IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier

Internet of Things 2.0: Concepts, Applications, and Future Directions

IAN ZHOU[1,2], (Student Member, IEEE), IMRAN MAKHDOOM[1,2], (Member, IEEE), NEGIN SHARIATI[1,2], (Member, IEEE), MUHAMMAD AHMAD RAZA[1], RASOOL KESHAVARZ[1], JUSTIN LIPMAN[1,2], (Senior Member, IEEE), MEHRAN ABOLHASAN[1], (Senior Member, IEEE), AND ABBAS JAMALIPOUR[3], (FELLOW, IEEE)

[1]Faculty of Engineering and IT, University of Technology Sydney, Ultimo, NSW 2007, Australia
[2]Food Agility CRC Ltd, 81 Broadway, Ultimo, NSW, 2007, Australia
[3]Faculty of Engineering, University of Sydney, NSW 2006, Australia

Corresponding author: Ian Zhou (e-mail: ian.zhou@student.uts.edu.au).

We would like to acknowledge the support of Food Agility CRC Ltd, funded under the Commonwealth Government CRC Program. The CRC Program supports industry-led collaborations between industry, researchers and the community.

ABSTRACT Applications and technologies of the Internet of Things are in high demand with the increase of network devices. With the development of technologies such as 5G, machine learning, edge computing, and Industry 4.0, the Internet of Things has evolved. This survey article discusses the evolution of the Internet of Things and presents the vision for Internet of Things 2.0. The Internet of Things 2.0 development is discussed across seven major fields. These fields are machine learning intelligence, mission critical communication, scalability, energy harvesting-based energy sustainability, interoperability, user friendly IoT, and security. Other than these major fields, the architectural development of the Internet of Things and major types of applications are also reviewed. Finally, this article ends with the vision and current limitations of the Internet of Things in future network environments.

INDEX TERMS IoT, IoT2.0, Machine Learning, Mission Critical Communication, Scalability, Energy Harvesting, Interoperability, Usability, Security, 5G, 6G.

I. INTRODUCTION

The term "Internet of Things" (IoT) was first coined by Kevin Ashton in 1999 [1]. The International Telecommunication Union (ITU) has formally defined IoT as, "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [2]." This definition can be viewed as the basis of IoT technologies. There is an increasing demand for the IoT applications and technologies worldwide. It is predicted that networked devices will increase from 18 billion in 2017 to 28.5 billion in 2022, and Machine to machine (M2M) connections will reach 15 billion in 2022 [3]. With recent advancements in the fifth-generation of mobile telecommunications technology (5G), high speed and low latency networks will further facilitate the development of IoT technologies and applications [4]. However, with the recent advancement of other technologies and application such as, machine learning, edge computing, and Industry 4.0, there is a need to update and redefine the concept of IoT towards IoT 2.0 [4, 5, 6]. There are many industry and public mentions of IoT 2.0 visions. Many of them focus on improving IoT application productivity and service quality with the vision of users [7, 8, 9]. AI-driven service development is viewed as a way to enhance service quality [10]. IoT interoperability is another field that attracted attention for IoT 2.0 [11]. Other than these fields, security and privacy vulnerabilities are also mentioned as issues to be solved in the next generation IoT systems [12]. A potential solution to reinforce IoT security and privacy could be blockchain [13].

At the Samsung Developer Conference 2019, interoperability, security, connectivity, and automation of IoT applications are major fields of further development in the IoT 2.0 vision [14]. Other than this conference, a report [15] from the Joint Research Centre (JRC) of the European Commission concluded that IoT 2.0 should utilize machine learning technologies to enhance the generated intelligence and knowledge available to users. In this process, interpolation is an issue that limits the advancement of specialized edge services. Therefore, approaches toward integration and standardization are inevitable for the evolution of IoT and further development of IoT applications. Compared to the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

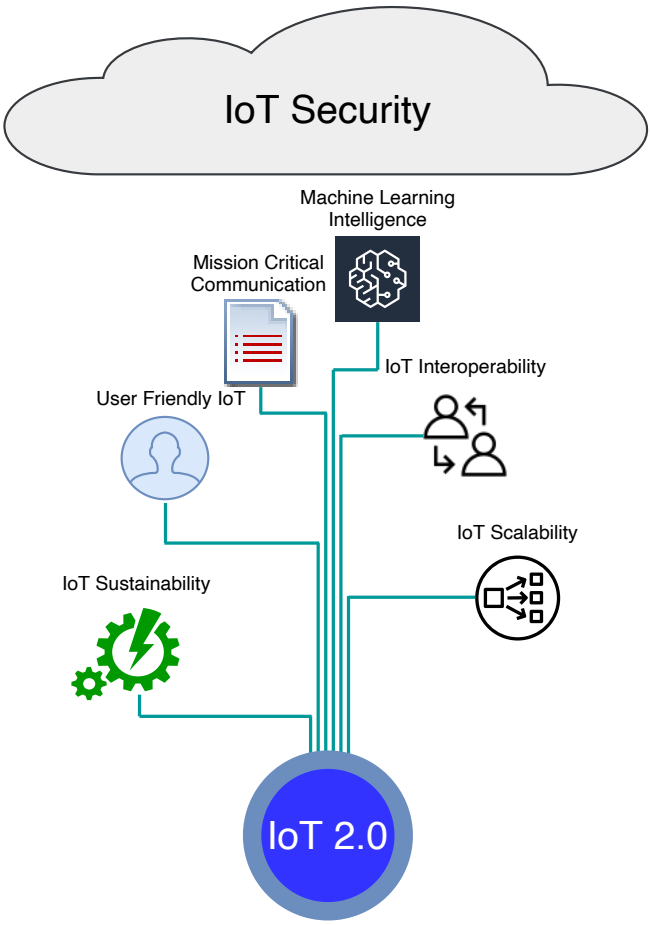

FIGURE 1. IoT 2.0 Concepts.

enthusiasm in the industry, academic works on the concept of IoT 2.0 are limited. In [16], an IoT 2.0 platform is proposed. This platform integrates application development, deployment, and sharing. Interoperability is featured as a key function of the IoT 2.0 platform [16, 17]. The authors of [18] demonstrated the "Identity of Things" as an IoT 2.0 component. IoT applications should also be identified by their manufacturers to avoid security issues generated by any criminal parties [18]. In [19], an IoT 2.0 conceptual framework is developed to emphasize the usability of IoT and systems for end-users. Distributed intelligence powered by artificial intelligence (AI) is discussed in [20] and recognized as an aspect of IoT 2.0. The above works only describe one or a few aspects of advancement in IoT. Also, the authors of [21] concluded that very few existing survey papers had connected different aspects of IoT. Therefore, the primary objective of this article is to provide an in-depth analysis of recent IoT advancement and define the concept of IoT 2.0. This article surveys the recent development of IoT technology over the period 2015–2020 in seven dimensions as IoT 2.0. These dimensions include machine learning intelligence, mission critical communication, IoT scalability, IoT sustainability, IoT interoperability, user friendly IoT, and IoT security shielding the previous six aspects from external attacks (Figure 1). The contributions of this article are:

1) Discussion of recent IoT architectures.
2) Identifying challenges and limitations on practical IoT applications.
3) Conclude and analyze recent research trend.
4) Establishing visions of IoT in future sixth-generation of mobile telecommunications technology (6G) environment.

The rest of this article is structured as follows. Section II provides an overview of related technologies and concepts. Section III examines the IoT architectures. Sections IV and V elaborate on the usage of machine learning techniques and the requirements of mission critical applications. Then, Section VI describes different types of scalability and scalability enabled by software defined networks (SDN). Sections VII and VIII establish the security and performance requirements of IoT 2.0. After that, Section IX focuses on energy harvasting-based IoT sustainability. Section X reports IoT interoperability with existing standards. Section XI illustrates user friendly IoT as the final dimension of IoT 2.0. Section XII addresses the recent development of IoT applications. Finally, Section XIII defines current challenges and future research directions, followed by Section XIV the conclusion.

II. TECHNOLOGIES AND CONCEPTS UNDERLYING IOT 2.0

A. 5G

The authors of [22] revealed the requirements of 5G-based IoT as high data rate, highly scalable and fine-grained networks, very low latency, reliability, resilience, security, long battery lifetime, connection density and mobility. Therefore, 5G grants IoT applications the capability to provide better services by gathering more data in a faster and more secure channel. Furthermore, 5G networks could support the development of next-generation IoT applications. In this subsection, the 5G enabling technologies are reviewed.

Wireless Network Function virtualization (WNFV) is a major part of 5G networks. It not only enables network services to be run through software, but also enables wireless networks to be managed more efficiency and provide better Quality of Service (QoS). Network slicing is key technology within 5G which is built on top of the WNFV to create logically separate networks and provide end-to-end QoS guarantees [23].

5G Heterogeneous networks have evolved to improve the speed of data transmission. To reduce latency, multi-tier cell architectures are deployed to offload data from higher tier centralized cells to lower-tier distributed cells. Lower tier cells are closer to the end users. Hence, latency is reduced [24].

Advanced spectrum sharing and interference management enable wider coverage area and higher traffic load balance [24]. To further improve spectral efficiency, device to device

(D2D) communication technology is also included in 5G networks. This technology allows users in close distance to communicate without a base station. Therefore, D2D communication improves not only spectral efficiency but also provides high throughput and energy efficiency [22].

One key enabler of real-time applications is edge computing. As edge computing enables low latency data transmission, real-time smart applications can be developed to provide high quality services [25]. Therefore, in a 5G network age, integration of AI and edge computing enhanced IoT will significantly enhance the quality of user experience [22].

B. TACTILE INTERNET

The authors from [26] highlighted that Tactile Internet includes human to machine interactions through haptic devices. They view Tactile Internet on the same level as IoT and 5G. Therefore, revealing the common properties of Tactile Internet, IoT and 5G as low latency, ultra-high availability, Human to Human (H2H)/M2M co-existence, data-centric technologies and security. However, the authors from [27] interprets Tactile Internet as another domain addressed by the low latency requirement of 5G and actuated by the wireless communications of IoT.

Based on the properties of Tactile Internet from [27], the authors of [28] further categorized the challenges of Tactile Internet into communications, haptics, artificial intelligence, and computation. Communication challenges are higher data rates, ultra-low latency, high reliability, and support of cloud/fog network overheads. These requirements are almost identical to the properties of 5G networks. Therefore, communication requirements can be resolved under the environment of 5G. Low latency services also require artificial intelligence and computation power. Artificial intelligence can be leveraged to predict future actions to compensate for latency. Furthermore, artificial intelligence is also the basis of intelligent services. Similar to artificial intelligence, faster computation also reduces the impact of latency. It also supports computation for artificial intelligence and real-time haptic services. The authors of [29] provided six use cases of Tactile Internet applications. The first use case is health care. An example of a health care application is exoskeletons for disabled people. The exoskeleton can detect changes in human muscle to perform certain movements. However, tactile latency is required to ensure safety. Exoskeletons can also be used for education and sports. It can be used in virtual training centers so that students can train in any location. Another use case is traffic. Tactile Internet enables fully autonomous traffic, where vehicles can react instantly to incoming humans on the street. Therefore, this system aims to prevent any injury or death from traffic accidents. This also enhances the performance of monitoring. The usage of free-viewpoint video provides multi-perspective monitoring for users [29]. In the industrial sector, Tactile Internet enables mobile robots for production, reducing any human injuries during production. The last use case is the smart grid. Using Tactile Internet, low latency networks can synchronize the usage of power to the suppliers. This allows the suppliers to precisely adjust the reactive power, preventing wastage of power.

C. EDGE COMPUTING

The aim of edge computing is to reduce bandwidth usage and latency for an IoT network. From Figure 2, as a major task of edge computing, machine learning is highly deployable on edge devices [30]. Edge computing is an enabler of low latency and real-time AI applications. In this subsection, the major architectures of edge computing are discussed.

There are three significant architectures of edge computing: fog computing, mobile edge computing (MEC) and cloudlet computing [30]. Fog computing is an extension of traditional cloud computing with fog computing nodes [30]. These fog computing nodes are placed between the end devices and a centralized cloud. The function of these fog computing nodes is to aggregate heterogeneous data from different sources. Furthermore, the fog computing nodes act as an interface to access these heterogeneous data, protecting any user from the heterogeneity of data. In the second architecture, MEC, is designed for cellular networks [30]. Unlike fog computing nodes, MEC nodes utilize both computational and storage capabilities. The functionality of these nodes can be modified through virtualization interfaces. Hence, MEC nodes can provide flexible, low latency, and real-time services to mobile end users. Finally, cloudlet computing is implemented with a cloudlet, which is a virtualized server that is one hop away from the end user [30]. Cloudlets are able to store provisional resources. Therefore, this architecture also can provide end users with flexible, low latency, and real-time services [31]. Based on these major architectures, there are also further enhancements in IoT networks improving energy efficiency [32, 33] and data reliability [34].

In conclusion, the major edge computing architectures are implemented with extended servers or nodes near the end users. The common purposes of these nodes are reducing latency, providing computation or storage capabilities, and delivering real-time services to end users. In a 5G environment, these node properties are the basis of intelligent services pushed by big data transmission and processing. Tactile Internet and Industry 4.0 also drive potential application requirements for IoT 2.0.

D. INDUSTRY 4.0

The authors of [35, p.835] defined Industry 4.0 as "the fourth industry revolution." The Cyber-Physical System (CPS) is the basis of this revolution. The authors of [5] revealed that "CPS are industrial automation systems that integrate innovative functionalities through networking to enable connection of the operations of the physical reality with computing and communication infrastructure." This definition shows that CPSs require heterogeneous data from multiple sources. As a result, data analytics techniques are suitable for implementing intelligence as part of the CPS service. The authors of [5] also pointed out that methods for processing data remain a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

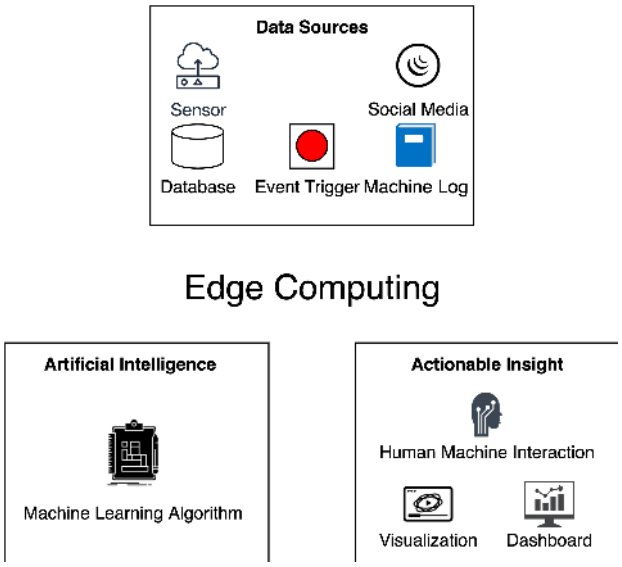

FIGURE 2. Major tasks of edge computing. [30]

challenge for these CPS applications. Hence, the implementation of big data analytics and machine learning are essential for the development of Industry 4.0. The amount of data generated by intelligent CPSs is difficult for a centralized cloud architecture to process. Inevitably, edge computing is used to distribute the load for data processing. Also, edge computing devices are closer to the end users. Therefore, it ensures lower latency of a service [36].

