliable decisions for IoT applications. The research of robust ML has received tremendous attentions from both academia and industry in recent years. This paper will investigate the state-of-the-art and representative works of robust ML models that can enable high resilience and reliability of IoT intelligence. Two aspects of robustness will be focused on, i.e., when the training data of ML models contains noises and adversarial examples, which may typically happen in many real-world IoT scenarios. In addition, the reliability of both neural networks and reinforcement learning framework will be investigated. Both of these two machine learning paradigms have been widely used in handling data in IoT scenarios. The potential research challenges and open issues will be discussed to provide future research directions.**

***Index Terms*—Machine Learning, Reliability, Robustness, Efficiency, IoT**

I. Introduction

Due to its fast development and advancement, the Internet-of-Things (IoT) has been adopted by many industry sectors, including automation, health, transportation, energy and manufacturing [1], [2], [3], [4]. Many applications in these verticals are critical and high stakes applications, e.g., autonomous vehicles and remote surgery [5]. The Statista estimated that 38.6 billion (by 2025) and 50 billion (by 2030) of IoT devices will be in use around the world[1]. The overwhelming volume of data is being generated and collected by billions of IoT devices at the network edge, leading to the term of "edge big data" [6]. The success of machine learning (ML), especially deep learning (DL), in many sectors has shown that it is a promising means to unleash the potential of edge big data and make intelligent decisions for many IoT applications [7], [8], [9], [10], [11], [12], [13], [14].

According to the requirements of IoT applications and the computing resources of IoT devices, data analytics can be carried out either at IoT devices or at the cloud, or both [15], [16], [17], [18]. Here, the cloud includes both legacy remote datacentres and edge servers that are located in closer proximity to IoT devices. In addition to the computation related challenges at the cloud side [19], [20], [21], [16], developing light-weight ML models has been a feasible way to cope with the limited computing resources of IoT devices [22], [23]. The offloading strategy is usually considered between IoT devices and the cloud to reach a balance among many factors, including energy consumption, communication delay, computation efficiency, edge server placement, and security factors [24], [25], [26], [27], [28], [29], [30].

It is well-known that ML models are data driven, i.e., models need to be trained and tested using the data collected by massive IoT devices. These data are essentially not completely clean, instead some may contain a fair amount of noises or adversarial examples [31], [32], [33]. Noisy data contains the data that are not useful for model training and testing, the data that are incorrectly labelled, and the data that do not contain the complete information required to get an ML model well trained [34], [35], [36], [37]. Adversarial examples include the data that can make ML models work erroneously with unexpected model behaviours [38], [39]. Data auditing schemes are usually considered to tackle the issue of non-cleaned data [40]. Supervised, semi-supervised and unsupervised learning are required depending on data labeling in practice [41].

Due to the nature of high stakes applications in many IoT scenarios, high robustness is urgently needed for ML models to efficiently handle the IoT data with various degrees of veracity. This paper will investigate the state-of-the-art and representative studies of robust ML models, which can handle IoT scenarios with noisy data and adversarial examples. For dealing with noisy data, existing works mainly have two strands. One is to pre-process the data to remove the noise, or predict and complement the missing values. The other strand is to develop robust models that can be resilient to the noise and missing values. For handling adversarial examples, this paper mainly focuses on the reliability of two well-known ML paradigms, i.e., neural network and reinforcement learning framework, and discusses the corresponding measurements of reliability. This paper will provide useful guidance for

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

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

[1] https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

researchers and engineers to perform related studies of IoT applications.

The rest of this paper is organised as follows. Section II introduces artificial intelligence (AI) powered edge computing that is of paramount importance to IoT applications and discusses two typical IoT scenarios that may cause the issues of noisy data and adversarial examples. Correspondingly, Section III and Section IV investigate the state-of-the-art and representative robust ML models that handle the data of the two cases discussed in Section II, respectively. In Section IV, we will discuss the reliability issues of neural networks and reinforcement learning framework, and the corresponding solutions in the literature. Section V provides a list of potential research challenges and open issues that can be useful for guiding future research. Finally, Section VI concludes this paper.

II. AI Powered Edge Computing for IoT and its Robustness to IoT Applications

Edge computing brings the computation and data storage closer to the network edge [42]. The IoT data can be therefore processed nearer the location where it is generated [43]. This computing paradigm shift is significant for reducing the response time of IoT applications and saving bandwidth towards remote datacentres [44], [45]. The benefits of edge computing have attracted the attentions from many IoT verticals, including autonomous vehicles, remote surgery, e-health, transportation, and industrial IoT (IIoT) [46], [47].

Before diving into the details of robust ML, in this section we will briefly discuss how AI can empower the intelligence in edge computing. Comparing with data processing in cloud datacentres, IoT data need to be processed more efficiently at the network edge [48]. This is driven by the requirement of many time-critical IoT applications, e.g., self-driving cars and oxygen monitoring in mines [49]. Recent years have witnessed a dramatically increasing number of computing devices deployed nearer the data at which they are generated [50], ranging from wearable smart devices to vehicle-mounted computers, all the way to the edge servers deployed at the base station. Due to advancement of computing technologies, ML has penetrated into every aspect of these computing devices, as shown in Fig. 1.

The robustness of data processing has become a dominate factor in IoT big data that has received numerous attentions from both academia and industry [51]. Robustness has various interpretations in different scenarios. In this paper, we will mainly focus on two typical IoT scenarios that may introduce noisy data and adversarial examples. In the following, we will briefly illustrate these two scenarios.

Scenario 1 – noisy data. Data collected by IoT devices usually introduce a certain amount of noise. This is due to several reasons. Since IoT devices are densely deployed, they are working under radio frequency noise [52], [53]. In addition, malfunction and/or abnormal behaviour (e.g., attack, connection errors and man-made errors) of data collection in IoT devices can also introduce noises [54], [55], [56]. Future, inappropriate measurement calibration is also a key factor that can make the collected data noisy. For example, an ML model requires per-minute data collection for training while per-hour data collection is achieved at random. Besides, some cheap IoT devices are equipped with sensors that may have high error rates due to quality of products. This will in turn contribute to errors in data collection. Existing studies resort to either developing pre-processing schemes to filter out noisy data or proposing robust ML models to reduce negative effects caused by noisy data.

Incomplete data is essentially not useful for the training of ML models, and thus it is also a kind of noise in model training. The incompleteness of data can be caused by several factors. One of them is related to the reasons mentioned above, where IoT devices are attacked or malfunctioning. This results in missing information in the collected data. A more important factor that causes the incompleteness of data is due to privacy considerations [57], [58], [59]. For example, some private data are not allowed to be collected, and some privacy protection protocols are intentionally designed to share only partial information between entities [60], [61], [62]. To improve the quality and performance of ML model training, existing works mainly focus on the prediction of missing data, and the recovery and complement of missing values in the data, or the improvement of ML models to make them resilient to incomplete data.

Scenario 2 – adversarial examples. IoT devices may be attacked and compromised to tamper the collected data. The purpose is to fool ML models and let them make incorrect decisions. This is particularly related to the reliability of ML models. The *reliability* is informally defined as the probability that a fault may cause a failure. There are many clearest real-world IoT scenarios that require high reliability of data processing, e.g., pedestrian detection in autonomous driving, and object recognition in images/videos for surveillance and monitoring in smart cities [63], [64]. There are several ML paradigms that can be used to handle IoT big data and achieve edge intelligence. In this paper, we will mainly focus on two well-known paradigms: neural networks and reinforcement learning framework. In the context of IoT, *neural networks* are mainly trained either in a supervised way or an unsupervised way using the data collected from IoT applications [41]. *Reinforcement learning framework* focuses on the interaction between the intelligent agent and the IoT environment [65], [66], [67], [68]. Through the iterative training from many times of interactions with the environment, the intelligent agent will be trained and get ready to use for a given IoT application. Most of research on neural networks and reinforcement learning framework are focused on improving the accuracy of ML models. Reliability and robustness are the two factors recently receiving increasing attentions, in particular for critical IoT applications. The evaluation of reliability of ML models is regulated by different standards depending on application domains, e.g., IEC 61508[2] for industrial systems and ISO 26262[3] for automotive. The discussion of these standards is out of scope of this paper.