E. MACHINE LEARNING

IoT data processing is a challenge due to the 5V (volume, velocity, variety, veracity, and value) features of these data [37]. Data analytics techniques like machine learning can process data with complex 5V features [38]. Furthermore, applying machine learning on heterogeneous IoT data ensures intelligence to IoT applications, providing better and efficient services.

The major types of machine learning are supervised learning, unsupervised learning and reinforcement learning [39]. The supervised learning methods use input data with expected outcomes to lead the learning process of a machine learning model. On the other hand, the expected outcome is not provided when training an unsupervised learning model. An unsupervised learning model is built through clustering and other statistical methods [40]. Reinforcement learning models perform actions with input features or state of the current environment. This model learns from the return reward of the action and improves through trial-and-error [41].

III. IOT ARCHITECTURES

In this section, technical improvements of current IoT architectures are revealed through a detailed analysis of novel IoT architectures under the environment of 5G, Tactile Internet, and Industry 4.0. There are many different IoT architectures [42, 43, 44, 45, 46, 47, 48, 49, 50]. The authors in [42] aggregated the conventional IoT architectures into a layered architecture of six layers. From Figure 3, this architecture consists of the physical layer, the perception layer, the network layer, the middleware/cloud layer, the application layer, and the business layer. With the assumption that end devices have limited power, memory and computational resource, the perception layer or the end devices in the perception layer are only responsible for data collection and transfer. Therefore, all data is transmitted to the middleware/cloud layer for further processing. For applications with extensive data flows like virtual reality and augmented reality, the throughput and latency of data transmission cannot meet the requirements of real-time, perhaps mission critical service. Therefore, novel IoT architectures are needed in this new era of 5G, Tactile Internet, and Industry 4.0 [51, 52, 43].

Similar to conventional IoT architecture, the recent IoT architectures reviewed in this paper also contain end-devices and cloud layers. On the other hand, the most significant difference is the utilization of an edge/fog layer in the recent IoT architecture to provide real-time services, data analytics, and data processing functionalities near the end devices. The combination of machine learning models for data analytics services is one of the drivers for these recent architectures [43, 44, 45, 46, 47, 48, 49, 50]. Figure 4 shows the layers with the functions of these recent IoT architectures. As an architecture providing basic edge computing, the authors followed a three-layered design. This design consists of the IoT end device layer, the fog/edge layer, and the cloud layer. The IoT end device layer is similar to the perception layer of the conventional IoT architecture. This layer also contains IoT sensors, actuators, and end devices for data collection and transmission. Data is passed to the fog/Edge layer to perform analytical procedures and processed for a higher-level layer. The final layer of the three-layered architecture is the cloud layer, providing a platform for centralized data analytics, storage, and decision making [44, 45, 46]. Comparing the above recent architectures with conventional IoT architectures, the involvement of the edge computing layer is the root of the changes between architectures.

The authors of [47] separated the cloud layer into a cloud layer and a new network core layer. This layer connects the cloud layer with the fog/edge layer. Also, it provides a flexible and scalable interface for controlling the fog/edge layers [47, 50]. This interface is also developed between the data edge/fog layer and the IoT end device layer. More specifically, the network domain and the communication layer have similar functions to the network layer of the conventional IoT architecture. These layers create a link between the end devices and the fog/edge level devices. Also, as a 5G process, the communication layer facilitates advanced spectrum sharing and interference management for D2D communication [43, 49].

The application layer is above the cloud layer. For different IoT applications, the application layer is different. However, in the recent IoT architectures, the application layer commonly acts as a software interface to control lower

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

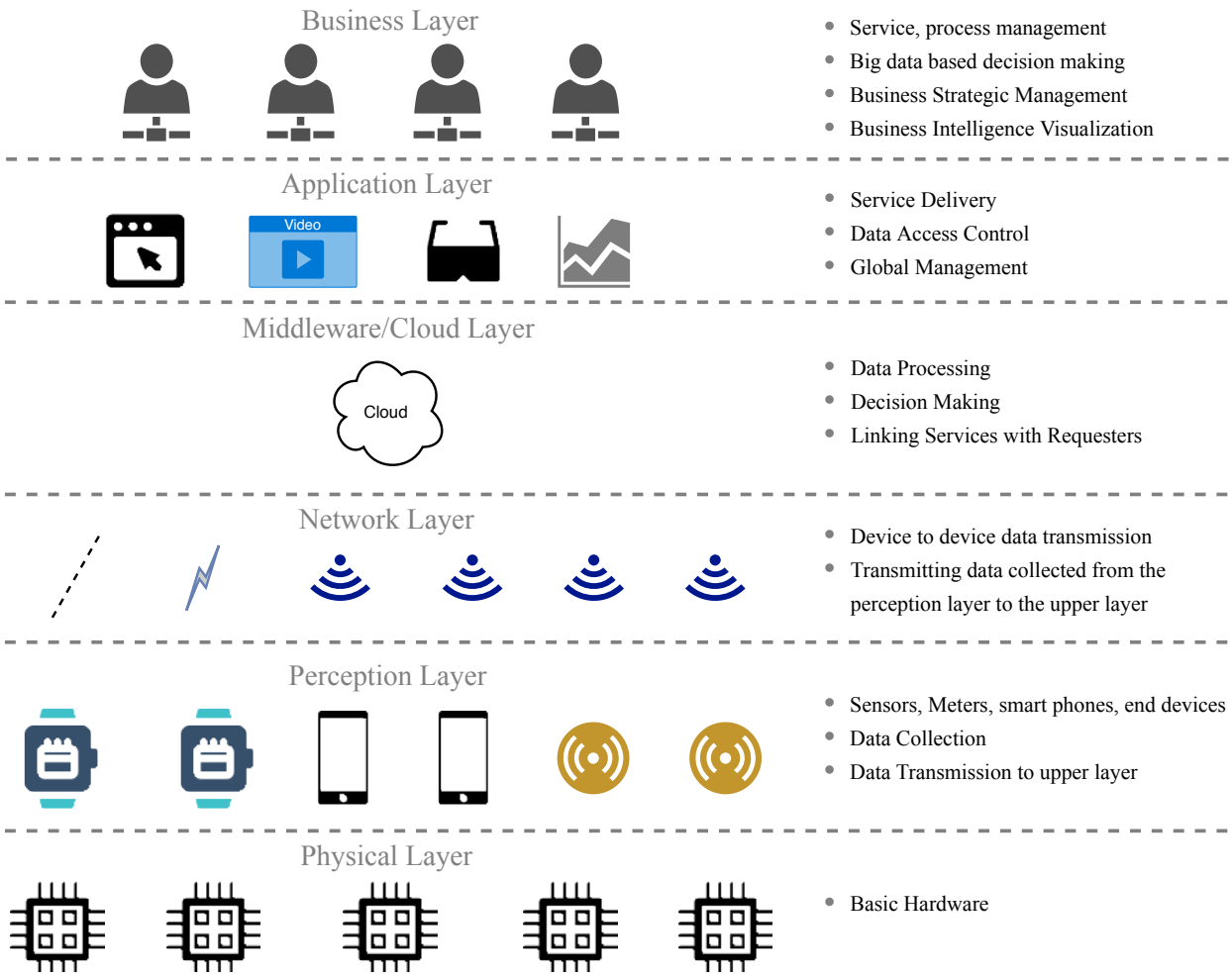

FIGURE 3. Layered Conventional IoT Architecture. [42]

layers. Services could be deployed on the cloud level and the edge/fog level to provide centralized high-level services and distributed, real-time services, respectively [43, 48, 49, 50].

The authors of [43] proposed an eight-layer IoT architecture. Different from the previous architectures, the data storage layer, the collaboration/process layer, and security aspects are added to consider the security and performance requirements under the 5G environment. The data storage layer stores raw data from the edge/fog layers. This expands the limited memory of edge devices and prepared for services with high volume traffic. The second layer, collaboration/process layer, is designed for modern business settings. It allows collaboration from different personnel. Finally, security is recognized as a concept applied to all layers to protect them against possible external attacks.

IV. MACHINE LEARNING INTELLIGENCE

This section presents the machine learning intelligence applications. As a start, the relevant supervised, unsupervised, reinforcement, and other relevant machine learning algorithms are introduced. Then, the usage of machine learning on the physical layer, the network layer, the edge computing layer, and the cloud layer are introduced. On the physical layer, machine learning helps end devices perform energy preservation scheduling and physical layer communication. Then, this section demonstrates the usage of machine learning to improve network layer performance and reduce management overhead. After that, edge layer devices and motivations of applying machine learning on edge are described. Finally, this section focuses on the collaboration between the cloud layer and the edge layer.

A. MACHINE LEARNING ALGORITHMS

1) Supervised Learning Algorithms

In supervised learning, the model learns through reducing the output of the cost function, which usually represents the model prediction and the true value. The major supervised learning methods are linear regression, logistic regression, support vector machines (SVM), Naïve Bayes classifiers, and k-nearest neighbors. Some deep learning algorithms, includ-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

Architectures						Functions
					Security	1. Data Encryption. 2. User Authentication. 3. Access Control. 4. Protection over all layers.
					Collaboration/ Process	1. Collaboration platform for multiple personnels
		Cloud Service	Application	Management	Application	1. Software interfaces to interact with lower levels. 2. Services interfaces between lower levels and users. 3. Control interface for lower level facilities. 4. Business Intelligence. 5. High Level Decision Making
Cloud	Cloud	Cloud	Cloud Computing	Server and Storage	Management Service	1. Complex Data Storage. 2. Complex Centralized Processing. 3. Training machine learning models for the cloud and the fog/edge layers. 4. Hosting Complex Machine Learning Model. 5. Basis for High Level Decision Making. 6. Multi-purpose servers. 7. Network management.
	Network Core			Core Network		1. Gateway to the cloud layer. 2. Interfaces to the fog/edge layer. 3. Linkage between the cloud and fog/edge layers.
					Data Storage	1. Storing huge data volume from the edge/fog layer.
Fog/Edge	Fog/Edge	Fog	Data Domain	Edge Network	Edge/Fog Computing	1. Connecting the end devices with the cloud. 2. Gathering data from the lower layer. 3. Basic Data Analytics. 4. Medium Data Analytics (e.g. Image Recognition) 5. Passing heavy analytical tasks to the cloud. 6. Running low level machine learning model. 7. Prepare data as inputs for high level analytics. 8. Data Storage. 9. Low level decision making. 10. Real time services
			Network Domain		Communication	
IoT End Devices	IoT End Devices	Edge Client	Device Domain	End User	Physical Devices	1. Connects lower layer end devices to the upper layer. 2. Management of time sequence sensitive data. 3. D2D Communication. 4. Advanced Spectrum Sharing and Interference Management.
(Peralta et al. 2017; Carnevale et al. 2018; Li, Ota & Dong 2018)	(Shahzadi et al. 2019)	(Kalatzis et al. 2018)	(Chen et al. 2018)	(Guo et al. 2018)	(Rahimi, Zibaeenejad & Safavi 2018)	1. Collecting data from the environment. 2. Transfer data to the upper layer. 3. Accept instructions from the upper layer.

FIGURE 4. Recent IoT Layered Architectures.

ing artificial neural networks (ANN), convolutional neural networks (CNN), and recurrent neural networks (RNN) are suitable for supervised learning [53]. There is a wide range of applications of supervised learning. For example, in the field of computer vision, many CNN-based applications are established in smart healthcare [54], smart home, smart city, smart energy, agriculture, education, industry, government, sports, retail, and IoT infrastructure [55]. The rest of this subsection explains some of the supervised learning algorithms.

a: *Support Vector Machine (SVM)*

SVM is created to solve binary classification problems [56]. The aim of SVM is to create a hyperplane over a multidimensional space to separate the data points of this space into two classes. The SVM model can be represented by Equation (1) [56]. In this equation y is the output class as a sign of positive and negative, ω is the weight vector, x is the input vector and b is the scalar bias factor.

$$y = sign(\omega \cdot x + b) \tag{1}$$

From Figure 5, the distance between the two classes can be represented by Equation (2) [56], where $||\omega||$ is the Euclidean distance.

$$D = \frac{2}{||\omega||} \tag{2}$$

The parameter ω is obtained through maximizing the distance D with minimum classification error. Therefore, the optimization problem can be defined as Equation (3) [56].

$$\Phi(\omega) = \frac{1}{2}||\omega||^2 \tag{3}$$

As indicated by [56], optimization of Equation (3) is a quadratic optimization problem, which could be solved through constructing a Lagrangian function as Equation (4), where α_i are the Lagrange multipliers.

$$L(\omega, b, \alpha) = \frac{1}{2}||\omega||^2 - \sum_{i=1}^{l} \alpha_i \{y_i(\omega \cdot x_i + b) - 1\} \tag{4}$$

The SVM described above are only suitable for linearly separable datasets. However, extensions as soft margin SVM

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

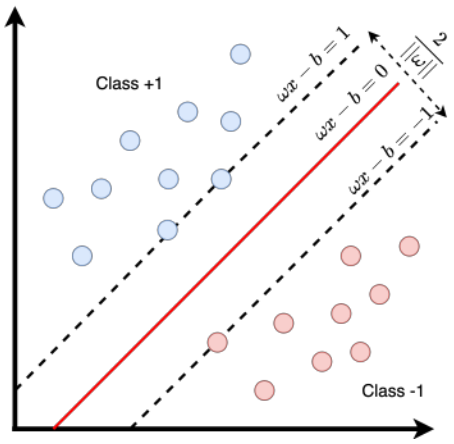

FIGURE 5. Support vector machine.

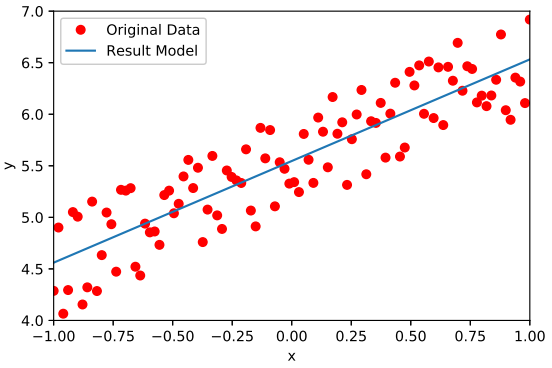

FIGURE 6. One-dimensional input linear regression.

and kernel SVM are all capable of handling non-linear datasets. Another form of SVM is the multiclass SVM, which is capable of classifying between more than two classes [56].

b: *Support Vector Regression (SVR)*

SVM can also be extended to solve regression problems [56]. The generic SVR function is defined by Equation (5) [56], where Φ transforms non-linear inputs of x into a higher dimension, the vector w and scalar b should be optimized to minimize the regression risk function defined by Equation (6) [56]. In Equation (6), C is a constant that represents penalty to errors and Γ represents the cost function. Equation (7) [56] defines this cost function with ϵ as the least-modulus loss.

$$f(x) = w \cdot \Phi(x) + b \tag{5}$$

$$Rreg(f) = C\sum_{i=0}^{l}\Gamma(f(x_i) - y_i) + \frac{1}{2}||w||^2 \tag{6}$$

$$\Gamma(f(x) - y) = \begin{cases} |f(x) - y| - \epsilon, & \text{if } |f(x) - y| \geq \epsilon \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

Finally, similar to the SVM, the optimal parameters can also be found by constructing the Lagrangian function as Equation (8) [56]. In this equation, function k is the kernel function to transform inputs into high-dimensional vectors. The variables α_i and α_i^* are the solutions for this optimization problem.

$$L = \frac{1}{2}\sum_{i,j=1}^{l}(\alpha_i^* - \alpha_i)(\alpha_j^* - \alpha_j)k(x_i, x_j)$$
$$-\sum_{i=1}^{l}\alpha_i^*(y_i - \epsilon) - \alpha_i(y_i + \epsilon); \tag{8}$$
$$\text{Where}, \sum_{i=1}^{l}\alpha_i - \alpha_i^* = 0, \text{AND} \sum_{i=1}^{l}\alpha_i, \alpha_i^* \in [0, C]$$

c: *Linear Regression*

Linear regression provides an approximation of the relationship between different data domains. In an example of one-dimensional input, the linear regression model is created in the form of the line of best fit (Figure 6). The authors in [57] gave a generic model of linear regression with multiple outputs. However, to simplify the process of demonstration, a single-output model is given by Equation (9). x and β of Equation (9) represent the input vector and the weight vector respectively.

$$f(x) = \beta \cdot x \tag{9}$$

The mean squared error (MSE) is computed to be utilized as the loss function (Equation (10)). The variable n is the number of data in the training set, x_i represents the ith input vector and y_i represents the ith real output.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(f(x_i) - y_i)^2 \tag{10}$$

d: *Logistic Regression*

The logistic regression solves the binary classification problem. The output of logistic regression is a value between 0 and 1. Thus, providing the confidence level of the prediction. Equation (11) demonstrates the logistic regression model, which is based on the Sigmoid function [58]. Similar to the linear regression, β and x are the input vector and the weight vector, respectively.

$$f(x) = \frac{1}{1 + e^{-\beta \cdot x}} \tag{11}$$

In order to find the optimal β, the method of maximizing likelihood is leveraged [58]. Equation (12) is the loss function. Similar to the linear regression, x_i is the ith input vector and y_i is the ith real output.

$$g = \prod_{i=1}^{n} f(x_i)^{y_i}(1 - f(x_i)^{y_i})^{(1-y_i)} \tag{12}$$

However, to ensure this loss function can be processed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

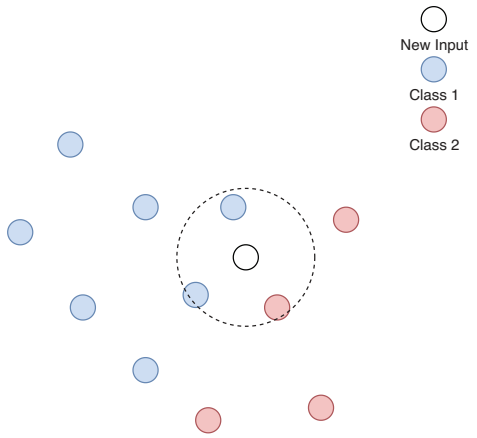

FIGURE 7. KNN inference with three neighbors.

with an optimization algorithm such as gradient descent, the problem is converted to maximizing the logarithm of the likelihood. This function is presented by Equation (13) [58].

$$log(g) = \sum_{i=1}^{n} y_i log(f(x_i)) + (1 - y_i) log(1 - f(x_i)) \quad (13)$$

The authors of [58] also provide the general form of the logistic regression using the Softmax function, which incorporates the ability to solve multi-class classification problems.

e: *K-Nearest Neighbor (KNN)*

KNN is mainly used for classification tasks. The model is built by plotting all training dataset in the feature space. When a new data point is inputted for inference, the model finds K nearest data points in the training set and provides an output based on the majority label of these nearest data points [38]. In order to calculate the distances, distance metrics such as the Euclidean distance, L-infinity norm, angle, Mahalanobis distance, and Hamming distance can be adopted [38]. Figure 7 demonstrates KNN with three nearest neighbors. The major label of the neighbors is class 1. Therefore, the new input data point is also labeled as class 1.

f: *Decision Tree (DT)*

The authors of [59] emphasized that the main objectives of DT classifiers are to limit the classification error to an insignificant level, to classify with high accuracy beyond the training dataset, to achieve incremental updates with new training data, and to structure in a simple form. To achieve the above objectives, algorithms are required to build a DT. Here the ID3 algorithm is used as an example to illustrate DT.

ID3 uses the concept of entropy to construct the DT. Equation (14) describes the calculation of entropy, where A is a vector of input features, x_1 and x_2 represent the two classes [60]. Entropy is calculated with all vector A in a tree node.

$$H(a) = \sum_{A} [-P(x_1|A) log_2 P(x_1|A) - P(x_2|A) log_2 P(x_2|A)] \quad (14)$$

New tree nodes should be created with minimal entropy [59]. Therefore, the first step of ID3 is to find an attribute within the input vectors to produce child nodes with the minimal entropy. Then, the input vectors in the root are split according to the attribute to produce the child nodes. Next, if a child node contains input vectors with only one class, the splitting process is terminated for this node and continued with the next child node. On the other hand, if the child node contains input vectors with more than one class, the algorithm repeats the first step with the child node recursively [60].

g: *Ensemble Learning*

The authors of [61, p.1] defined ensemble learning as "methods that combine multiple inducers to make a decision..." Therefore, as an advantage, models compensate errors of other models. The authors of [61] also divided ensemble methods into the dependent framework and the independent framework. In the dependent framework, the construction of the current model depends on the output of the previous model. An example is the AdaBoost algorithm, where the current model considers the error in the previous model. Gradient boosting machines also adopts a similar concept [61].

The independent framework includes multiple models, which are built independently from each other. Some examples of these methods are bagging, random forest, random subspace methods, error-correcting output codes, rotation forest, and extremely randomized trees [61]. Random forest is described in the next part of this subsection.

h: *Random Forest*

The random forest is an ensemble learning method based on DT [61]. It consists of multiple DTs. Each DT is trained by a random subset of the training data. Also, another random subset of the attributes is produced for the creation of new child nodes. Therefore, the algorithm only examines part of the attributes for an attribute of the best split. Furthermore, this randomness provides a low correlation between trees, avoiding the domination of a few strong attributes [62].

i: *Naïve Bayes Classifier (NB)*

NB is a supervised learning algorithm based on the Bayes rule (Equation (15)). The Bayes rule provides a model of the conditional probability of a result Y with the given input or the condition X. This algorithm is generally applied to classification problems. In classification problems, Y is from a discrete set of classes. Moreover, an input X belongs to the Y giving the greatest $P(Y|X)$ [63].

$$P(Y|X) = \frac{P(Y)P(X|Y)}{P(X)} \quad (15)$$

The NB model consists of the probability of a class Y and the joint probability of attributes (Equation (16)). Therefore, the model is constructed by estimating $P(Y)$ for every class

Y in the training set and the conditional probabilities of each attribute $P(X_i = a_i|Y)$ for every class.

$$P(Y = y_i|X = a_0, a_1, ..., a_i) = \frac{P(Y = y_i)P(X = a_0, a_1, ..., a_i|Y = y_i)}{P(X = a_0, a_1, ..., a_i)} \quad (16)$$

j: ***Bayesian Network (BN)***

NB models assume that all attributes are independent of applying the Bayes rule. However, in the real world, the correlation between attributes is inevitable [63, 64]. BN is a classifier that is not limited by the assumption of attribute independence. A BN can be represented by Equation (17), where G is a directed acyclic graph, where nodes represent the different events and the edges represent the dependency. The symbol Θ contains the Conditional Probability Table (CPT) for all possible values of the attributes and their conditions [64].

$$B =< G, \Theta > \quad (17)$$

The learning process is divided into two phases. During the first phase, the graph structure is determined and then in the second phase, the CPT is constructed [65]. The structure can be determined by an expert or learned by data with score-based structure learning methods and constraint-based structure learning methods [66]. The goal of score-based methods is to find a structure that provides the maximum score of a score function. For example, the Bayes Dirichlet equivalent uniform and the Bayesian Information Criterion. In the first step of score-based methods, the algorithm provides a score of suitable parents for every node. Then, parents are assigned to nodes to maximize the scores and to avoid cycles. On the other hand, constraint-based methods use conditional constraints to update the model. An example is the PC algorithm. When using the PC algorithm, the graph starts as a fully connected undirected graph. Edges are removed according to the result of CI tests. This method is repeated until no edges can be removed [67]. After obtaining a graph structure, CPT can be constructed to obtain a full model.

k: ***Kernel Bayes Rule (KBR)***

The KBR extends the Bayes rule by applying kernels to represent probabilities in reproducing kernel Hilbert spaces. Moreover, the prior and likelihood can be expressed by data, which does not require a distribution model [68].

l: ***Gaussian Process Regression (GPR)***

GPR is a non-parametric regression method as the complexity is determined by the data [69]. GPR utilizes the Gaussian Process (GP) to model the function between the input X and output Y. GP is an infinite dimension version of the multivariate Gaussian distributions [69]. GP can be defined by a mean and covariance function. The mean value is usually set as zero and the covariance function can be modeled by a kernel function representing the dependence between different function outputs for different input X [69]. The GPR learning process adjusts hyperparameters of the kernel, such as the length-scale, signal variance, and noise variance [69].

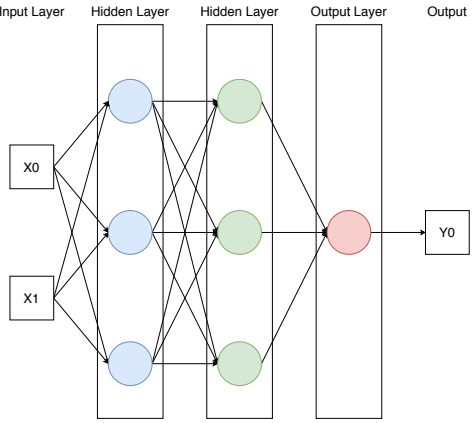

FIGURE 8. Sample Feedforward Neural Network Architecture.

m: ***Collaborative Filtering (CF)***

CF algorithms provide recommendations to a user from experiences of other users [70]. CF operates under two assumptions: Opinions of users do not change over time; Users with similar characteristics provide similar opinions. With these assumptions, CF can be implemented to provide a decision basis for product promotion, social media recommendations, e-commerce reputations, and even strategy [70].

n: ***Feedforward Neural Network (FFNN)***

A sample model of the FFNN is demonstrated by Figure 8. An FFNN contains an input layer, an output layer and one or multiple hidden layers [71].

$$f(X) = f^{output}(f^{hidden2}(f^{hidden1}(X))) \quad (18)$$

Equation (18) [71] provides the general form of the sample model. In these layers, the input layer consists of the input vector, and the hidden layers can be represented in the form of (19) [71], where W is a matrix of coefficients, X is the input vector, B is the bias vector, and g is the activation function. W and B can be learned through the backpropagation algorithm. Whereas, g is chosen by the data analyst to provide nonlinearity [71]. Some candidates of g are the ReLU function, the Sigmoid function, and the Tanh function. Finally, the output layer defines the output type of the model. If the output layer is a Softmax function similar to logistic regression, the FFNN provides the output of discrete values, which solves classification problems. On the other hand, if the output layer provides continuous values like linear regression, the FFNN solves regression problems.

$$f(X) = g(WX + B) \quad (19)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

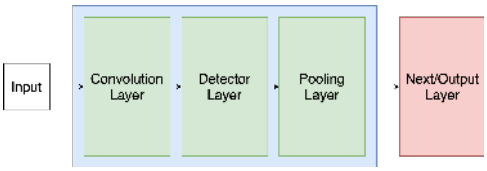

FIGURE 9. General Convolutional Neural Network Architecture.

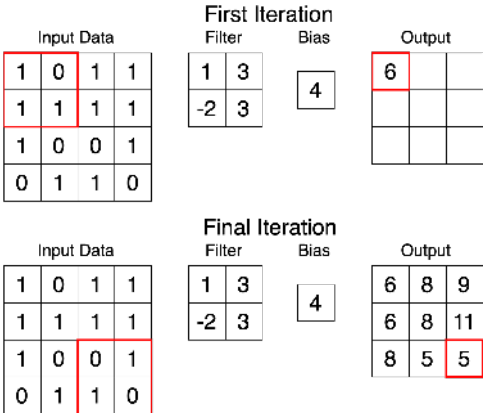

FIGURE 10. 2D Convolution Filtering.

o: *Convolutional Neural Network (CNN)*

CNN is a special type of FFNN. CNNs also process input data in a layer-by-layer style. The major motivation of CNN is to reduce the number of parameters to be trained [72]. Figure 9 demonstrates the general architecture of CNNs. A full convolutional layer group consists of the convolutional layer, the detector layer, and the pooling layer. In the convolutional layer, the input data is processed by a convolutional filter. This filter is in the form of a vector for one-dimensional data and matrix for two-dimensional data. The filter sweeps through the input data as a moving window, and during each iteration, the dot product of the filter matrix and the current region is calculated. Figure 10 provides an example of the first iteration and the final iteration of convolutional layer calculation with 4×4 input and a 2×2 filter.

After the convolutional layer, the detector layer processes the data as a hidden layer with the ReLU activation function. The ReLU function provides nonlinearity to the network [71]. Finally, a filter is also used in the pooling layer. Similar to the convolutional layer, the filter in the pooling layer also sweeps through the input. However, the filter only represents the area for the current iteration. Pooling calculation could be simply obtaining the average or the maximum of the filter area [72]. CNN is widely used for image processing.

p: *Recurrent Neural Network (RNN)*

Unlike the basic FFNN, which only accepts one input a time, RNNs accept several inputs [73]. In terms of time-series data, individual data points are processed at once in the sequence of time [73]. As shown in Figure 11, the output of the current hidden state H^t is generated from the input X^t of the current

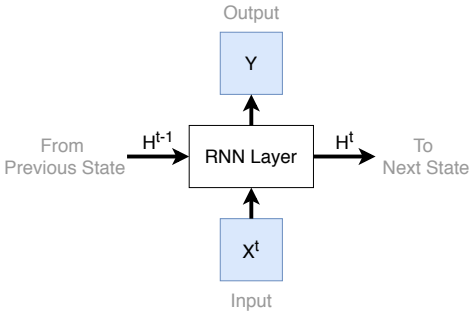

FIGURE 11. RNN Layer at time t.

time state and the output X^{t-1} of the previous time state, recursively [73]. Finally, if only one output is required (for classification or regression), the output Y is calculated from the final hidden state [73].

q: *Long Short-term Memory (LSTM)*

Since gradient propagates through multiple stages in RNNs, issues such as gradient explosion and gradient vanishing arise [73]. To address these issues, Long Short-Term Memory (LSTM) is proposed as variants of the RNN [73]. The LSTM incorporated an additional cell state to enhance long term memory [74]. Also, the additional forget and input gates are utilized to forget and insert information into the cell state [74].

r: *Random Neural Network (RandNN)*

The RandNN is a type of RNN. Excitatory impulse signals of "+*1*" and inhibitory impulse signals of "-*1*" are transmitted between the neurons of RandNN [75]. The neuron state or potential at a certain time is represented by a non-negative integer. This potential increases when the neuron receives an excitatory impulse and decreases when the neuron emits a signal. The neuron emits signals when its potential is positive. Also, the acceptance of an inhibitory signal outside of the network decrements the neuron potential [75]. The RandNN can be applied in multiple fields such as associative memory, optimization, texture generation, magnetic resonance imaging, function approximation, mine detection, and automatic target recognition [75].