[2] https://www.iec.ch/functionalsafety/?ref=extfooter

[3] https://www.iso.org/standard/68383.html

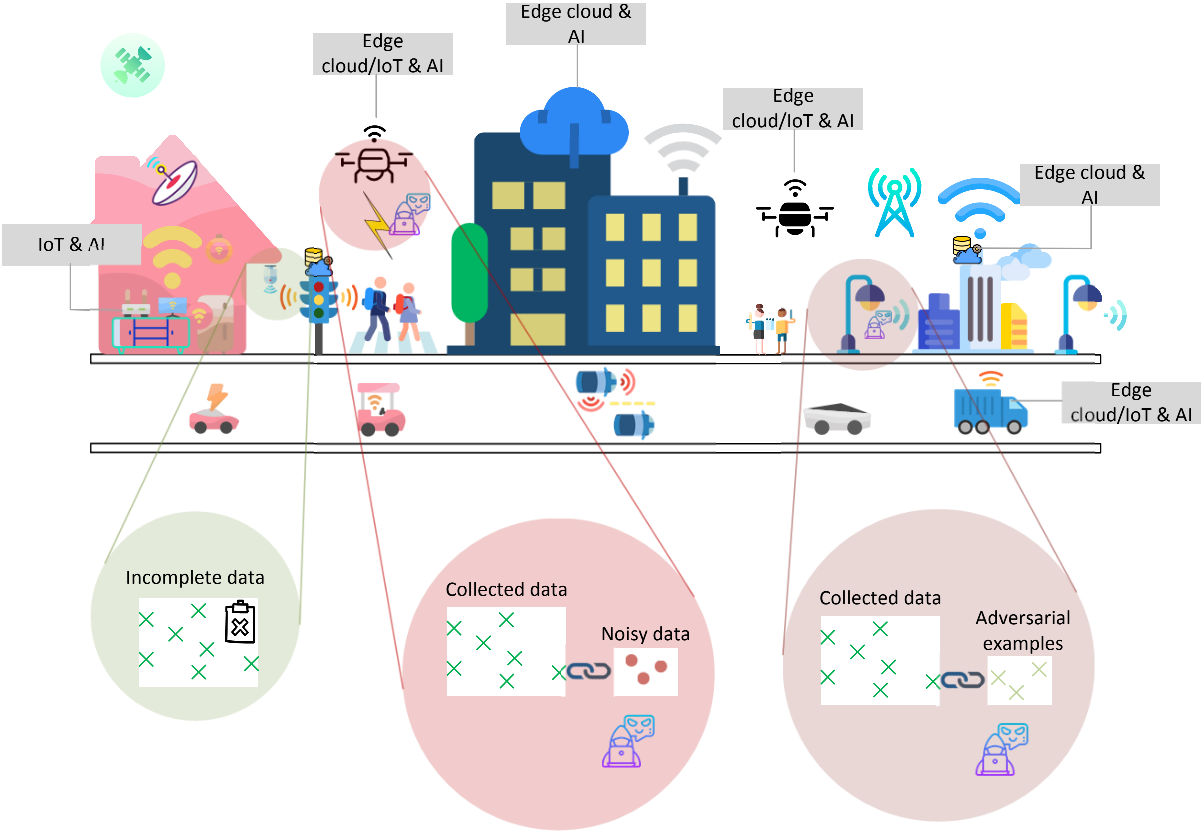


Fig. 1. Artificial intelligence is everywhere in the IoT and network edge, and a couple of typical cases that can cause noisy data (including incomplete data) and adversarial examples.

In what follows, we will discuss state-of-the-art and representative studies on robustness of ML models for the above two IoT scenarios.

III. Robust Learning under Noisy Data

With the fast growth in the scale of IoT, noise is a common factor in the IoT data; in most of the datasets, more than 10% of data have missing values, or they contain outliers [34]. IoT has been adopted in many sectors, e.g., smart city and smart industry. In a smart city, IoT has been widely deployed for the built environment, energy infrastructure, telecommunications, transportation and mobility, health and human services, water and waste water, public safety and payments and finance. Many of them are critical infrastructures (a.k.a. national critical infrastructures in the United Kingdom[4]). Given that ML models have been widely adopted in these infrastructures for intelligent operations, ensuring the efficiency and robustness in data handling is paramount of importance. However, noisy data significantly affects the performance of ML models. In what follows, we mainly investigate the state-of-the-art for handling two cases of noisy data, i.e., incomplete data and outlier data. A summary of these studies can be found in Table I, with the details discussed below.

A. *Incomplete Data*

Due to many reasons, e.g., cyberattacks, connection errors and sensor failures, IoT may collect data with missing information. For example, missed values may exist in some rows of collected data. Incomplete data may affect the training of ML models, resulting in degradation of model performance. To tackle this issue, one strand of existing research is to carry out imputation, which is the process of replacing missing information with substituted values.

In this family of research, the authors in [69] proposed a hybrid neural network using a dynamic and recurrent network called Jordan network to make prediction of missing data in a medical IoT application. Then, a genetic algorithm was proposed to enhance the neural network performance by optimising its weights. Izonin et al. [70] proposed a regression method for missing data recovery in an IoT based system. In the proposed method, each data was transformed into a vector using Ito decomposition [88], and coefficients of the decomposition were searched using AdaBoost algorithm [89]. In order to tackle missing data recovery issues, Azimi et al. [71] proposed a resilient decision-making framework for IoT systems. The developed framework adopted multiple imputation methods augmented by additional auxiliary information obtained via the IoT system. The missing data were then estimated via various methods. Yu et al. [72] developed a method to reconstruct the missing data with high accuracy. Specifi-

[4] https://www.cpni.gov.uk/critical-national-infrastructure-0

TABLE I
THE REPRESENTATIVE STUDIES ON ROBUST LEARNING FOR NOISY DATA

Types of Noises	Classes of Solutions	Representative Works	Main Contributions
Incomplete Data	Performing imputation to replacing missing data with substituted values	Al-Milli and Almobaideen [69]	A hybrid neural network with a genetic algorithm was developed to make prediction of missing data in a medical IoT application
		Izonin et al. [70]	A regression method for missing data recovery in an IoT based system
		Azimi et al. [71]	A missing data resilient decision-making framework for IoT systems to tackle missing data recovery issues
		Yu et al. [72]	A method to reconstruct the missing data with high accuracy based on adaptive weighted nuclear norm minimisation and a K-means clustering algorithm
		Sanyal and Zhang [73]	A data aggregation approach for raw IoT data with high uncertainties; a more reliable data matrix can be estimated
		Naveen, Sharma and Nair [74]	The missing data are pre-processed by replacing them with special characters to facilitate data handling
		Kok et al. [75]	An approach to handle missing IoT data issue from the perspectives of edge, fog and cloud computing
	Developing privacy-preservation enabled models	Lin, Hsu and Shen [36]	A new privacy preserving model was developed with the consideration of missing data
		Vakilinia et al. [37]	A solution for privacy-preserving data aggregation over incomplete data for crowdsensing
		Feng et al. [76]	A privacy-preserving tensor analysis and processing model for cloud computing to provide services for IoT applications
		Du et al. [77]	A survey for privacy-preserving techniques in IoT applications, in terms of data aggregation, trading and analysis
		Wang et al. [78]	A privacy-preserving outsourced support vector machine scheme for the deployment of Internet of Medical Things
		Chamikara et al. [79]	A local differentially private algorithm to protect IoT data privacy
Outlier Data	Robust models that can be resilient to outlier data	Moldovan et al. [80]	Studying several ML techniques that can be applied to handle the IoT datasets that are characterised by noisiness, high-dimensional feature space and imbalance in classification
		Lu et al. [33]	A learning-based IoT solution to associate a specific identity with a particular voiceprint; experimental results show significant improvement in performance especially in noisy environments
		Postol et al. [32]	Investigating the classification problem of time-series data analysis with noisy and incomplete IoT datasets, using the topological data analysis (TDA) approach
		Vrbaski, Bolic and Majumdar [81]	A micro-service based solution that uses complex event recognition to handle the uncertainties of IoT systems under heavy loads of incoming data
		Tang et al. [82]	An anomaly detector based on ensemble learning, targeting the data anomalies in smart IoT devices
	Removing noisy data to better fit in an ML model	Aksoy and Gunes [83]	A genetic algorithm was used to determine relevant features in different protocol headers, so as to reduce the complexity and increase the accuracy of classification by eliminating noisy features
		Rahul and Banyal [34]	A solution to remove outliers, missing values from the massive data as a data cleaning stage, and only correct and cleaned data are collected
		Gupta et al. [84]	A real time model to filter out noise from IIoT data
		Han et al. [35]	A deep learning paradigm named co-teaching for tackling the issue of noisy labels; there are two deep neural networks teaching each other and obtain the good data for training
		Salimitari, Joneidi and Chatterjee [85]	A ML based framework for outlier-aware consensus in blockchain-based IoT networks
		Zou et al. [86]	A strategy to enable robust and adaptive localisation in dynamic indoor environment
		Zhao et al. [87]	A two-layer learning framework for robust anomaly detection under unreliable anomaly labels

cally, the K-means algorithm was used to classify sensors into different groups with similar patterns of measurement. Then, given the correlations among attributes of sensor data, the authors proposed an algorithm to adaptively assign different weights to each singular value simultaneously. Sanyal and Zhang [73] proposed a data aggregation approach to handle raw IoT data with high uncertainties. The devised approach used sample data to reconstruct the subspace, and tracked down the low-rank approximation of the dominant subspace with high uncertainties. The robust dominant subspace is used to find more reliable data from the uncertain raw IoT data. The proposed approach can achieve this in a fully unsupervised manner. Naveen, Sharma and Nair [74] pre-processed the missing data by replacing them with special characters to facilitate data handling. Kok et al. [75] proposed an approach to handle missing IoT data issues from the perspectives of edge, fog and cloud computing.

The special requirement of IoT applications, e.g., privacy preservation, is another main reason of causing missing data [90], [91]. Existing research in this area manage to develop privacy-preservation enabled models. Lin, Hsu and Shen [36] considered the missing data due to privacy issues and proposed a new privacy-preserving model. They further developed a method to anonymise the dataset. Vakilinia et al. [37] proposed a solution for privacy-preserving data aggregation over incomplete data. The solution was developed based on linear transformation and homomorphic encryption scheme. It can obtain aggregation results from the recovered sensing results with no need to learn the individual details. Given that tensors are useful tools for IoT big data analysis, Feng et al. [76] proposed a privacy-preserving tensor analysis and processing model for cloud computing to provide services for IoT applications. Du et al. [77] provided a survey for privacy-preserving techniques in IoT applications, in terms of data aggregation, trading and analysis. Wang et al. [78] proposed a privacy-preserving outsourced support vector machine scheme for the deployment of Internet of Medical Things. The solution can protect the privacy of training data and ensure the security of the trained support vector machine model. Chamikara et al. [79] redesigned the training process of privacy-preserving deep learning that relied on the traditional server-centric approaches and proposed a local differentially private algorithm. Basically, for a convolutional neural network, the proposed solution enables a data owner to add a layer between the convolutional part and fully connected part before the data is released.

B. Outlier Data

The outlier data include those that are not useful for ML model training, e.g., imbalance in dataset and anomaly in labels. One direction of solutions for this problem is to develop robust ML models that are resilient to such kind of noises. The representative studies in this research direction will be discussed below, some of which cover both the cases of outlier data and the missing data that we have discussed in Section III-A. Moldovan et al. [80] studied several ML techniques that can be applied to handle the IoT datasets that are characterised by noisiness, high-dimensional feature space and imbalance in classification. Lu et al. [33] proposed a learning-based IoT solution to associate an identity with a voiceprint. An algorithm was developed to simultaneously handle clustering and association. Experimental results showed significant improvement in performance especially in noisy environments. A recent study [32] investigated the classification problem of time-series data analysis with noisy and incomplete IoT datasets, using the topological data analysis (TDA) approach. The authors showed the analysis results of a 9-month dataset that depicts hundreds of interacting IoT devices running in multiple residential settings. The dataset is noisy and incomplete. They performed the experiments of multi-class IoT classification. The results demonstrated that TDA works well for classifying incomplete and noisy IoT data. Vrbaski, Bolic and Majumdar [81] discussed complex and challenging issues in IoT due to a huge amount of raw sensor data with noises. They developed a micro-service based solution that leverages event recognition to handle the uncertainties of IoT systems under heavy loads of incoming data. Tang et al. [82] proposed an anomaly detection method based on an ensemble model, detecting data anomalies in smart IoT devices. The robustness of the proposed method lies on the ensemble ML model training.

Another direction of solving the issue of outlier data is to remove those data, to allow more cleaned data as inputs to ML models. A system for automated classification of IoT device characteristics was developed based on network traffic [83]. In this work, a genetic algorithm (GA) was used to decide useful features in different protocol headers. This decision can eliminate noisy features from the data, and reduce the complexity and increase the accuracy of classification. ML models are then leveraged to classify the types of host devices by analysing features selected by GA. Rahul and Banyal [34] proposed a solution to remove outliers, missing values from the massive data as a data cleaning stage, and only correct and cleaned data are collected. Gupta et al. [84] followed the similar idea to develop a real-time method to filter out noise from IIoT data. They then used extreme learning machines (ELM) to generate outputs for predicting adverse digressions. Han et al. [35] dealt with noisy label issues in deep learning. The authors mentioned deep neural networks have some preferences in memorising training data. The data with cleaned labels would be memorised before those of noisy labels. They proposed a deep learning paradigm named co-teaching for tackling the issues with noisy labels. Basically, there are two deep neural networks teaching each other simultaneously. The result of co-teaching is to obtain what data is good for training. Salimitari, Joneidi and Chatterjee [85] proposed an ML-based framework for outlier-aware consensus in blockchain-based IoT networks. The framework first used a supervised ML algorithm to detect anomaly activities. It then allows the transactions to go through a traditional consensus protocol for ledger update. Zou et al. [86] proposed a robust localisation model for dynamic indoor environment based on the paradigm of transfer learning. They used WiFi routers to extract real-time received signal strength readings from target mobile devices as unlabeled target data. So, the localisation model does not need to learn from the raw noisy signal space. Zhao et al. [87] proposed a robust two-layer learning model to detect anomalies in the context of unreliable anomaly labels. In the proposed model, the suspicious data was removed by the first layer and the anomaly types were detected by the second layer.

IV. Robust Learning for Adversarial Examples and Reliability of ML Models

The data with adversarial examples is another issue that can fool learning models to make erroneous decisions. Developing a learning solution with reliable behaviour for emerging high stakes applications has attracted great attentions. In this section, we will focus on the reliability of both neural networks and reinforcement learning framework that have been widely used in handling data in IoT scenarios.