2) Unsupervised Learning Algorithms

The two major types of unsupervised learning models are principal component analysis (PCA) and K-means clustering. PCA is used as a technique to compress data. This is important for IoT applications, such as wireless sensor networks (WSN), with limited throughput and energy [76]. The K-means algorithm is used for the clustering of multiple sensors. By dividing the monitored field into areas using the unsupervised K-means clustering, the complexity of data gathering and processing are reduced [76]. Some other unsupervised learning algorithms are also explained further in this subsection.

a: ***K-means***

The K-means algorithm produces a classification model through clustering [77]. It aims to generate multiple K centroids from the dataset. Data points close to a centroid forms a cluster [77]. The centroids are initialized by choosing random data points from the dataset. Then, data points are assigned to the cluster of the nearest centroid. Next, the new K centroids are calculated by averaging the assigned data points within their clusters. The above steps are iterated until the centroids are stable, or the algorithm reached a preset number of iterations [77]. With the centroids calculated, a data point can be classified by computing the distance towards the centroids. The new data point belongs to the cluster of the closest centroid [77].

b: ***Density-Based Spatial Clustering of Applications with Noise (DBSCAN)***

DBSCAN is another clustering method similar to K-means. However, compared to K-means, DBSCAN does not require a predefined number of K centroids. Also, DBSCAN can identify noises. Moreover, the shape of the cluster can be arbitrary [78]. DBSCAN has two hyperparameters the minimum number of neighbor points $minPoints$ within the distance R [78]. To construct the clusters, DBSCAN iterates through all points in the dataset [78]. If an unvisited data point has more than $minPoints$ neighbors within R, the data point is marked as a core point, and a new cluster is created. After that, recursively, all previously unvisited neighbors of the core point are visited and added into the cluster. Also, if the neighbor point is another core point, the two clusters would merge [78]. If a data point has less than $minPoints$ of neighbors within the range R, the data point is classified as noise [78].

c: ***Hierarchical Clustering Analysis (HCA)***

HCA is a clustering method, where the data sample is recursively merged or split to form a tree diagram [79]. HCA methods can be divided into agglomerative hierarchical clustering and divisive hierarchical clustering. Agglomerative hierarchical clustering is the bottom-up approach, where each data point forms its own cluster, and similar clusters merge until the desired architecture is obtained. On the other hand, divisive hierarchical clustering is the top-down technique as it starts with a huge cluster containing the whole data sample. Then, the cluster is divided to form the tree [79]. Merging and division decisions are made with similarity criteria. The three different sets of criteria are single-link clustering, complete-link clustering, and average-link clustering. For the three clustering methods, the distance between two clusters is calculated as the shortest distance between any two members from different clusters, the longest distance between any two members from different clusters, and the average distance between any two members from different clusters, respectively [79].

d: ***Expectation Maximization (EM)***

The EM algorithm computes maximum likelihood estimations for latent variables [80]. The algorithm consists of the Expectation (E) and Maximization (M) steps. The E step computes the missing data from current function parameters. During the M step, the function parameters are updated to maximize the log-likelihood of the estimated latent variables [80]. The E and M steps are repeated until the model converges slowly to a local maximum [80].

e: ***Gaussian Mixture Modelling (GMM)***

The superposition of multiple Gaussian distributions can approximate any continuous density through the adjustment of their means, covariances, and coefficients [81]. Unlike the parameters of a single Gaussian model that can be determined directly by the maximum likelihood method, GMM is trained using EM in an iterative way [81]. GMM can be applied to solve clustering problems [81].

f: ***Principal Component Analysis (PCA)***

PCA reduces the number of attributes in a dataset by transforming the original inputs into another set of vectors with low information loss [82]. Dimensionality reduction is achieved by eliminating components with a lower variance. These components are detected through the computation of the eigenvectors and eigenvalues of a covariance matrix from the original dataset [82]. A component with a higher eigenvalue indicates more information contained. Therefore, features can be extracted by choosing the corresponding components or eigenvectors with higher eigenvalues [83].

g: ***MultiDimensional Scaling (MDS)***

MDS is another dimensionality reduction technique. However, unlike PCA, MDS preserves the distance or difference between sample cases instead of the variance [84]. Stress, the loss function of MDS is defined as Equation (20), where d_{ij} is the difference between sample cases i and j in the original data space, and D_{ij} is the distance between i and j in the lower dimension or projected data space [85]. MDS consists of four steps [86]. In the first step, a squared distance matrix is computed from the data points in the original data space. Then, the matrix B is computed by applying double-centering to the squared distance matrix. After that, the eigenvalues V and eigenvectors Q of matrix B can be obtained. V_m is a matrix of the first m eigenvalues greater than zero, and Q_m is a matrix of corresponding eigenvectors. Finally, the coordinate matrix can be calculated by multiplying Q_m and $V_m^{\frac{1}{2}}$ [86].

$$Stress = \frac{\sum_{i=1,j=1}(d_{ij} - D_{ij})^2}{\sum_{i=1,j=1} D_{ij}^2} \tag{20}$$

h: ***Diffusion Maps (DM)***

DM is also an algorithm for dimensionality reduction [87]. In contrast to PCA and MDS, DM unravels the potential

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

manifold structures in the dataset [87]. The DM algorithms initiate by defining a kernel and a kernel matrix. Through normalization of the kernel matrix, the diffusion matrix can be acquired. Finally, DM utilizes n numbers of the most dominant eigenvectors from the diffusion matrix to project the dataset from the original data space to n-dimensional diffusion space [88].

i: *Window Sliding with De-Duplication (WSDD)*

WSDD is used to mine patterns from system events sorted in chronological order [89]. WSDD utilizes a sliding window over the training dataset to learn patterns in a brute force approach. The algorithm is capable of detecting both frequent sequential patterns and periodic sequential patterns [89]. To increase efficiency, the algorithm stores mined patterns in a hashmap and avoided mining duplicate patterns. The pattern itself is stored as the key in the hashmap, and the count of the pattern is stored as the value. Finally, only patterns detected over a minimum count are returned as the output of WSDD [89].

j: *Autoencoders (AE)*

The AE is a neural network consisting of the encoder, code, and decoder components [90]. The encoder maps the raw input to the output of the code component, and the decoder reconstructs the raw input from the output of the code component. AEs can be used for feature reduction as the output of the code component from a trained AE holds near lossless information of the raw input [90].

k: *Hopfield Neural Network (HNN)*

The HNN is a type of RNN for solving optimization problems [91]. Each neuron provides non-linear outputs through a sigmoid function. All neurons are interconnected with each other to restrict and revise the outputs of each other. Each connection includes an interconnection weight. Each neuron contains a user adjustable input bias [91]. The neurons update according to the energy function (Equation (21)), where T_ij is the weight of the connection between neurons i and j, V is the output of a neuron [92]. The HNN neurons evolve until a local minimum of the energy function is reached [92].

$$E = -\frac{1}{2}\sum_{i \neq j} T_{ij} V_i V_j \tag{21}$$

l: *Self-Organizing Map (SOM)*

The SOM is a type of neural network that can perform clustering similar to the K-means [77]. In each iteration, the neuron closest to a randomly selected data point moves towards the data point by a preset learning rate [93]. Neurons within the preset neighbor range of the first neuron also move towards the data point. The learning rate and the neighboring radius delays over the number of iterations [93].

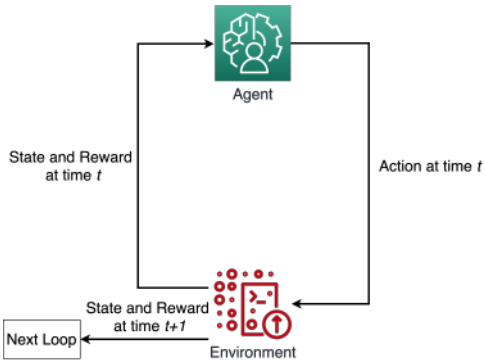

FIGURE 12. Agent-Environment Relationship. [41]

3) Reinforcement Learning Algorithms

The goal of reinforcement learning is to solve the problem of Markov decision processes (MDP). MDP is a sequential decision problem. As demonstrated in Figure 12, any action made by the agent will influence the environment and generate a reward. The goal of reinforcement learning is to maximize long-term rewards [41]. Q-learning, a type of reinforcement learning, is used to solve routing problems in IoT networks. Unfortunately, most of these algorithms are based on wired networks [94]. In WSNs, energy, processing power, and storage might become a bottleneck for distributed reinforcement learning routing algorithms [37]. Reinforcement learning algorithms aim to provide high-level intelligence to IoT applications.

a: *Temporal-Difference (TD)*

TD learning includes various model-free reinforcement learning algorithms, which require no model of the environment [95]. TD algorithms bootstrap or update the estimates based on current estimations. The value function is updated at every step of TD [95]. There are three fundamental types of TD-based learning algorithms mentioned in the sections after. The on-policy TD algorithm **SARSA** learns the action values from the current policy, while the off-policy algorithm **Q-learning** learns from the optimal policy [95]. Finally, a third type of TD learning, the **Actor-critic learning** learns both a policy (Actor) and value function (critic) [96]. Actor-critic learning is always on-policy as the "critic" needs to learn from and correct the TD errors from the "actor" or the policy.

b: *Least-Squares Policy Iteration (LSPI)*

LSPI is a model-free off-policy reinforcement algorithm [97]. LSPI is also an approximate policy-iteration algorithm, where the value function and policy representation are approximated. Therefore, compared to tabular methods, the policy search process is more efficient for LSPI [97]. Also, LSPI is based on least squares temporal difference learning [97]. Thus, as TD learning methods update incrementally, data efficiency of LSPI can be preserved [95].

4) Other Relevant Machine Learning Techniques

a: *Transfer Learning*

By adopting transfer learning techniques, a model trained to solve one problem can be transferred and adapted to solve a different problem [98]. This prevents time-consuming labeling processes. Transfer learning can be categorized into inductive transfer learning, transductive transfer learning, and unsupervised transfer learning [98]. In the inductive transfer learning setting, the domains can be the same or different, but the tasks are different for the two problems. Whereas in transductive transfer learning, the tasks are the same, and the domains are different. Finally, in unsupervised transfer learning, similar to inductive transfer learning, the tasks are different. However, unsupervised transfer learning performs unsupervised learning tasks in the target problem [98].

b: *Federated Learning*

Federated learning is a technique of multiple users training a common machine learning model without leaking their local dataset to other users [99]. There is the horizontal federated learning technique, where different datasets share the same features, but different sample cases [99]. On the other hand, vertical federated learning can be applied to datasets with more overlapping sample cases and different features [99]. Finally, federated transfer learning is suitable for datasets with different sample cases and features [99].

B. PHYSICAL LAYER APPLICATIONS

One major application of machine learning influencing IoT end devices is communication control. The authors in [100] used Q-learning for transmission power control to reduce the unnecessary waste of power due to interference. This model is only tested under the scenario of one-to-one transmission. A scenario of multiple sources toward multiple receivers should be tested.

The authors of [101] explored the usages of deep learning in end-to-end communication systems. The authors adopted the AE to replace different compensation techniques during the transmission of data. Data is encoded between transmission and decoded after transmission to protect the payload during transmission. Another application is the implementation of CNN for modulation classification. This is a prerequisite for developing an intelligent receiver.

Machine learning algorithms increase the energy consumption of IoT devices. Therefore, it is important to apply energy preservation techniques. The authors of [102] concluded that the two major energy preservation methods are energy saving and energy harvesting. Most of the energy saving techniques are implemented through the estimate and control of the uptime of end devices [100, 103, 104, 105, 106, 107, 108]. The rest of this subsection focuses on machine learning-based energy saving techniques. The authors of [103] established ARIIMA or A Real IoT Implementation of a Machine-Learning Architecture for reducing energy consumption. This is an IoT architecture that uses machine learning to forecast end device usage to control the up and downtime of IoT end devices. The aim is to reduce energy consumption. The authors compared different methods of calculating the loss of the predicted outcome. However, the authors did not link energy efficiency improvement to any specific machine learning algorithms.

The authors of [105] utilized the Naïve Bayes Classifier for calculating the optimized uplink period for IoT data collectors. The goal of this work is to optimize the uplink time for power efficiency and preserve the accuracy of data.

The authors from [107] used a single hidden layer feed-forward neural network to predict the power usage based on smart meters. With these predictions, the power suppliers can balance the power production with consumption to avoid power wastages. Also, individual home devices can be controlled to relieve the grid pressure at power peaks.

The authors of [106] used logistic regression, KNN, and Naïve Bayes algorithm to increase the power efficiency of smart buildings. Light, temperature, and motion data of a room are fed into the models to determine whether if people are present in a room. In conclusion, this work only determines the existence of people. Nevertheless, further work needs to be done on the development of an energy efficient device control scheme based on the predictions of these machine learning models.

The authors of [108] extended the model for predicting human presence in smart buildings. A random neural network model is applied with inputs of carbon dioxide level and temperature readings to predict the number of occupants in a room. This model is used to control the heating, ventilation, and air conditioning (HVAC) systems. HVAC devices will be turned off to save power if no occupants are detected in the room.

The authors from [104] pointed out that the manual labeling of training data is time consuming in supervised learning algorithms. Therefore, the authors proposed an energy saving scheme based on unsupervised learning. The WSDD algorithm is used to extract patterns of device behavior from historical data.

C. NETWORK LAYER APPLICATIONS

The authors of [109, 110] summarized existing network layer applications using machine learning algorithms. These applications are IoT device identification, network routing, traffic profiling, traffic prediction, traffic classification, congestion control, resource management, fault management, QoS and Quality of Experience (QoE) management, and network security. Table 1 links these applications to implemented machine learning algorithms. However, these applications alone might not be feasible to deal with the complexity of networks such as 5G, Tactile Internet, and Industry 4.0 requirements. Furthermore, an autonomous network structure is required.

1) Self-organizing networks

The increasing network complexity and device numbers for 5G and beyond networks are inducing conflicting demand

TABLE 1. Network applications and related machine learning algorithms. [109, 110]

Applications	Machine Learning Algorithms
IoT Device Identification	KNN, SVM, GMM, decision tree, ensemble learning, random forest
Network Routing	LSPI, Q-Learning, n-step TD, SARSA
Traffic Profiling	K-means, Clustering
Traffic Prediction	FFNN, SVR, KBR, LSTM, GPR
Traffic Classification	SVM, NB, HCA, KNN, DT, K-means, Random Forest, FFNN, DBSCAN
Congestion Control	EM, DT, Random forest, KNN, FFNN
Resource Management	FFNN, RandNN, SVM, HNN, RNN, Q-Learning, TD, BN
Fault Management	BN, FFNN, DT, SVM, Ensemble Learning, Linear Regression, Autoencoders, K-means, EM, RNN, SOM
QoS and QoE Management	FFNN, DT, Random Forest, NB, SVM, KNN, SVR, Q-learning
Network Security	FFNN, Ensemble Learning, DT, BN, NB, SVM, KNN, Linear Regression

over network resources and routing decisions. Therefore, self-organizing networks (SON) are required to reduce the complexity of managing these networks [111]. Management functionality of SONs consists of self-configuration, self-optimization, and self-healing. Self-configuration processes automate network design, network planning, and network deployment. After that, the self-optimization functionalities maintain the network performance and conduct routine network operations [112]. Finally, self-healing functionalities focus on fault detection and recovery [113].

The authors of [114] organized machine learning in SONs into four modules: sensing, mining, prediction, and reasoning. Sensing involves the detection of network anomalies and routine events. Therefore it contains functionalities of self-optimization and self-healing. Mining aims to classify services to help the network to optimize its performance. Moreover, mining belongs to the self-configuration functionalities. Finally, reasoning could apply to the offline parameter tuning during self-configuration and the online parameter tuning for self-optimization during network runtime.

The authors of [115] categorized machine learning applications on SONs according to the three functionalities. In Table 2, the self-configuration applications are operational parameters configuration, neighbor cell list configuration and radio parameters configuration. In Table 3, the self-optimization applications consist of backhaul, caching, coverage and capacity, mobility, handover, load balancing, resource optimization, and coordination. In Table 4, the self-healing applications include fault detection, fault classification and outage management. Table 2, 3 and 4 only include the algorithms that are relevant to supervised learning, unsupervised learning and reinforcement learning. Therefore, controller models, Markov models, and heuristics algorithms are out of the scope of this article.

The authors from [116] promoted self coordination as a fourth functionality group of SONs. Their work demonstrates that the current design of standalone management functionalities of SONs could lead to conflicting parameter adjustment between distinct functions. This work also concludes that DT, Q-learning, actor-critic learning, and SVM can be solutions for self-coordination.

The authors from [117] proposed another method to avoid collision between different functionality results. Their distributed Q-learning model considers both base station power allocation and user quality of service. Q-learning consists of a list of actions, a list of states, and a list of rewards. The actions are the power allocation for the base stations. The states are the ring that the agent is covered with current power allocation. Finally, the rewards are calculated considering the higher capacity of the base station and better user quality of service.

The network applications for traditional networks in Table 1 could be applied to support the SON functionalities. The authors of [118] emphasized that the result of traffic forecasting and prediction can increase the performance and accuracy of all other SON functionalities. The authors tested three types of machine learning models for traffic forecasting. The first type of model is autoregressive algorithms. This includes linear or polynomial regression. The second type of model is neural networks and finally, the authors used GPR for traffic forecasting. The authors also mentioned that this application can be further extended for QoS management and congestion control, providing possible use cases for models in the traditional networks. To improve the current management scheme in 5G and beyond networks, the implementation of SDN and Network Function virtualization (NFV) architectures in SONs fulfills the intelligence, automation, management, and optimization requirements [119]. In this architecture, machine learning works at the core to enable intelligent network management. This work also demonstrates that traffic classification as an essential application provides results affecting consecutive decision making processes.

D. EDGE COMPUTING APPLICATIONS

1) Edge Computing Hardware

The development of edge computing hardware enables machine learning on the edge level. Table 5 includes some of the representative edge computing devices. These devices can be classified into three device types. The first type is the board devices. Board devices are standalone embedded computers that run machine learning algorithms independent of external devices. The second type is the accelerator devices. These

TABLE 2. Machine Learning applications in self-configuration. [115]

Applications	Description	Machine Learning Algorithm
Operational Parameters Configuration	Configuration of the base station for basic operations.	SOM
Neighbor Cell List Configuration	Neighbor discovery, Self-advertisement	N/A (Control-based algorithms)
Radio Parameters Configuration	Transmission power, radio angle, topology configuration.	Q-Learning

devices cannot operate alone. Accelerator devices often act as an add-on to provide extra machine learning capabilities to embedded boards, personal computers, and other devices. The final type is smartphone chips. Smartphone chip manufacturers like Qualcomm, Hisilicon, Samsung, and MediaTek are pushing machine learning processing to mobile devices. Most of these chips rely on an AI accelerator to provide real-time machine learning processing capabilities.

2) Machine Learning on the edge

Machine learning applications on the edge layer can be separated into two major types. The first type aims to offload part or all of the existing functionality to the edge layer. This type of application is defined in this article as process offloading applications [46, 130, 131, 132]. The second type of application is referred to as sole functionality applications in this article. Sole functionality machine learning models often perform subtasks, which assist the main task on the cloud. The machine learning model of these subtasks is different from the model of the main tasks [133, 134, 135, 136]. Table 6 summarizes all the works with different motivations for applying edge computing.

The motivation for process offloading applications is the limited resources of devices. The authors from [130] pointed out that low latency is essential for vehicle-to-everything applications. This work classifies vehicle-related applications into critical applications, high priority applications, and low priority applications. Critical applications include vehicle control systems, system monitoring, and accident prevention. These applications must be deployed on the very edge to the vehicle for a near-instant response. High and low priority applications include navigation and entertainment. These applications should be deployed on edge servers to enhance the computational capability of end user devices. This also ensures a relatively low latency.

The authors of [131] applied a similar offloading scheme to general machine learning web applications. The aim of this work is to offload computation power demanding machine learning tasks from embedded devices to an edge server. To achieve this, the edge device transmits a snapshot of the execution state before processing a machine learning task to the edge server. This method is independent of the type and model of the machine learning algorithm. However, the size

TABLE 3. Machine Learning applications in self-optimization. [115]

Applications	Description	Machine Learning Algorithm
Backhaul	Connection between user, base station and the core network.	Q-Learning
Caching	Temporarily storing functions and services on the base stations	CF, K-means, Game Theory, Q-learning, Transfer Learning
Coverage and Capacity	Managing tradeoff between network coverage and network capacity	SOM, Q-learning
Mobility	Locate and predict the location of the user.	Naïve Bayes classifier, FFNN, SVM, DT, K-means
Handover	Realtime change of channel parameters when the user is using the channel. Often associated with mobility management when users move between cells.	FFNN, SOM, Game Theory, Q-learning,
Load Balancing	Intelligently balancing network load	Q-learning
Resource optimization	Allocation and prediction of network resource usage.	FFNN, K-means, SOM, Game Theory, Q-learning, Transfer Learning
Coordination	Minimizing the interference between two different functionalities.	DT

TABLE 4. Machine Learning applications in self-healing. [115]

Applications	Description	Machine Learning Algorithm
Fault Detection	Detect and locate the fault	Naïve Bayes classifier, SVM, K-means, SOM, PCA
Fault Classification	Determining source of the fault, Classifying the fault	Naïve Bayes classifier, DT, Transfer Learning
Outage Management	Detection of outage, Outage compensation	KNN, FFNN, SVM, DT, CF, K-means, SOM, Q-learning, PCA, MCA, DM, MDS

of a snapshot is still enormous for embedded devices.

The authors from [46] further revealed that edge computing could also be used to protect user privacy. Their application uses a neural network to recognize certain objects from live streaming video. To protect user privacy, the first few layers of the neural network are offloaded to the edge servers. This also reduces energy consumption for the whole system, since processing is distributed among the network. However, as the users still need to send raw information to edge servers to be processed, privacy leakage remains an issue. This issue can be solved by directly deploying these first layers of the neural network to the end device. As a result, users only send processed intermediate data to the network. All the works above only use edge computing primitively to offload computation requirements. However, machine learning by edge computing should leverage some unique properties of edge devices. The authors of [132] proposed a collaborative edge-centric learning method to train machine learning models. Each sensor contains a model that is trained locally using only data from that sensor. Training locally allows sensors to utilize contextual parameters to improve model accuracy. After training the local models, only the parameters of the models are sent to the sink from the sensors. This method reduces network overhead and energy consumption during training.

Different from the previous process offloading applications, sole functionality applications improve the performance of the system by performing a different subtask of the major task in the cloud. Earlier motivations are also related to the limited resources of devices. The authors of [135] utilized multiple filters, including CNN and SVM, to drop blurry and unwanted image data at the edge layer. The usage of filters reduces the processing power required on upper layers to create a training dataset for other applications.

Similarly, The authors from [133] also applied data cleansing on the edge layer to filter blurry images. Data cleansing is done by K-means in their food recognition system. Image segmentation is further applied as a data preprocessing method to reduce the load of the cloud server. However, the significance of this work is the utilization of locational data as a unique data type provided by edge devices. Furthermore, the authors used the locational data as a basis for collaborative recognition on the cloud layer.

To enhance localized service, the authors of [136] implemented network traffic prediction via LSTM on the edge cloudlets of a healthcare system. The purpose of this machine learning model is to predict bidirectional traffic between the cloud and the cloudlet to control data transmission rate and data caching frequency. These improve the quality of service and the reliability of data. As the LSTM model is deployed locally on cloudlets, the control decisions of the model are different between different cloudlets due to the different local network traffic.

Similarly, the authors from [134] also used machine learning to predict future sensor data. This is based on multivariable regression and LSTM in their traffic monitoring system. These models are implemented on the edge servers to provide parameters for determining the quality of the video to be sent from the edge servers to the cloud. Therefore, this application aims to reduce network traffic by control data transmission from edge servers during non-critical events. The origin of these advantages is the increase of connectivity by introducing more edge servers to the system.

As machine learning applications on the edge attract much attention, the emergence of TinyML provides further advancement of these applications. TinyML combines embedded IoT technologies with machine learning [137]. It has the advantage of low bandwidth usage and latency like other edge computing applications [30]. On the other hand, TinyML applications aim to minimize energy consumption (below 1 mW). To deploy a machine learning model on such a low consumption device, model size also needs to be minimized. Balancing between model size and accuracy is a challenge for implementing TinyML applications [137].

E. EDGE-CLOUD COLLABORATION

In the traditional IoT architecture, machine learning algorithms on the cloud layer usually perform analytical tasks. However, novel applications are proposed utilizing the collaboration between edge and cloud layers. Table 7 includes some edge-cloud collaboration methods.

A most common type of edge-cloud collaboration is the sole functionality applications from the subsection above. The healthcare system from [136] is an example. The system aims to classify and store data at different nodes of the cloud server. Data is collected from mobile devices and passed to the cloudlet layer. In the cloudlet layer, LSTM is implemented to predict network traffic. The prediction results are

TABLE 5. Machine Learning Edge Computing Hardware.

Reference	Hardware Series	Recent Model	AI Processor/Accelerator	AI Performance	Device Type
[120]	Nvidia Jetson	Jetson AGX Xavier	512-core NVIDIA Volta GPU with 512 Tensor Cores	32 TOPs	Board
[121, 122]	Intel Neural Compute Stick	Intel Neural Compute Stick 2	Intel Movidius Myriad X Vision Processing Unit	4 TOPs	Accelerator
[123, 124]	Coral Dev Board	Coral Dev Board	Google Edge TPU ML accelerator coprocessor	4 TOPs	Board
[124, 125]	Coral USB Accelerator	Coral USB Accelerator	Google Edge TPU ML accelerator coprocessor	4 TOPs	Accelerator
[126]	Qualcomm Snapdragon	Qualcomm Snapdragon 855 Mobile Platform	Using CPU, GPU and DSP	Undisclosed	Smartphone Chip
[127]	HiSilicon Kirin	HiSilicon Kirin 980	Dual Neural Processing Unit	Undisclosed	Smartphone Chip
[128]	Samsung Exynos	Samsung Exynos 9820	Neural Processing Unit	Undisclosed	Smartphone Chip
[129]	MediaTek Helio P Series	MediaTek Helio P90	MediaTek APU 2.0	Undisclosed	Smartphone Chip

used for data transmission rate control and caching frequency control. Then, data is transmitted to an upper network layer. This layer utilizes a FFNN to classify traffic. Finally, these data are stored on the cloud according to the classified traffic types. In this application, the edge layers support upper cloud layers by completing subtasks. The result of the subtasks helps the cloud layer to perform the main task.

Edge assisted training is another type of edge-cloud collaboration. The authors from [135] used CNN and SVM to filter out images on the edge layer. This filter is to prevent corruption of the training on the cloud. Hence, it decreases the time required for an expert to create a training set.

The authors from [138] used federated learning to create an AE model for anomaly detection. A local version of the AE model is trained on every edge device using its local datasets. Then, the weights of these local models are transmitted to the cloud server and aggregated to form one AE model. This cloud level AE model is redistributed to the edge devices for local anomaly detection. As less data is sent from the edge to the cloud, this method reduces bandwidth demand during training and ensures that the training dataset is not corrupted due to data transmission. However, this method only considers one model across the system.

The authors of [139] extended training to multiple models. This is achieved with a machine learning model management module on the cloud server. This module accepts sensor data from the edge layer and uses these data to train different machine learning models. Then, the machine learning model selector selects and distributes a suitable model for every edge platform based on device performance and characteristics. This method optimizes network performance as the most suitable model is deployed for every device.

Another edge-cloud collaboration method is process offloading scheduling. The authors from [46] addressed that edge servers have limited bandwidth. Thus, scheduling of cloud process offloading should be implemented to avoid network congestion. The authors of [140] implemented a similar scheduling method on 5G networks. They use deep Q-learning to schedule server app migration on mobile edge servers. This method aims to provide users with an optimal quality of service. The authors from [141] incorporated cross-layer communication into process offloading decisions. In this work, end IoT devices can communicate both with Unmanned Aerial Vehicle (UAV) edge servers and satellite cloud servers. If the IoT devices loose connection with UAV edge servers, the IoT devices could offload their computation tasks to the satellite cloud. A deep actor-critic learning method is proposed considering energy consumption and network delay to solve this scheduling problem.

This section summarizes many machine learning algorithms, hardware and applications. The usage of machine learning from a network perspective are described. Machine

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

TABLE 6. Motivation of Edge Computing.

Reference	Application	Edge Motivation	Application Type
[130]	Vehicle-to-Everything	Enhance computational capabilities Reduce latency	Process Offloading
[46]	Video Recognition	Process offloading Reduce latency Reduce energy consumption Protect privacy	Process Offloading
[131]	Machine Learning Web App	Process offloading	Process Offloading
[132]	Smart IoT Application	Reduce network overhead Reduce energy consumption	Process Offloading
[133]	Food Recognition	Data preprocessing Data cleansing Reduce latency Reduce energy consumption Location awareness	Sole Functionality
[134]	Traffic Control	Reduce network Traffic Increase scalability Ensure mobility Reduce latency	Sole Functionality
[135]	Graphical Expert System	Process offloading Data preprocessing Data cleansing	Sole Functionality
[136]	Healthcare System	Reduce latency Reduce network traffic Increase reliability Increase security	Sole Functionality

learning applications in the physical layer and network layer are elaborated. Scheduling and management of different network resources and process are major applications of machine learning on these two layers. Then, for the cloud layer, the applications of machine learning that enable edge-cloud collaboration are illustrated. Edge computing aids cloud applications through process offloading and edge-only functions (sole functionality). However, this only shows collaboration in the application layer (Edge-Cloud). Collaboration between lower layers or cross-layer machine learning applications are still limited. The need of cross-layer machine learning models and other limitations of current applications are further discussed in Section XIII.

V. MISSION CRITICAL COMMUNICATION

An important dimension of IoT 2.0 is the mission critical communication based systems, which address the situations where human life and any form of infrastructure can be at risk. Mission critical communication currently takes the form of mission critical machine-to-machine (M2M) communication, or machine type communication (MC-MTC), where machines need to communicate with each other to perform various tasks such as coordination, sensing, and actuation. Mission critical communication systems put stringent requirements of ultra-reliable and low-latency communications (URLLC) and system availability [142]. The M2M communication systems which do not involve the mission critical element are referred to as low-cost M2M or massive MTC (mMTC) with low-power consumption and massive connectivity [143]. In this section, we review important use cases of mission critical communication systems and recently proposed physical (PHY) and higher-layer mechanisms to meet the desired requirements of URLLC in these mission critical communication networks.