A. Reliability of Neural Networks

Most of the high stakes applications rely on prevailing deep neural networks. However, many deep neural networks can provide predictions with high accuracy only in general cases. Neural networks can be easily fooled and are vulnerable to unexpected egregious errors [38], [39]. For example, a very small change to an image, which is imperceptible to human eyes, can cause a deep neural network to label it as something else completely (e.g., mislabeling a building as a dog). Another example is that a deep neural network can produce an image that is unrecognisable to humans, with 99.99% certainty to believe that the produced image is recognisable natural objects (e.g., labeling with certainty that TV static is a motorcycle).

Another strand for the research of reliable neural networks is from the perspective of robustness, i.e., the reliability of a neural network model for unseen data. A neural network is trained using training dataset and tested based on testing dataset. We usually divide a dataset into 80% for training and 20% for testing. After training the neural network model with those 80% training data, we test the model on the 20% unseen data. It is hard to predict the reliability of the trained neural network model on other data. Especially, you have no idea if the other data share the same pattern with training and testing data.

Many existing studies have devoted to improve the reliability of neural networks. In this section, we first review some existing directions of research on reliable neural networks and show a few useful metrics that can be used to measure the reliability of neural networks.

1) State-of-the-art and representative works: The *learning with reject option* framework is a promising idea of achieving reliability of deep neural networks [92]. Instead of optimising the overall accuracy on all the test samples, this idea provides a means to select a subset from the test dataset, in which the averaged prediction accuracy is higher than a given threshold, as shown in Fig. 2. The reliability of the prediction model can be effectively modelled by a generative adversarial approach, e.g., generative adversarial networks (GAN) or its variations. A generative adversarial learning with variance expansion (GALVE) was proposed to obtain a sample generator via GANs, and adversarial samples with higher variance were used to fine-tune the discriminator in order to improve the reliability performance of discriminator.

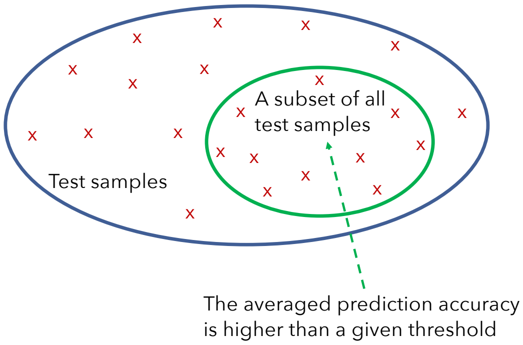

A subset of all
test samples
Test samples
The averaged prediction accuracy
is higher than a given threshold

Fig. 2. Learning with reject option for reliable neural networks.

Black box learning models are being developed to assist human experts in a wide spectrum of decision making jobs. Lack of clear understanding and explanations of the behaviour of these black box models is not acceptable for high stakes applications. The model understanding through subspace explanations (MUSE) is another research direction in the area of reliable neural networks [93]. It can facilitate the understanding of a given black box model. In this framework, the quantification of fidelity, unambiguity and interpretability was performed to construct a better explanation to the original model. The joint optimisation of the fidelity to the original model, and unambiguity and interpretability of the explanation, is an important way to improve the reliability of deep neural networks.

Tackling the reliability issues of deep neural networks (DNNs) from the perspective of software testing is a new idea in this research area. It is promising as most of deep neural network models are presented in the form of software. DeepTest [94], an automatic testing tool for detecting erroneous behaviors of a deep neural network was proposed. The authors carried out this study in the context of autonomous cars that employ deep neural networks to make decisions. DeepTest is able to generate the test inputs that can maximize the exploring of the logics of different parts of the deep neural networks. The neural network models considered in this study were convolutional neural network (CNN) and recurrent neural network (RNN).

Transfer learning is a new learning paradigm that focuses on applying the knowledge gained from solving one problem to a different but related problem. Neural networks have been widely used in transfer learning to gain and store knowledge. Different from the above problems, the problem to be discussed in transfer learning is sequential tasks. Tackling the reliability issues in sequential tasks is from the perspective of improving the interpretable explanations in each stage of the sequential tasks [95]. The purpose of this research was to enable the user to trust and use the system output from one task to the next. This solution can be applied to the more general case of emerging iterative human-machine interaction where interpretable explanations from machine are crucial for human understanding.

Table II provides a summary of the representative works in the above research directions on the reliability of neural networks, in terms of the proposed mechanisms, deep learning models used, model outputs and evaluation metrics.

2) Measuring reliability for neural networks: In addition to the evaluation metrics mentioned in Table II, calibration is

TABLE II
THE REPRESENTATIVE STUDIES ON RELIABLE NEURAL NETWORKS

Representative work	**Proposed mechanism**	**Deep learning models**	**Model output**	**Evaluation metrics**
Gao, Yao and Shao [92]	Learning with reject option	Generative adversarial network with variance expansion	A reliable sample generator	The error rate on a certain ratio of test samples with highest reported reliability
Lakkaraju et al. [93]	Model understanding through subspace explanations	Deep neural networks, gradient boosted trees, random forests, decision trees, support-vector machine	Global explanations of black box classifiers	The quantification of fidelity, unambiguity and interpretability Human accuracy
Tian et al. [94]	Software testing	Deep neural networks including convolutional neural network and recurrent neural network	Generating test inputs that maximize the number of activated neurons	Neuron coverage
Ramakrishnan and Shah [95]	A survey of existing approaches	Mentioned a number of models	Generating explanations for sequential decision-making problems	N/A

also widely used to measure a model's predicted probabilities of outcomes against true probabilities of those outcomes. It is widely used to indicate the reliability of a deep learning model's confidence in its predictions. Nixon et al. [96] identified and examined challenges in measuring calibration in deep learning. In particular, current calibration metrics are unable to consider all of the predictions made by a machine learning model, and are inefficient in the estimation of the calibration error. The authors proposed several new calibration metrics, including Static Calibration Error (SCE), Adaptive Calibration Error (ACE), and Thresholded Adaptive Calibration Error (TACE), which are more robust in calibrating a model.

A quantitative metric was proposed to evaluate the intrinsic robustness of a neural network [97]. The metric was developed based on the model predictions' maximum Kullback-Leibler (KL) divergence. In other words, they computed the divergence between two predictions on an original input and an adversarial input with perturbations in a defined range. This metric can identify the upper bound of a model's prediction divergence in a given constraint and can therefore indicate whether the model can maintain a stable prediction. The advantages of the proposed metric were demonstrated through experiments, including uniformed evaluation to different models, invariant evaluation to different test settings, and low testing overhead.

B. Reliability of Reinforcement Learning

Reinforcement learning (RL) is an area of machine learning. It has made remarkable achievements in a number of applications. An important milestone in the development of RL is that, DeepMind proposed the first deep RL, named deep Q-network (DQN) that is capable of playing Atari games at human skill level. However, lack of reliability is a well-known issue for RL. The literature has reported a wide range of results for the same baseline algorithms.

The performance of RL is sensitive to many factors, including hyper-parameters, codebases, environment properties, random seeds, etc. For example, two runs of a well-trained agent with different random seeds can yield different results due to the stochasticity in the RL process. In addition, a simple change to the policy or value network activations can significantly affect the performance of RL. Besides, for the same baseline algorithm, different authors have different implementations. The performance is obvious due to implementation details across algorithms. These variabilities in performance hinder reproducibility of RL results.

Numerous efforts have been made to tackle this problem in recent years. In this section, we will first review some of the representative works on reliable RL research and then provide a number of metrics that are useful for measuring the reliability of RL.