TABLE 7. Applications Involving Edge-Cloud Collaboration.

Reference	Application	Collaboration Method
[46]	Video Recognition	Process offloading decisions.
[140]	5G Mobile Network	Process offloading decisions.
[141]	General IoT Application	Process offloading decisions.
[135]	Graphical Expert System	Data cleansing to aid training.
[138]	Anomaly Detection	Training using Federated Learning.
[139]	Indoor Condition Prediction	Dynamic model selection.
[136]	Healthcare System	Collaborating the results of different subtasks on different layers.

A. IMPORTANT APPLICATIONS OF MISSION CRITICAL COMMUNICATION NETWORKS

In order to protect citizens and infrastructure during disasters and emergencies, different public safety organizations are put in place [144, 145]. The emergency first responder is the most important entity in all emergency management agencies. Public safety communication (PSC) systems used by these agencies for coordinating teams and providing quick emergency-response are regarded as mission critical because they need to be ultra-reliable, resilient, and secure while meeting other stringent network functionalities [146]. Public warning systems (PWS) also come under the umbrella of PSC systems as they share many of the characteristics of mission critical communications. An important use case of PWS is the earthquake and tsunami warning system. During the last few years, there has been a significant increase in the interest of advancing the PSC systems. The authors of [144] presented a detailed survey on wireless communication technology while covering the different aspects related to regulatory, standardization, and research activities in PSC systems. The main focus in this work is on Europe and the USA. In [145] a comparative analysis of legacy and emerging technologies for PSC is presented. The authors of [146] discussed the use of broadband technologies for public safety, considering existing LTE specifications. The authors from [147] proposed a software architecture design as well as a set of distributed protocols to meet the strict requirements of PSC networks. The use of wireless networks in the mining industry for mobility support, rapid deployment, and scalability within dynamic environments is another use case of the PSC system. The authors of [148] discussed the mission critical requirements of PSC systems for open-pit mining, and a framework is proposed that integrates mine and radio network planning.

Automated transportation systems are meant to provide mission critical services to self-driving vehicles, connected cars, road safety, and traffic management systems. These intelligent transportation systems can increase the efficiency of traffic management agencies and provide numerous benefits, including a considerable reduction in the road-accidents rate. However, to get these systems realizable, the stringent requirements of MC-MTC networks should be fulfilled.

Vehicular connectivity or Vehicle-to-everything (V2X), is another important use case of MC-MTC in which time-critical data exchange takes place under three different scenarios: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-personal device moving at pedestrian speeds (V2P) [149]. UAVs, also known as drones, have potential usages in many mission critical communication systems due to their inherent features of mobility, flexibility, and adaptive altitude [150]. Such UAVs assisted MC-MTC networks can be used in the transportation of important goods in emergency situations being handled by the public safety and rescue systems. UAVs can be part of existing cellular networks as new types of user equipment (UE) and flying base stations. UAVs as flying base stations can help increase the coverage, spectral efficiency, and QoS in the MC-MTC supported cellular networks [150]. The authors of [151] presented a comprehensive survey of different types of promising solutions for the smooth integration of UAVs into cellular networks.

Industrial automation involving time-critical processes requires highly reliable data transfer links between sensors, actuators, and controllers, and thus is an important application of MC-MTC networks. Detailed performance requirements of different MC-MTC network applications are listed in [152]. Health monitoring systems for remote patients and remote robots for surgeries are potential applications of MC-MTC networks. Similarly, both augmented reality (AR) and virtual reality (VR) systems require very low end-to-end latency. Another important use case of mission critical communication networks is found in the smart grid, which is an advanced form of conventional power grid having capabilities of automation, monitoring, and communication. The key features that distinguish smart grids from the conventional electrical power grid are two-way communication, demand-side management, and real-time billing. All these features require mission critical communication infrastructure for smart grids [153].

1) PHY Layer Considerations for Mission Critical Communication Networks

Table 8 summarizes works related to PHY layer considerations for mission critical communication networks. For both licensed and unlicensed bands employing URLLC, many promising PHY and medium access control (MAC) layer techniques are discussed in [154]. The following techniques

are among the PHY layer mechanisms proposed specifically for MC-MTC networks to meet the associated URLLC requirements.

a: Short packet transmission

In contrast to the conventional wireless communication systems, the traffic in MC-MTC networks generated by different types of devices and sensors contains short packets where the size of metadata (control information) is comparable with that of the actual information payload. Thus, new principles are required to design wireless protocols supporting short packets. The authors of [155] reviewed information-theoretic principles developed for communication systems generating short packets. These principles are applied in different communication scenarios such that the control information is optimized for short packet transmission.

The probability that a network provides the required level of QoS is called the network availability, and in the context of MC-MTC networks, QoS is the set of desired reliability and latency levels [156]. To meet the stringent requirements of URLLC in MC-MTC networks, high SNR is required at the receiver, and SNR of the received signal depends upon the range between the transmitter and the receiver. The authors of [156] proposed a framework to optimize the available range and transmission duration in MC-MTC networks employing short packet transmission. To enhance network availability, the base station is equipped with multiple antennas, while the end nodes have only one antenna. This framework can be used in different transmission modes, including device-to-device, amplify and forward, and decode and forward.

b: Physical layer authentication (PLA)

Although, the use of short packets in mission critical communications systems can lead to the satisfaction of the stringent requirements of URLLC; the impact of finite block-length coding can cause serious physical-layer security issues. PLA is another promising way of meeting the reliability requirement in MC-MTC systems employing short packet transmission without using cryptographic methods. A common model considered in this regard is composed of three nodes. One node called Bob needs to exchange information with the other node called Alice in a secure way. There is a third node called Eve, physically distanced in the network which can sniff information being exchanged between Bob and Alice, and thus can send wrong information to the communicating parties. PLA aims to provide information security at the physical layer such that the interference from the undesired nodes can be avoided. A PLA based mechanism is proposed in [157] as a lightweight authentication in reliable MC-MTC systems. In this work, the receiver employs a GMM to make two clusters of the channel estimates, and based upon this clustering, it predicts the actual transmitter. The authors of [158] presented a queuing theory based detection and delay performance analysis of a PLA protocol for single-input multiple output (SIMO) MC-MTC networks. This protocol is investigated under different possible attack cases. The authors of [159] analyzed the secrecy throughput of MC-MTC networks while considering single and multiple antenna access points (AP) in the presence of an eavesdropper equipped with multiple antennas, and presented the corresponding latency-reliability tradeoff analysis.

2) Programmable Mission Critical Communication Networks

5G is envisioned to provide many heterogeneous services. By using network slicing, we divide a single physical network into multiple isolated virtual networks such that each virtual network takes care of a specific service [160]. Network slicing help manage these diverse network services efficiently. Thus, the design and implementation of MC-MTC networks supported by 5G can take advantages offered by the network slicing techniques. In [160], different aspects of network slicing are discussed in the context of 5G. A network slicing based logical network architecture for 5G systems is presented in [161], which covers all the fundamental aspects of a cellular communication system. The authors of [162] presented a mathematical model of network slicing for three main service groups of 5G, such that each group of services is provided with a dedicated set of policies. The authors of [163] proposed a network slicing design customized for different time mission critical vehicle-to-everything services. The authors of [164] discussed non-orthogonal slicing of the radio access network (RAN) resources among enhanced Mobile Broadband (eMBB), mMTC, and URLLC devices communicating in the uplink to a common base station. Because of the heterogeneous services being addressed, this RAN slicing is termed as non-orthogonal multiple access (H-NOMA), which is different from the conventional NOMA techniques which share radio resources among devices of the same type with homogeneous requirements.

SDN and NFV are promising techniques to implement network slicing. SDN opens new ways to implement MC-MTC networks, and some recent studies provide insight regarding the potential usage of SDN in the design of future MC-MTC networks. In [165] an SDN and NFV based solution is presented and evaluated for critical infrastructure use cases. The authors of [166] presented a software-based framework for 5G systems and its hardware implementation MC-MTC networks. The authors also presented a practical framework for an experimental study that uses different types of network traffic to prioritize mission critical traffic. This framework is used to evaluate the end-to-end performance of the proposed systems. The authors of [167] proposed an SDN based architecture for 5G to address critical communications. Two important switching paradigms named Bare-Metal and fully virtualized switching, are used to evaluate the performance of the proposed system. The authors of [168] proposed a multi-controller architecture that provides a dynamic load balancing scheme for SDN based MC-MTC networks. This mechanism reduces the communication overheads by allowing the controller to send the load status to the load balancer only when the load exceeds a prescribed threshold. This helps reduce the communication overheads in MC-MTC networks

employing SDN. Communication in smart grid systems is an important use case of MC-MTC networks. In this regard, the authors of [169] presented a comprehensive survey on the utilization of SDN architectures in smart grid systems.

While addressing the mission critical communication design challenges at the PHY and MAC layers, it can be observed that the current approaches are primarily base station-centric and lead towards centralized decision-making strategies. Although these works aim to reduce latency and target to achieve ultra-reliability, the centralized control strategies may cause additional latency, which might not be avoided in these methods [170]. This triggers the need to design new solutions that involve less control signalling and employ distributed decision-making approaches. Moreover, in the current literature, mission critical communication network design considers the heterogeneity caused by three primary services of 5G, namely: URLLC, eMBB, and mMTC. However, different mission critical applications may have different latency-reliability criteria, and this type of variation in the QoS requirement creates another level of design complexity that needs to be addressed accordingly. Hence, these gaps in the literature can open new avenues for the research community.

VI. IOT SCALABILITY

Universal scalability is discussed in this section. Universal scalability is separated into hardware scalability, network scalability and service scalability. Table 9 defines these different scalability concepts.

Hardware scalability is the ability of a piece of hardware to be extended to cope with different environmental, network, and service requirements. A common method for implementing hardware scalability is offloading part of the device functionality to a server [171, 172]. The authors of [171] proposed an architecture that extends device functionality through device virtualization. Additionally, this work demonstrates device virtualization in the case of a multi-protocol scenario. As a solution, virtual gateways are deployed on fog servers to process the packets received by the end devices. However, adding functions of another functionality group (for example, adding image sensors to a transceiver device) still requires modification from the hardware level. To avoid modification from the hardware level, the concept of synthetic sensors is proposed [172]. Synthetic sensors can be separated into the device level and the server level. The device level is assembled by sensor tags capable of sensing data from multiple sensing dimensions. These sensing dimensions are low-level data types include vibration, audio, camera, temperature, humidity, air pressure, illumination, color, motion, magnetic field, and Received Signal Strength Indicator (RSSI). Then, low-level data is transmitted to the server level. On the server level, machine learning algorithms process these low-level data and convert them into valuable results to users. In conclusion, synthetic sensors create a platform with all the raw data types required and extend its functionalities through server-based machine learning analytics.

Network scalability is the ability to dynamically scale resources up and down to process the incoming IoT traffic. A common method to ensure network scalability in wireless sensor networks is clustering. The authors of [173] reviewed common clustering algorithms. Their work outlines clustering into processes of cluster head election and cluster formation. Cluster head election is the process of choosing cluster heads from wireless devices, and these cluster heads gather data from other members of its cluster and transmit it towards the base station [173]. After the cluster heads are elected, other wireless devices advertise themselves to the cluster heads and form clusters around these cluster heads to join the network [173]. Therefore, new devices can easily join the network with the cluster formation process. As a result, scalability is achieved with clustering.

The clustering techniques assume devices in the network are homogeneous. However, in an IoT scenario, devices are heterogeneous [173]. As a solution, intermediate fog devices are utilized [174]. Similar to the cluster heads, these fog devices gather information from the end IoT devices and transmit it towards a centralized server. Different to the wireless sensor network scenario, fog devices are not chosen by algorithms. These devices are specialized as an intermediate server. The authors of [174] pointed out that as a new IoT device joins the network, the device drivers and services can be distributed on the fog devices to achieve a simpler integration process. Therefore, fog servers increase the scalability of IoT networks.

The extensibility of network coverage affects the availability of network services to mobile users. The authors of [175] explored antenna-based coverage and capacity optimization in cellular networks. Their work is based on two major phenomena. The first phenomenon is that the tilting of mobile network antennas affects network coverage and capacity. The second phenomenon is that there is a tradeoff between coverage and capacity. These phenomena are caused by an increase in the power of the received useful signal in a cell and the reduction of signal coverage due to antenna tilting. On the other hand, the authors of [176] addressed energy efficient parent selection of mobile IoT nodes.

To ensure further coverage, scalability induced by antenna tilting, online and dynamic antenna configuration using reinforcement learning can be applied to cellular networks [177]. This method also belongs to the SON self-optimization functionalities [115]. Finally, to further extend network coverage, satellites are incorporated to provide network backhaul for IoT networks. The usage of satellite backhauls provides advantages of cost efficient, ease of deployment, avoidance of damage from natural disasters, seamless coverage, and reliability [178]. This could be part of the universal coverage solution.

Service scalability emphasizes the ability to incorporate new services into the existing IoT system. The authors of [179] defined scalability requirements of IoT applications as explicit control flow, decentralized interactions, the separation between control and computation, and service location

TABLE 8. Summary of Recent Works Addressing Mission Critical Communication.

Reference	Communication Scenario	Challenges Addressed	Reliability and Latency Improvement Mechanism
[155]	Point to point, downlink multiuser, and uplink multiuser	Short packet transmission	Tradeoff between coding rate and packet length, data concatenation for multiple users, tradeoff between the probability of collision and packet error probability
[156]	D2D and cellular modes with single antenna users and multiple antenna base stations	Network availability for short packet transmission	Available range improvement by optimizing transmission duration
[157]	Point to point	Physical layer security	Clustering based upon channel estimates
[158]	Uplink transmission: single antenna users and multiple antennas base stations over a line of sight path	Physical layer security	Feature based physical layer authentication while considering the associated delays
[159]	Downlink transmission: single and multiple antenna base stations, single antenna actuator and multiple antenna eavesdropper	Physical layer security for short packet transmission	Blocklength optimization to maximize the secrecy throughput for different cases
[163]	Vehicle to everything communication	Slicing the RAN and core network for V2X communication	End-to-end network slicing for different scenarios of V2X communication use cases
[164]	Uplink multiuser	RAN resource management for heterogenous services for 5G	Non-orthogonal slicing of the RAN resources
[166]	Mission critical communication between a server and a mobile user	End-to-end reliability for high data rate	Software-based framework prioritizing mission critical traffic

transparency. This work also categorized IoT service interaction types into direct interactions, indirect interactions, event-driven interactions, and exogenous interactions. After the evaluation of the service interaction types with the scalability requirements, exogenous interactions are the only service interaction type, which satisfies all scalability requirements.

Exogenous interactions incorporate a coordinator to manage all service interactions with different devices and services. Therefore control is always managed by coordinators and is separated from service computation. From [179], this type of interaction is controlled with explicit control flow as the control flow is defined by the coordinators. Also, as a definition of exogenous interaction, the control is always separated from service computation. Furthermore, exogenous can be decentralized in a hierarchical manner. Finally, location transparency is provided by exogenous interaction because coordinators are controlling the service interactions, and location data is encapsulated during the process.