1) State-of-the-art and representative works: Microsoft Research and Orange Labs investigated the problem of algorithm selections for RL under the umbrella of reliable RL research [98]. An online algorithm selector was proposed to select the fittest algorithm from a pool of algorithms for the next episode of RL running, as shown in Fig. 3. The proposed algorithm selector improves the robustness of RL, where if an algorithm fails or provides an abnormal output, it will be discarded and an alternative algorithm will be selected. In the algorithm selection, a fair budget allocation between the algorithms was considered, so that each algorithm can be equitably evaluated and compared. The authors further improved the algorithm selector in terms of convergence guarantee and flexible objective function definition. In addition, the authors also adopted the curriculum learning in the design, where shallow models are used in the early stages and deep models discover the best solution in late stages.

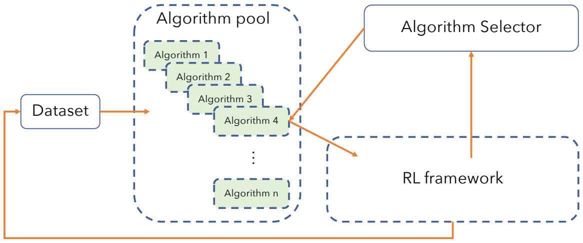


Fig. 3. An algorithm selector for reliable reinforcement learning [98].

Another work from Microsoft Research devised safe algorithms with guarantees on the policy performance for RL [99]. The authors adopted batch RL where the learning agent does not interact directly with the true environment, but instead it is

TABLE III
THE REPRESENTATIVE STUDIES ON RELIABLE REINFORCEMENT LEARNING

Representative work	Proposed mechanisms	Learning algorithms	Model output	Evaluation metrics
Laroche and Feraud [98]	An online algorithm selector	A meta-algorithm	Selecting the fittest algorithm from a pool of algorithms for the next episode of RL running	Selecting the algorithm that is the most fitted with the data size Less redundant generated policies Robustness
Laroche, Trichelair and des Combes [99]	Safe algorithms with guarantees on the policy performance for reinforcement learning (RL)	batch RL	A policy that can be guaranteed to perform at least as well as the baseline policy	Conditional value at Risk (CvaR)
Berkenkamp et al. [100]	Using statistical models of the dynamics to safely optimise policies of RL	Extending control-theoretic results on Lyapunov stability verification	High-probability safety guarantees for policies	Theoretical guarantee
Dean et al. [101]	An end-to-end finite sample bound on the performance of constrained linear quadratic regulator (LQR)	Constrained LQR with unknown dynamics	The trade-off between safety and exploration	Estimation error Safety vs. exploration Robust optimal cost sub-optimality gap

used to collect data that is fed into an algorithm to train a new policy that can be guaranteed to perform at least as well as the baseline policy. To achieve reliable policy improvement, they used Conditional value at Risk (CvaR), measuring the average of the worst runs, to evaluate the worst-case scenarios of the trained algorithm. In addition, the researchers provided a practical and commonsensical rule for policy updates in order to develop their safe policy improvement with baseline bootstrapping method. The rule was stated as follow:

> *"If there is sufficient data to support the policy change, then it is allowed to do so. Otherwise, just reproduce the baseline policy that was used during the data collection."*

Most RL algorithms need to explore all possible actions, in order to find optimal policies. This costly strategy is not practical for real-world systems. Berkenkamp et al. [100] developed a learning algorithm that explicitly considers stability guarantee. By extending control-theoretic results on Lyapunov stability verification, the authors presented how to use statistical models of the dynamics to gain high performance control policies with provable stability guarantees. In addition, the authors provided theoretical safety and exploration guarantees for an algorithm that can expand the safe region of the state space. In the implementation of the proposed algorithm, the authors sacrificed exploration guarantees while retaining stability guarantee to obtain a more practical algorithm.

An UC Berkeley team addressed the trade-off problem between safety and exploration in data-driven techniques, by studying the constrained linear quadratic regulator (LQR) with unknown dynamics [101]. The researchers derived an end-to-end finite sample bound on the performance of constrained LQR synthesized from collected data. The proposed scheme provided an important solution to guarantee safety in RL from system level synthesis. It is able to guarantee that the required constraints remain during the course of system operations and sufficient noise can be tolerated in obtaining a statistical guarantee on learning.

Similarly, Table III provides a summary of the representative works on reliability of RL, in terms of proposed mechanisms, learning algorithms, model output and evaluation metrics.

2) Measuring reliability for reinforcement learning: In addition to the evaluation metrics mentioned in Table III, there are some studies that have systemically investigated the useful evaluation metrics for measuring the reliability of RL. In what follows, we will present these studies.

A benchmark of continuous control problems for RL was provided [102]. This benchmark covers a wide range of tasks, including classic tasks like cart-pole swing-up, tasks with very high state and action dimensionality such as 3D humanoid locomotion, tasks with partial observations, and tasks with hierarchical structure. The authors implemented 9 continuous-control RL algorithms and benchmarked the average performance of these algorithms in the context of general policy parameterisations. These algorithms include random, REINFORCE, truncated natural policy gradient (TNPG), reward-weighted regression (RWR), relative entropy policy search (REPS), trust region policy optimization (TRPO), cross entropy method (CEM), covariance matrix adaption evolution Strategy (CMA-ES), and deep deterministic policy gradients (DDPG).

Henderson et al. [103] focused on the analysis of reliability for several model-free policy gradient algorithms of RL for continuous control. These algorithms include TRPO, DDPG, proximal policy optimisation (PPO), and actor critic using Kronecker-factored trust region (ACKTR). The authors investigated the reliability issue from the perspective of reproducibility of RL methods. They discussed several key factors affecting the reproducibility, including hyperparameters, network architecture, reward scale, random seeds and trials, environments and codebases.

A set of metrics that can quantitatively measure different aspects of reliability was proposed [104]. The authors focused on variability, both during training and after training. In this work, dispersion and risk were used to measure variability.

Dispersion is defined as the width of the distribution, while *risk* is defined as the heaviness and extent of the tails of the distribution. The specific metrics for "during training" include dispersion across time (DT), short-term risk across time (SRT), long-term risk across time (LRT), dispersion across runs (DR), and risk across runs (RR). The metrics for "after training" cover dispersion across fixed-policy rollouts (RF) and risk across fixed-policy rollouts (RF).

V. Potential Research Challenges and Open Issues

Because ML has been penetrated into every aspect of human lives, robustness of ML models has received tremendous attentions. Many research efforts have been devoted to tackle this issue in the IoT environment, but this research is still in its infancy. There are more potential research challenges and open issues on which we need to keep a watchful eye. In this section, we will introduce some of the emerging challenges and issues, as well as those that are currently under investigation.