TABLE 9. Applications Involving Edge-Cloud Collaboration.

Reference	Type of Scalability	Definition
[171, 172]	Hardware Scalability	The ability of a piece of hardware to be extended to cope with different environmental, network and service requirements.
[173, 174, 175]	Network Scalability	The ability to dynamically scale resources up and down to process the incoming IoT traffic.
[179]	Service Scalability	The ability to incorporate new services into the existing IoT system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

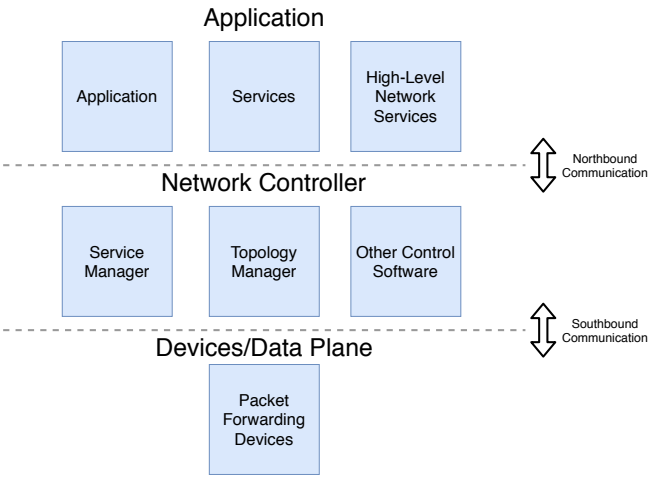

FIGURE 13. SDN Architecture. [180]

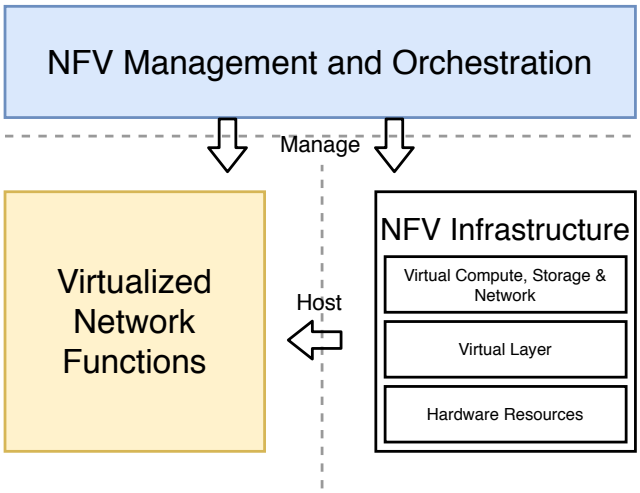

FIGURE 14. NFV Architecture. [182]

A. SDN INDUCED SCALABILITY

SDNs bring programmability into traditional networks. Forwarding devices such as switches and routers can be virtualized in SDNs. This is achieved through the separation of control plane and data plane. As a result, SDNs simplify network management, minimize the limitation from hardware, and are easier to extend network functionality [180]. The advantages of SDNs could also be beneficial to manage D2D communication in 5G networks [181].

From Figure 13, an SDN architecture consists of the application layer, the control layer, and the data-plane layer. The application layer consists of software applications communicating with the control layer, the control layer process requests from the application layer and manage network devices, and the data-plane layer is network infrastructure such as switches and routers [180]. NFV is another technique that leverages service virtualization to increase network scalability. European Telecommunications Standards Institute (ETSI) defines a standard for NFV architecture (Figure 14) [182]. This architecture is assembled by the virtualized network functions (VNFs), the NFV infrastructure (NFVI), and NFV management and orchestration. NFVI includes the physical resource, which hosts VNFs as virtualized software implementations of network functionalities. Both NFVI and VNF are all managed by the NFV management and orchestration module. The advantages of the NFV architecture are reduction of hardware implementation costs, increasing flexibility and scalability by hosting VNFs on hardware, faster service modification due to software-based deployment, improved operational efficiency due to possible automation and operating procedures, improved power efficiency by planning and offloading workloads. NFV architecture is also able to create software interfaces to associate elements from different vendors.

The authors of [183] pointed out that SDN and NFV can benefit each other. SDN controllers can be treated as a VNF

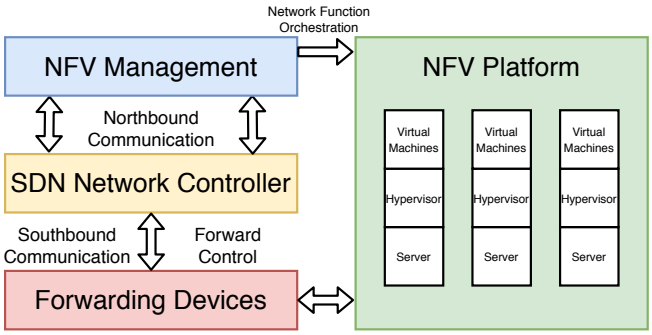

FIGURE 15. Software defined NFV Architecture. [183]

on the cloud providing flexibility to controller distribution. On the other hand, SDN provides its programmability to NFV, allowing communication between different VNFs. The combination of SDN and NFV further increases scalability. The authors of [183] also provided a software-defined NFC architecture that consists of the forwarding devices, the controller module, and the NFV Platform. From Figure 15, the forwarding devices are switches and routers from the data-plane layer of SDNs. These forwarding devices store forwarding tables to process a particular data packet. The forwarding tables are defined by the SDN controller. The SDN controller also controls NFV orchestration on the control module. Another function of NFV orchestration is to assign functions to the NFV platform, where servers host hypervisors supporting virtual machines running with the network functions [183].

The authors from [184] identified that in the environment of SDN and NFV, connecting and modification of virtual functions are complex due to multiple heterogeneous end-user demands and network parameters. Service function chaining could be a solution to reduce this complexity and

optimize the use of resources. The authors from [184] also categorized existing service function chaining models into six optimization types as follows: network latency minimization, resource utilization optimization, cost minimization, power/energy minimization, service level agreement based optimization and quality of service based optimization. Finally, the authors of [183] provided a vision of implementing service function chaining on the software-defined NFV Architecture. The optimal path of service chains is coordinated with the SDN controller fulfilling user requirements and resource constraints. Then, service chains are created from multiple VNFs, and data packets flow through the path of the service chains.

In this section, network and service scalability achieved with SDN and NVF are reviewed. The authors of [185] indicated the emerging network scalability issues trigger by the network management overhead in current networks with increasing size and dynamism. Autonomic or self-management of the networks (SONs) [185] could be a solution for these issues. On the other hand, IoT interoperability could be another solution to resolve scalability issues [186].

VII. IOT SECURITY

The diversified and ubiquitous use of IoT systems in foreseeable future necessitate the need of evaluating security and privacy requirements for various IoT technologies and applications. In this context, due to constrained resources of IoT end-devices, lack of host-based security measures, and data-enabled services, numerous threats emerge at different layers of IoT architecture.

A. PHYSICAL LAYER

Some of the noteworthy threats at physical layer include:

1) Eavesdropping: Attackers can introduce devices similar to the end nodes in an IoT system to sniff wireless traffic and capture sensitive user data.
2) Hardware Failure: IoT device hardware may fail due to manufacturing faults or as a result of a cyber-attack. This failure may lead to substantial damage to the IoT system as a whole or it may cause physical impairment to the users [187]. An example of such a successful cyber-attack is Stuxnet [188], that caused physical damage to a critical equipment installed at Iranian Nuclear Enrichment Facility.
3) Malicious Data Injection: Any persistent attacker can introduce a forged device to eavesdrop on the radio traffic, inject fabricated messages or flood the radio channels with fake messages to render the system unavailable to the legitimate users [189].
4) Man-in-the-Middle Attack (MITM): There is always a possibility that an attacker can tap and listen to the unprotected communications links between the end users and the network/applications servers. Such an attack is often called as (MITM) attack. A successful MITM attack may enable the attacker to eavesdrop the communication channel or to inject forged malicious data.
5) Sybil Attack: In this attack, a malicious node may present multiple identities by generating fake new identities or by impersonating other nodes. In the worst case scenario, multiple identities may be generated using a single physical device [190]. The attacker has the option to present all the Sybil identities simultaneously or one by one at different instances. A Sybil attack may affect the outcome of a voting-based fault tolerance system or a routing protocol.
6) Loss of Power: In order to abnormally drain the battery of an IoT device an attacker can bombard the node with a large no of requests (mostly legal) thus preventing it from going to sleep or energy saving mode.
7) Disclosure of Critical Information: It is not always the case that a communications channel is unprotected. Currently, most of the communications protocols especially the wireless protocols such as 802.15.4, LoRaWAN, SigFox, ZigBee, and WiFi, encrypt data during transmission. However, still a smart attacker may continuously monitor the wireless sensors traffic, for example, of a smart home and analyze the pattern of data traffic to differentiate between an idle mode or when an event occurs. Hence, even if the data is encrypted, the frequency of data traffic may infer critical information to the attacker that the house is empty. Therefore, he can plan a robbery.
8) Side-Channel Attacks: Other than intercepting the plain text or cipher text messages, attackers may resort to gather and analyze side-channel information about the IoT device hardware components. This information may include, data about processing time or power consumption while encrypting or decrypting data packets of varying lengths generated from different sensors/end nodes [191]. Such an analysis may help the attacker to identify the duty cycle of various IoT devices based on the frequency of particular messages being transmitted.
9) Device Compromise. Most of the IoT devices designed for a particular application such as environmental monitoring, temperature, and pressure sensing, etc., are not security hardened, thus have weak authentication mechanisms or open debugging ports. Hence, these devices can easily be compromised by the malicious attackers. In an effort to demonstrate such an attack, security researchers in [192] exploited an open Universal Asynchronous Receiver/Transmitter (UART) interface of a home automation system controller. The sequence of actions adopted by the researchers to compromise an IoT device is shown in Figure 16. Once the attacker gains access to the device, he is able to view the start-up sequence. Hence, he can modify the boot parameters and gain low-level access to the device. Attacker may also brute force the root password and launch network layer attacks such as port scanning. In addition, the attacker may perform network traffic analysis. Attackers also have the option to fetch and analyze device firmware, find weaknesses and launch further attacks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

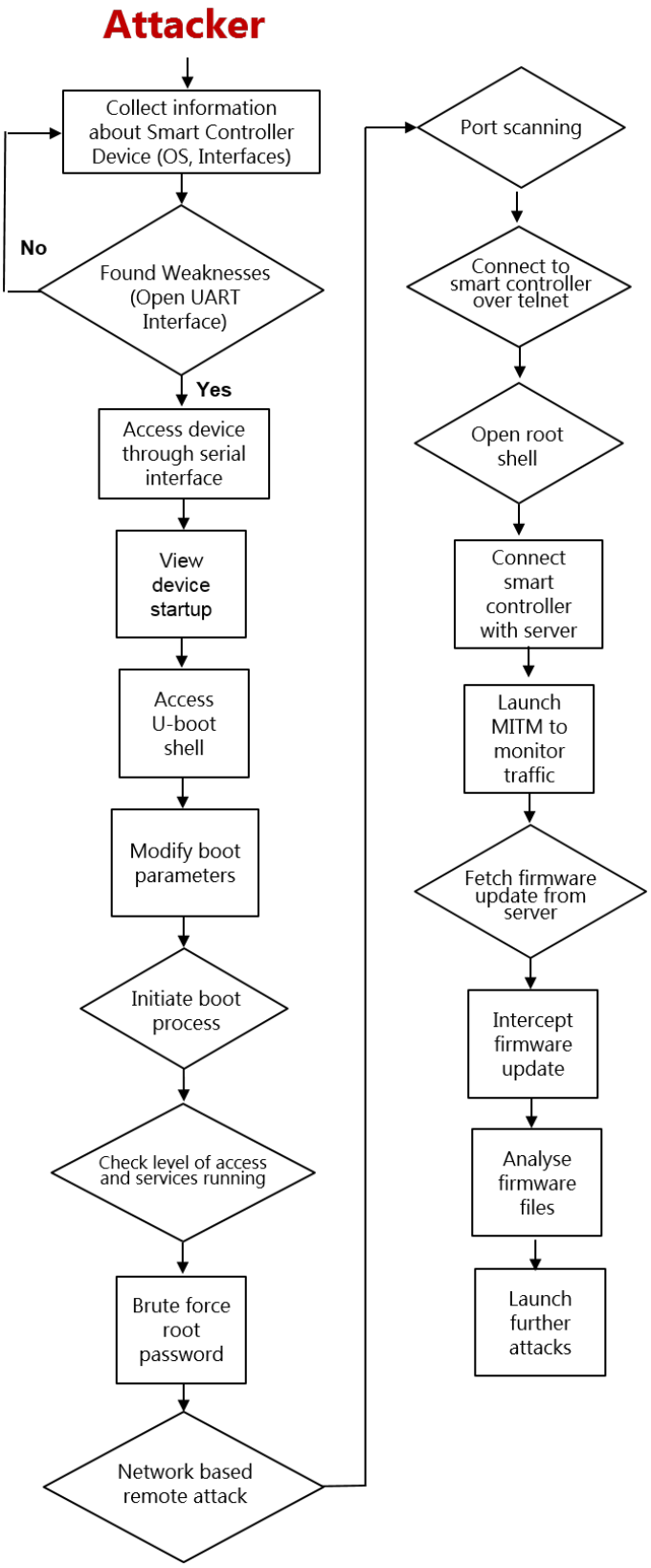

FIGURE 16. Sequence of a device compromise attack.

In another endeavor, security researchers compromised a smart meter device through an unsecured Joint Test Action Group (JTAG) interface and modified the identity of the device. The researchers also modified write permissions to an Electrically Erasable Programmable Read-only Memory (EEPROM) that stored the device ID. As a result of such a successful attack in real-world malicious users can use the spoofed device identity to feed altered power consumption data to the controller/gateway device [193]. Similarly, researchers also successfully compromised a Google Nest Learning Thermostat and Nike+ Fuelband SE fitness tracker by exploiting vulnerabilities in the boot process and some weaknesses in the physical design. The attack was successful despite the availability of secure transmission protocols such as Wi-Fi Protected Access II (WAP2) and Transport Layer Security (TLS) 1.2. In addition, the smart devices also had fairly strong authentication mechanism in terms of OAuth authentication tokens and Public Key Cryptography Standards VII (PKCS 7) certificates.

10) Node Cloning: Due to cost-effective solutions most IoT devices are developed without any hardware tamper-proofing. Therefore, it is very easy for a persistent attacker to forge and replicate these devices for malicious objectives. Such a replication is called "node cloning" [194]. An attacker can clone the devices either in manufacturing phase, or during the operational phase. During device manufacturing, an inside attacker can target and substitute a particular legitimate device with a similar, pre-programmed one for unauthorized purposes. Whereas, during the operational phase attacker has to resort to a carefully planned attack to compromise and clone an IoT device.
11) Invasive/Semi-invasive Intrusions: Invasive and semi-invasive intrusions are significant threats to IoT devices. By using invasive intrusion methods, attackers can steal the cryptographic primitives stored on the chip and may compromise any protocol utilizing that secret information. In a practical manifestation of such an attack, security researches in [195], successfully extracted the Advanced Encryption Standard (AES) Key from the internal memory of Actel ProASIC3 FPGA, by launching "Bumping Attacks" [196].