- *The structure of neural networks.* Neural networks are usually designed without considering the reliability of the output results. Adding additional layers into the network structure of a neural network for assessing its reliability is a promising way of regulating a neural network with certain reliability. How to design such layers and how to maintain the introduced overhead on computational complexity are challenging.
- *The interpretability of block-box learning models.* One of the important reasons that cause the reliability issues of neural networks is the lack of interpretability of black-box learning models. The research of tackling the interpretability of neural networks is still in its infancy, especially in the IoT community. How to efficiently improve the interpretability and achieve human-in-the-loop optimisation is still a hard research problem. The outcome of this research is promising to improve the reliability of neural networks.
- *Robust testing.* In this paper, we discussed the robustness of learning phase from the perspectives of noisy data and adversarial examples. Model testing is also a way to eliminate the model vulnerabilities that are caused by noisy data and adversarial examples. Due to the complexity of the IoT application environment, manually created testing specifications are infeasible. There is a great need for a systematic testing framework that can automatically evaluate all the possible input-output cases and detect erroneous behaviours of the proposed model.
- *Reliable computing in graphics processing units.* Graphics processing units (GPUs) have been widely used for the training of deep neural networks. The learning time can be significantly reduced by virtue of the many computational cores of a GPU. However, there is no implementation to support reliable computing in GPUs. When a GPU-enabled deep neural network is used in high stakes applications, ensuring its reliability becomes critical and paramount importance.
- *Measuring reliability.* In terms of measuring the reliability of a neural network, a few potential research directions can be considered, e.g., how to characterise reliability-wise importance of different parts of a deep neural network, and how to design a unified calibration that can be used across scenarios and implementations.
- *Model-based reinforcement learning.* Deep RL algorithms require a large number of samples, to maintain their reliability, which is not feasible in some real world applications. The existing studies have shown that model-based RL algorithms are more sample efficient than model-free RL algorithms. How to guarantee the reliability and safety of model-based RL algorithms is still an open issue.
- *Zero-day vulnerability.* It is the vulnerability or attack that has been unaddressed or has not been unknown before. In the context of this paper, if the adversarial examples have not been addressed, how to promptly and efficiently detect them and mitigate the vulnerability is still a challenge. There are some promising solutions to tackle this important issue. For example, Pang et al. [105] proposed a novel training procedure and a threshold testing strategy to make it. However, there is still room for research that considers the requirements of many real-world IoT applications.
- *Ethics in reinforcement learning.* Deep RL algorithms need to be able to learn in real world scenarios without risking lives. Ethically sound RL algorithms need to be designed to improve their reliability. To achieve this, some design principles need to be considered, e.g., fairness, accountability, safety and transparency. *Fairness* includes data fairness, design fairness, outcome fairness, and implementation fairness. *Accountability* should consider across the entire design and implementation workflow. *Safety* includes accuracy, reliability, security, and robustness. Finally, *transparency* is more about interpretable AI systems as we discussed in the Section IV-A.

VI. Conclusions

Robustness in deep learning is becoming more important than ever, due to the wide spread penetration of deep learning algorithms into human lives and safety-critical applications. IoT and edge computing have become a paramount important platform to make deep learning a reality at the network edge, creating edge intelligence for beyond 5G and 6G. Robust learning in IoT is therefore a fundamental factor to guarantee the operation of many critical and high stakes applications at the network edge. This article has discussed the existing research on robust learning facing the IoT data issues, i.e., noisy data and adversarial examples. The reliability of two popular ML paradigms, i.e., neural network and reinforcement learning framework, has been discussed and related literature has been investigated. The potential research challenges and open issues have also been discussed at the end of this paper.

References

[1] Y. Wu, H. Huang, C.-X. Wang, and Y. Pan, *5G-enabled internet of things*. CRC Press, 2019.

[2] 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.

[3] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H. Dai, Y. Wu, and W. Wang, "Sctsc: A semicentralized traffic signal control mode with attribute-based blockchain in iovs," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1373–1385, 2019.

[4] L. Jiao, Y. Wu, J. Dong, and Z. Jiang, "Toward optimal resource scheduling for internet of things under imperfect csi," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1572–1581, 2020.

[5] J. Wu, S. Luo, S. Wang, and H. Wang, "Nles: A novel lifetime extension scheme for safety-critical cyber-physical systems using sdn and nfv," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2463–2475, 2019.

[6] Z. Chang, L. Lei, Z. Zhou, S. Mao, and T. Ristaniemi, "Learn to cache: Machine learning for network edge caching in the big data era," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 28–35, 2018.

[7] M. Chen, Y. Cao, R. Wang, Y. Li, D. Wu, and Z. Liu, "Deepfocus: Deep encoding brainwaves and emotions with multi-scenario behavior analytics for human attention enhancement," *IEEE Network*, vol. 33, no. 6, pp. 70–77, 2019.

[8] M. Chen, Y. Jiang, N. Guizani, J. Zhou, G. Tao, J. Yin, and K. Hwang, "Living with i-fabric: Smart living powered by intelligent fabric and deep analytics," *IEEE Network*, pp. 1–8, 2020.

[9] 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.

[10] 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. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025519303986

[11] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, "Channel state information prediction for 5g wireless communications: A deep learning approach," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 227–236, 2020.

[12] X. Liu, J. You, Y. Wu, T. Li, L. Li, Z. Zhang, and J. Ge, "Attention-based bidirectional gru networks for efficient https traffic classification," *Information Sciences*, vol. 541, pp. 297 – 315, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S002002552030445X

[13] 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.

[14] Z. Zou, J. Ge, H. Zheng, Y. Wu, C. Han, and Z. Yao, "Encrypted traffic classification with a convolutional long short-term memory neural network," in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, pp. 329–334.

[15] Z. Hong, W. Chen, H. Huang, S. Guo, and Z. Zheng, "Multi-hop cooperative computation offloading for industrial iotedgecloud computing environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 12, pp. 2759–2774, 2019.

[16] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3632–3641, 2019.

[17] A. Yousafzai, I. Yaqoob, M. Imran, A. Gani, and R. Md Noor, "Process migration-based computational offloading framework for iot-supported mobile edge/cloud computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4171–4182, 2020.

[18] L. Cui, D. Su, Y. Zhou, L. Zhang, Y. Wu, and S. Chen, "Edge learning for surveillance video uploading sharing in public transport systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–1, doi: 10.1109/TITS.2020.3008420, 2020.

[19] J. Li, Z. Ming, M. Qiu, G. Quan, X. Qin, and T. Chen, "Resource allocation robustness in multi-core embedded systems with inaccurate information," *Journal of Systems Architecture*, vol. 57, no. 9, pp. 840 – 849, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1383762111000361

[20] M. Qiu, Z. Chen, J. Niu, Z. Zong, G. Quan, X. Qin, and L. T. Yang, "Data allocation for hybrid memory with genetic algorithm," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 4, pp. 544–555, 2015.

[21] M. Qiu, Z. Ming, J. Li, S. Liu, B. Wang, and Z. Lu, "Three-phase time-aware energy minimization with dvfs and unrolling for chip multiprocessors," *Journal of Systems Architecture*, vol. 58, no. 10, pp. 439 – 445, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1383762112000719

[22] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, "Towards secure network computing services for lightweight clients using blockchain," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–12, 11 2018.

[23] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for iot medical devices," in *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*. IEEE, 2019, pp. 1–5.

[24] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and R. Fujdiak, "A secure publish/subscribe protocol for internet of things," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1–10.

[25] S. Lou, G. Srivastava, and S. Liu, "A node density control learning method for the internet of things," *Sensors*, vol. 19, no. 15, p. 3428, 2019.

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

[27] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, "Application-aware consensus management for software-defined intelligent blockchain in iot," *IEEE Network*, vol. 34, no. 1, pp. 69–75, 2020.

[28] Z. Zhao, G. Min, W. Gao, Y. Wu, H. Duan, and Q. Ni, "Deploying edge computing nodes for large-scale iot: A diversity aware approach," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3606–3614, 2018.

[29] S. Seng, C. Luo, X. Li, H. Zhang, and H. Ji, "User matching on blockchain for computation offloading in ultra-dense wireless networks," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2020.

[30] 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, doi: 10.1109/TCCN.2020.3004592, 2020.

[31] N. Mani, M. Moh, and T. Moh, "Towards robust ensemble defense against adversarial examples attack," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[32] M. Postol, C. Diaz, R. Simon, and D. Wicke, "Time-series data analysis for classification of noisy and incomplete internet-of-things datasets," in *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*, 2019, pp. 1543–1550.

[33] C. X. Lu, Y. Xiangli, P. Zhao, C. Chen, N. Trigoni, and A. Markham, "Autonomous learning of speaker identity and wifi geofence from noisy sensor data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8284–8295, 2019.

[34] K. Rahul and R. K. Banyal, "Data cleaning mechanism for big data and cloud computing," in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2019, pp. 195–198.

[35] B. Han, Q. Yao, X. Yu, G. Niu, M. Xu, W. Hu, I. W. Tsang, and M. Sugiyama, "Co-teaching: Robust training of deep neural networks with extremely noisy labels," in *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, ser. NIPS18. Red Hook, NY, USA: Curran Associates Inc., 2018, p. 85368546.

[36] W. Lin, K. Hsu, and Z. Shen, "Privacy-preserving srs data anonymization by incorporating missing values," in *2018 Conference on Technologies and Applications of Artificial Intelligence (TAAI)*, 2018, pp. 106–109.

[37] I. Vakilinia, J. Xin, M. Li, and L. Guo, "Privacy-preserving data aggregation over incomplete data for crowdsensing," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–6.

[38] A. Nguyen, J. Yosinski, and J. Clune, "Deep neural networks are easily fooled: High confidence predictions for unrecognizable images," in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2015, pp. 427–436.

[39] S. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "Deepfool: A simple and accurate method to fool deep neural networks," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2016, pp. 2574–2582.

[40] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a

service," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 289–300, 2020.

[41] M. Chen and Y. Hao, "Label-less learning for emotion cognition," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–11, 2019.

[42] H. Li, K. Ota, and M. Dong, "Learning iot in edge: Deep learning for the internet of things with edge computing," *IEEE Network*, vol. 32, no. 1, pp. 96–101, 2018.

[43] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Network*, vol. 33, no. 5, pp. 156–165, 2019.

[44] S. Wang, Y. Guo, N. Zhang, P. Yang, A. Zhou, and X. S. Shen, "Delay-aware microservice coordination in mobile edge computing: A reinforcement learning approach," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2019.

[45] K. Cao, L. Li, Y. Cui, T. Wei, and S. Hu, "Exploring placement of heterogeneous edge servers for response time minimization in mobile edge-cloud computing," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[46] A. Alnoman, S. K. Sharma, W. Ejaz, and A. Anpalagan, "Emerging edge computing technologies for distributed iot systems," *IEEE Network*, vol. 33, no. 6, pp. 140–147, 2019.

[47] A. Aissioui, A. Ksentini, A. M. Gueroui, and T. Taleb, "On enabling 5g automotive systems using follow me edge-cloud concept," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5302–5316, 2018.

[48] Y. Zhang, X. Ma, J. Zhang, M. S. Hossain, G. Muhammad, and S. U. Amin, "Edge intelligence in the cognitive internet of things: Improving sensitivity and interactivity," *IEEE Network*, vol. 33, no. 3, pp. 58–64, 2019.

[49] A. Kouris, S. I. Venieris, M. Rizakis, and C. Bouganis, "Approximate lstms for time-constrained inference: Enabling fast reaction in self-driving cars," *IEEE Consumer Electronics Magazine*, vol. 9, no. 4, pp. 11–26, 2020.

[50] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, "The role of edge computing in internet of things," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 110–115, 2018.

[51] B. Lorenzo, J. Garcia-Rois, X. Li, J. Gonzalez-Castano, and Y. Fang, "A robust dynamic edge network architecture for the internet of things," *IEEE Network*, vol. 32, no. 1, pp. 8–15, 2018.

[52] A. Z. Mohammed, A. K. Nain, J. Bandaru, A. Kumar, D. S. Reddy, and R. Pachamuthu, "A residual phase noise compensation method for ieee 802.15.4 compliant dual-mode receiver for diverse low power iot applications," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3437–3447, 2019.

[53] L. Yu, J. Wu, and P. Fan, "Energy efficient designs of ultra-dense iot networks with nonideal optical front-hauls," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7934–7945, 2019.

[54] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in iiot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, 2020.

[55] N. Zhang, X. Fang, Y. Wang, S. Wu, H. Wu, D. Kar, and H. Zhang, "Physical layer authentication for internet of things via wfrft-based gaussian tag embedding," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[56] N. Zhang, R. Wu, S. Yuan, C. Yuan, and D. Chen, "Rav: Relay aided vectorized secure transmission in physical layer security for internet of things under active attacks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8496–8506, 2019.

[57] X. Yang, L. Gao, J. Zheng, and W. Wei, "Location privacy preservation mechanism for location-based service with incomplete location data," *IEEE Access*, vol. 8, pp. 95 843–95 854, 2020.

[58] 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

[59] 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

[60] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data sharing and privacy for patient iot devices using blockchain," in *International Conference on Smart City and Informatization*. Springer, Singapore, 2019, pp. 334–348.

[61] 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

[62] X. Guo, H. Lin, Y. Wu, and M. Peng, "A new data clustering strategy for enhancing mutual privacy in healthcare iot systems," *Future Generation Computer Systems*, vol. 113, pp. 407 – 417, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19335319

[63] L. Duchesne, E. Karangelos, and L. Wehenkel, "Recent developments in machine learning for energy systems reliability management," *Proceedings of the IEEE*, pp. 1–21, 2020.

[64] A. Yazidi, H. L. Hammer, K. Samouylov, and E. Herrera-Viedma, "Game-theoretic learning for sensor reliability evaluation without knowledge of the ground truth," *IEEE Transactions on Cybernetics*, pp. 1–11, 2020.

[65] F. De Vita, G. Nardini, A. Virdis, D. Bruneo, A. Puliafito, and G. Stea, "Using deep reinforcement learning for application relocation in multi-access edge computing," *IEEE Communications Standards Magazine*, vol. 3, no. 3, pp. 71–78, 2019.

[66] A. Khune and S. Pasricha, "Mobile network-aware middleware framework for cloud offloading: Using reinforcement learning to make reward-based decisions in smartphone applications," *IEEE Consumer Electronics Magazine*, vol. 8, no. 1, pp. 42–48, 2019.

[67] Z. Yan, J. Ge, Y. Wu, H. Zheng, L. Li, and T. Li, "Automatic virtual network embedding based on deep reinforcement learning," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2019, pp. 625–631.

[68] C. Huang, Y. Wu, Y. Zuo, K. Pei, and G. Min, "Towards experienced anomaly detector through reinforcement learning," in *AAAI Conference on Artificial Intelligence*, 2018. [Online]. Available: https://www.aaai.org/ocs/index.php/AAAI/AAAI18/paper/view/16048

[69] N. Al-Milli and W. Almobaideen, "Hybrid neural network to impute missing data for iot applications," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 121–125.

[70] I. Izonin, N. Kryvinska, R. Tkachenko, and K. Zub, "An approach towards missing data recovery within iot smart system," *Procedia Computer Science*, vol. 155, pp. 11 – 18, 2019, the 16th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2019),The 14th International Conference on Future Networks and Communications (FNC-2019),The 9th International Conference on Sustainable Energy Information Technology. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050919309184

[71] I. Azimi, T. Pahikkala, A. M. Rahmani, H. Niela-Viln, A. Axelin, and P. Liljeberg, "Missing data resilient decision-making for healthcare iot through personalization: A case study on maternal health," *Future Generation Computer Systems*, vol. 96, pp. 297 – 308, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18316480

[72] X. Yu, X. Fan, K. Chen, and S. Duan, "Multi-attribute missing data reconstruction based on adaptive weighted nuclear norm minimization in iot," *IEEE Access*, vol. 6, pp. 61 419–61 431, 2018.

[73] S. Sanyal and P. Zhang, "Improving quality of data: Iot data aggregation using device to device communications," *IEEE Access*, vol. 6, pp. 67 830–67 840, 2018.

[74] Naveen, R. K. Sharma, and A. R. Nair, "Iot-based secure healthcare monitoring system," in *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2019, pp. 1–6.

[75] . Kk, B. H. orak, U. Yavanolu, and S. zdemir, "Deep learning based delay and bandwidth efficient data transmission in iot," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 2327–2333.

[76] J. Feng, L. T. Yang, X. Liu, and R. Zhang, "Privacy-preserving tensor analysis and processing models for wireless internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 98–103, 2018.

[77] J. Du, C. Jiang, E. Gelenbe, L. Xu, J. Li, and Y. Ren, "Distributed data privacy preservation in iot applications," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 68–76, 2018.

[78] J. Wang, L. Wu, H. Wang, K. R. Choo, and D. He, "An efficient and privacy-preserving outsourced support vector machine training for

internet of medical things," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[79] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "Local differential privacy for deep learning," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[80] D. Moldovan, T. Cioara, I. Anghel, and I. Salomie, "Machine learning for sensor-based manufacturing processes," in *2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, 2017, pp. 147–154.

[81] M. Vrbaski, M. Bolic, and S. Majumdar, "A performance driven micro services-based architecture/system for analyzing noisy iot data," in *2019 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 2019, pp. 173–177.

[82] S. Tang, Z. Gu, Q. Yang, and S. Fu, "Smart home iot anomaly detection based on ensemble model learning from heterogeneous data," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 4185–4190.

[83] A. Aksoy and M. H. Gunes, "Automated iot device identification using network traffic," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–7.

[84] A. Gupta, P. Manikumar, R. Reddy, and A. K. Bhattacharya, "Extreme learning machines with frequency based noise filtering for prediction of critical digressions in a noisy industrial process," in *2017 14th IEEE India Council International Conference (INDICON)*, 2017, pp. 1–6.

[85] M. Salimitari, M. Joneidi, and M. Chatterjee, "Ai-enabled blockchain: An outlier-aware consensus protocol for blockchain-based iot networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[86] H. Zou, Y. Zhou, H. Jiang, B. Huang, L. Xie, and C. Spanos, "Adaptive localization in dynamic indoor environments by transfer kernel learning," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6.

[87] Z. Zhao, S. Cerf, R. Birke, B. Robu, S. Bouchenak, S. Ben Mokhtar, and L. Y. Chen, "Robust anomaly detection on unreliable data," in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2019, pp. 630–637.

[88] R. Tkachenko, I. Izonin, P. Vitynskyi, N. Lotoshynska, and O. Pavlyuk, "Development of the non-iterative supervised learning predictor based on the ito decomposition and sgtm neural-like structure for managing medical insurance costs," *Data*, vol. 3, no. 4, 2018. [Online]. Available: https://www.mdpi.com/2306-5729/3/4/46

[89] C. Lin, D. Deng, C. Kuo, and L. Chen, "Concept drift detection and adaption in big imbalance industrial iot data using an ensemble learning method of offline classifiers," *IEEE Access*, vol. 7, pp. 56 198–56 207, 2019.

[90] Y. Ma, Y. Wu, J. Ge, and J. LI, "An architecture for accountable anonymous access in the internet-of-things network," *IEEE Access*, vol. 6, pp. 14 451–14 461, 2018.

[91] Y. Ma, Y. Wu, J. Ge, and J. Li, "A new architecture for anonymous use of services in distributed computing networks," in *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, 2017, pp. 368–374.

[92] J. Gao, J. Yao, and Y. Shao, "Towards reliable learning for high stakes applications," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 3614–3621, 07 2019.

[93] H. Lakkaraju, E. Kamar, R. Caruana, and J. Leskovec, "Faithful and customizable explanations of black box models," in *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, ser. AIES '19. New York, NY, USA: ACM, 2019, pp. 131–138. [Online]. Available: http://doi.acm.org/10.1145/3306618.3314229

[94] Y. Tian, K. Pei, S. Jana, and B. Ray, "Deeptest: Automated testing of deep-neural-network-driven autonomous cars," in *Proceedings of the 40th International Conference on Software Engineering*, ser. ICSE '18. New York, NY, USA: ACM, 2018, pp. 303–314. [Online]. Available: http://doi.acm.org/10.1145/3180155.3180220

[95] 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

[96] J. Nixon, M. W. Dusenberry, L. Zhang, G. Jerfel, and D. Tran, "Measuring calibration in deep learning," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops, CVPR Workshops 2019, Long Beach, CA, USA, June 16-20, 2019*, 2019, pp. 38–41.

[97] F. Yu, Z. Qin, C. Liu, L. Zhao, Y. Wang, and X. Chen, "Interpreting and evaluating neural network robustness," in *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI 2019, Macao, China, August 10-16, 2019*, 2019, pp. 4199–4205. [Online]. Available: https://doi.org/10.24963/ijcai.2019/583

[98] R. Laroche and R. Feraud, "Reinforcement learning algorithm selection," in *Proceedings of the 6th International Conference on Learning Representations (ICLR)*, May 2018. [Online]. Available: https://www.microsoft.com/en-us/research/publication/reinforcement-learning-algorithm-selection/

[99] R. Laroche, P. Trichelair, and R. Tachet des Combes, "Safe policy improvement with baseline bootstrapping," in *International Conference on Machine Learning (ICML)*, June 2019. [Online]. Available: https://www.microsoft.com/en-us/research/publication/safe-policy-improvement-with-baseline-bootstrapping-2/

[100] F. Berkenkamp, M. Turchetta, A. Schoellig, and A. Krause, "Safe model-based reinforcement learning with stability guarantees," in *Advances in Neural Information Processing Systems 30*, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds. Curran Associates, Inc., 2017, pp. 908–918. [Online]. Available: http://papers.nips.cc/paper/6692-safe-model-based-reinforcement-learning-with-stability-guarantees.pdf

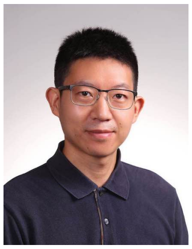
[101] S. Dean, S. Tu, N. Matni, and B. Recht, "Safely learning to control the constrained linear quadratic regulator," in *2019 American Control Conference (ACC)*, July 2019, pp. 5582–5588.

[102] Y. Duan, X. Chen, R. Houthooft, J. Schulman, and P. Abbeel, "Benchmarking deep reinforcement learning for continuous control," in *Proceedings of the 33rd International Conference on International Conference on Machine Learning - Volume 48*, ser. ICML'16. JMLR.org, 2016, pp. 1329–1338. [Online]. Available: http://dl.acm.org/citation.cfm?id=3045390.3045531

[103] P. Henderson, R. Islam, P. Bachman, J. Pineau, D. Precup, and D. Meger, "Deep reinforcement learning that matters," 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*, 2018, pp. 3207–3214. [Online]. Available: https://www.aaai.org/ocs/index.php/AAAI/AAAI18/paper/view/16669

[104] Anonymous, "Measuring the reliability of reinforcement learning algorithms," in *Submitted to International Conference on Learning Representations*, 2020, under review. [Online]. Available: https://openreview.net/forum?id=SJlpYJBKvH

[105] T. Pang, C. Du, Y. Dong, and J. Zhu, "Towards robust detection of adversarial examples," in *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, ser. NIPS18. Red Hook, NY, USA: Curran Associates Inc., 2018, p. 45844594.



Yulei Wu (Senior Member, IEEE) is a Senior Lecturer with the Department of Computer Science, College of Engineering, Mathematics and Physical Sciences, University of Exeter, UK. 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, UK, 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. His research has been supported by Engineering and Physical Sciences Research Council of United Kingdom, National Natural Science Foundation of China, University's Innovation Platform and industry. He is an Editor of IEEE Transactions on Network and Service Management, IEEE Transactions on Network Science and Engineering, and Computer Networks (Elsevier). He is a Fellow of the HEA (Higher Education Academy).