B. NETWORK LAYER

Most of the attacks are anticipated at network layer because it not only links multiple Local Area Networks (LANs) but also enables a connection to the Internet. Some of the threats that affect data security at this layer include unfairness, impersonation, Sybil, and interrogation attacks [197, 198, 199]. Similarly, numerous Denial-of-Service (DoS) attacks that threaten the availability of network services include; channel congestion, collision and battery exhaustion attacks [200, 201]. The battery congestion attack may be launched by increasing the frame counter value and spoofing of acknowledgment frames

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

[202, 203]. Correspondingly, hello flood attack, selective forwarding, wormhole attack, blackhole attack [200] and storage attacks [187] also threaten availability of network services. Some other DoS attacks may include exploitation of Carrier Sense Multiple Access (CSMA) protocol by transmitting on multiple channels [202, 201] and initiation of fake Previous Access Network Identifier (PANId) conflicts. DoS Attacks can also be launched by sending fake/false messages to a node, server [204] or a gateway device [205].

In addition, some of the threats to the security and integrity of the system include MITM, eavesdropping [189], spoofing [200], message fabrication/modification/replay attacks [189], unauthorized access to network, compromise of a device (done remotely using malware) [187], node replication [197] and insertion of rogue devices [206].

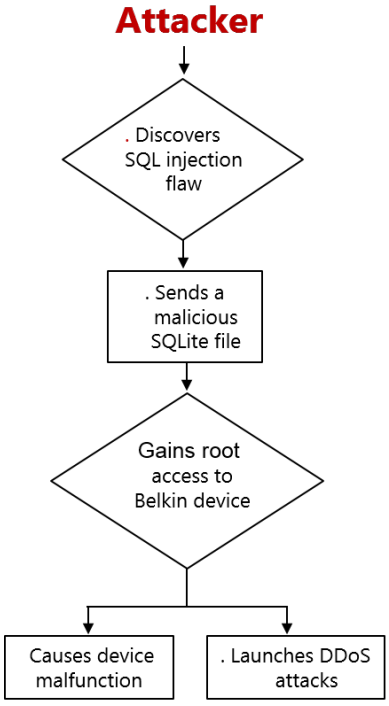

FIGURE 17. SQL Injection Attack on Belkin WeMo Switch.

C. FOG/EDGE LAYER

The introduction of fog/edge computing with IoT to reduce latency, decrease bandwidth, enhance computing power, increase storage and augment security is a paradigm shift from centralized cloud-based infrastructure [207, 208]. However, as fog/edge is believed to be a nontrivial extension of the cloud, hence certain new security and privacy issues have been identified in addition to the existing ones. Some of the significant security and privacy challenges include:

1) IoT device authentication.
2) Lack of trust measurement mechanism.
3) Absence of IoT device integrity check technique and detection of rogue devices.
4) IoT device security and user data security and privacy.
5) Non-availability of IoT-centric access control and intrusion detection system to avoid insider and external attacks.
6) Key management at end devices.

D. SECURITY AND PRIVACY ISSUES DURING DATA STORAGE AND ANALYTICS ON CLOUD

Today, the reliance on Big Data analytics to provide valuable business intelligence has paved the way for the integration of IoT and cloud computing. No doubt, cloud infrastructure has relieved IoT systems from issues involving scalability, constrained processing power, limited memory and power to run heavy applications [209]. However, like other IoT layers, the vulnerabilities in cloud interfaces can also become attack vectors. Therefore, the cloud gateways should be equipped with requisite security controls to restrict malicious actors from compromising security and privacy of user data [210].

Some of the major security issues in cloud-supported IoT systems include: Cloud services are provided under the centralized control of one trusted entity. Hence, the cloud is vulnerable to the single point of failure concerning security and privacy issues [189] including data manipulation [211, 212], and the availability of cloud services. Moreover, cloud also has trust issues, as the users have to put their trust in the entity that is providing cloud services and handling their data. Hence, users have no control over their data assets. Further concerns for user data include: Users do not know where their data is stored and what is happening to it. Who has access to it, and is there any unauthorized disclosure to the third parties. In regard to data manipulation, the cloud service provider has to be a trusted party as it has control over the data stored in the cloud and related services. Therefore, the cloud provider can manipulate user data [212]. Correspondingly, single point of failure also concerns the availability of services when the cloud servers are down because of software bugs, cyber-attacks, power problems, cooling and other issues, users find it difficult to access the cloud services [211]. Cloud is also vulnerable to un-authorized data sharing. For example, in the recent past, private data of 87 million users was provided by Facebook to a British political consulting firm “Cambridge Analytica” without user permission [213, 214]. Such a data breach results in irreversible data security and privacy issues.

E. APPLICATION LAYER

Most application developers focus more on efficiency and service delivery rather than security. As a result, applications remain vulnerable to numerous threats. Lack of application security, and weak authentication and authorization mechanisms enable attackers to compromise IoT devices using various attack vectors such as malicious code, and brute force attacks to guess the hard coded login credentials. The device compromise can then result in unwanted disclosure of sensitive information, elevation of privileges and data tampering. The attacker can also turn the infected devices into bots to

launch further attacks on other end devices or network applications [187]. Moreover, once an adversary gains an initial foothold on the IoT device through an insecure application he can also do the exploitation via binary patching, code substitution or code extension [215]. Correspondingly, some significant security risks to web-based IoT systems have been ranked by OWASP (Open Web Application Security Project) [216]. These risks include:

a) Injection flaws in SQL/noSQL Databases, Operating Systems (OS) and Lightweight Directory Access Protocol (LDAP). This vulnerability not only affects traditional Information Technology (IT) systems but also poses an equal threat to the IoT applications and database servers. In a practical manifestation of such an attack, researchers in [217] successfully compromised a smart home device, i.e., a Belkin WeMo Switch. As shown in Figure 17 firstly, the attacker discovers an SQL injection vulnerability in the IoT device. The adversary also discovers that the data is not encrypted during transmission between the Belkin WeMo Android Application and the Belikn device. He also finds that the authentication mechanism is lacking. The attacker then sends a malicious SQLite file to the device and resultantly gets root level access. Once inside, the attacker can alter the functionality of the device or he has the option of launching a DDoS attack. For example, The lamp is kept on for a long time irrespective of the rules defined by the user. It is imperative to mention here that once an attacker gains root level access to the device; he can even kill the firmware update process initiated remotely by the vendor. Hence, the device can be kept in the compromised state for as long as desired by the attacker or until the device is updated on site [218].
b) Malicious actors can steal user identities and compromise passwords, cryptographic keys, and session tokens due to incorrect session management and incorrect implementation of authentication in applications. For example, a user does not change the default username and password or the wireless router has hardcoded credentials for the admin account. Hence, researchers in [219] were able to hijack the session using ARP poisoning and gain access to the camera feed of the Withings Smart baby Monitor.
c) Security misconfiguration is one of the most common weaknesses. It implies insecure default configurations, open cloud storage, mis-configured Hyper Text Transfer Protocol (HTTP) headers, and overblown error messages that may contain sensitive information. An IoT device is insecure without secure configuration and timely upgrades of its OS and applications [218].
d) XSS (Cross Site Scripting): By exploiting this vulnerability, attackers can run an arbitrary JavaScript code in the browser of target systems [217, 220]. Resultantly, it can lead to the hacking of the smart devices and ultimately the theft of private data.
e) Security Issues in Application Layer Protocols: Security researchers have shown concern over the security issues in various application layer protocols such as HTTP, Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), and Extensible Messaging and Presence Protocol (XMPP) [221]. These protocols rely on TLS and Datagram Transport Layer Security (DTLS) for the security during communication especially in a client-server environment. However, these protocols are vulnerable to plain-text recovery attacks, as demonstrated by the researchers in [221]. Moreover, another significant issue with these protocols is that they were not designed to be used for resource constrained IoT devices. Subsequently, these protocols add additional traffic overheads with every connection establishment that ultimately drain the computing and power resources of IoT devices [222].

F. BUSINESS LAYER

Data received from IoT devices through web/application servers is stored and processed mostly in the cloud. The processed data is then used to provide various data-enabled services to the users, and third parties. This big data analytics is no doubt beneficial, but at the same time various security and privacy issues emerge. Users that are basically the data owners do not know where their data is stored and who has access to it. Moreover, cloud service providers may share some private information of the users with third parties without de-anonymization. Most of the tools currently being used to store and compute big data, such as Hadoop Distributed File System (HDFS) and MapReduce framework lack adequate security to protect sensitive user data [223]. Hence, there is a need to develop a comprehensive defense strategy to protect IoT systems from various security and privacy threats.

G. APPLICATION SPECIFIC SECURITY REQUIREMENTS

There are myriad of IoT applications that have significant impact concerning safety, security and privacy of people, in case of any security breach. All of these applications cannot be discussed here; however some of the critical ones are highlighted in the subsequent paragraphs.

1) IoT in Healthcare

IoT has revolutionized healthcare domain by connecting wearable healthcare devices, smart homes, hospitals, medical staff, and other processes. Such an integration is no doubt beneficial. However, being interconnected and remotely accessible, these services are vulnerable to major cyber-physical security risks [224]. Some of the significant security and privacy issues concerning Healthcare IoT infrastructure, and services include:

- Weaknesses in network access control mechanisms and threats to data authentication, integrity and availability [225].

- Due to the interconnections, a failure in one infrastructure can cause cascading failures among its dependent systems/processes [226].
- Unauthorized access to user data by third parties.
- Lack of role-based controlled access to patient data.
- Existing single party owned centralized systems to store and process user data provide single point of failure.
- Vulnerability to ransomware attacks [227].

2) Industrial IoT

The development of first Programmable Logic Controller (PLC) in 1968 by Modicon laid the foundations of classical industrial automation. This automation pyramid comprise of Enterprise Resource Planning (ERP) layer, Manufacturing Execution System (MES), Supervisory Control and Data Acquisition (SCADA) layer, PLC layer and sensing layer comprising sensors and actuators [228]. For a longtime the security of industrial systems was based on the principle of obscurity, i.e., by hiding the details about internal network and related technologies. However, with the increase in the level of automation, and reliance on remote access for ease in monitoring and control, the industrial systems have become a lucrative target for the cyber-attackers/hackers. In this context, Stuxnet was the game changer, that made the world realized that the security of critical infrastructure is a necessity [218]. Stuxnet is believed to be a targeted computer worm that was designed to sabotage CPS installed in Iranian Nuclear Enrichment Facility. It exploited four zero-day vulnerabilities in Windows-based systems to gain an initial foothold [229]. Stuxnet specifically targeted personal computers running WinCC/PCS-7 control software used for programming the PLCs [230]. It could act as a MITM attacker and mask the malicious code execution by replaying twenty one seconds of legitimate process input signals. The malware payload comprised rootkits which could hide its presence and was also equipped with stolen digital certificates to appear legitimate. The payload altered the speed of frequency converter drives (from specific vendors Fararo Paya from Iran and Vacon from Finland) to cause physical damage to over 900 centrifuges [188]. Other than malware attacks, the industrial systems are also vulnerable to numerous threats including: DoS, DDoS, ransomware, message spoofing, data integrity and non-repudiation, information disclosure, and elevation of privileges.

3) Smart city Security Requirements

The advances in IoT technologies and related smart gadgets have given birth to a new paradigm called "Smart Cities." That aims to dynamically optimize the use and availability of numerous tangible and intangible resources. However, due to reliance on IoT devices for sensing and initial processing of perceived data, and vulnerability of IoT devices to numerous cyber attacks, the attack surface for a smart city also increases. Hence, authors in [231] highlight certain necessary requirements to design a secure smart city. These requirements include: secure communication [232], secure booting of IoT devices [233], security monitoring and incident response strategy [231], secure software/firmware update and patching [234], authentication, identification, and access control [235, 236, 237], and data and application security.

VIII. SECURITY MEASURES

Figure 18 shows a defense-in-depth approach that acts as a guideline to protect IoT systems against threats at all the layers of IoT architecture. Not all the IoT applications may require all these measures. Depending upon the nature of IoT application, a combination of these guidelines may suffice.

a) Risk Assessment and Threat Modelling: For the development of an effective defense mechanism firstly, there is a requirement of carrying out the risk assessment for all processes, equipment (both hardware and software), stakeholders and information assets at each layer of IoT architecture. The aim of such an assessment is to identify the assets that are deemed critical for the business. Failure of any of which may cause significant security, privacy, financial and safety issues. It is followed by an appropriate risk treatment/mitigation process to minimize the damage of such events. Correspondingly, most of the information security standards such as International Standards Organization (ISO)-27001 [238], and National Institute of Standards and Technology (NIST) publication 800-30 [239] enforce risk management as an integral part of the overall controls. Any such standard can be followed until there are some IoT specific standards on board.

b) Preventive Measures: The primary objective of preventive measures is to mitigate the weaknesses which attackers can exploit to initiate a security breach. These measures include:

- Security by design: IoT solution architects should consider a non-zero likelihood of security breaches while planning, designing and developing an IoT system. It is very important that security should be enabled by design and users should have the option to change the security settings as per their personal requirements [240, 241]. Certain practices that help achieving security by design are: trusted environment for secure computing, security of all open/debugging ports, preserving integrity of the firmware/code, multi-factor authentication, and by default block all traffic at the ingress.
- Identity Management: An effective identity management mechanism not only protects against identity spoofing, and device replication attacks but also compliments network layer security protocols such as Transmission Layer Security (TLS), and IPSec [242].
- Tamper-Proofing: IoT device tamper-proofing is considered to be a potent defense against physical device compromise, unauthorized access, firmware modifications and device cloning [243, 244]. Moreover,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

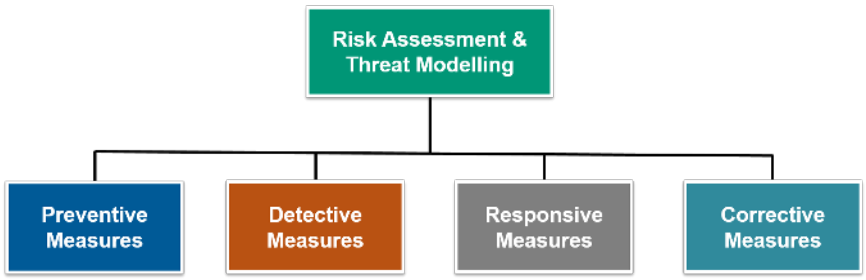

FIGURE 18. Defense-in-Depth Approach

complimented by a secure execution environment, it can protect against code modification and malicious payload execution attacks [242].

- Use of Pseudonymous Identities: Use of pseudonyms protects the users against most of the privacy threats by de-linking user identities from the Personally Identifiable Information (PII). It can be achieved by using Public Key Infrastructure (PKI), i.e., by issuing public keys to the users of an IoT system for authentication and authorization of various services. These public keys can be issued in the form of X.509 certificates by a trusted Certificate Authority (CA) [245].
- Identity-based Authenticated Encryption and Mutual Authentication Scheme: Such an authentication and data security technique not only protects against impersonation, MITM, and eavesdropping threats but also from data forgery, data modification, and message replay attacks [246, 247, 248].
- Homomorphic Encryption: To avoid privacy issues in a cloud environment where user data is processed, analyzed and shared with third parties, homomorphic encryption is considered to be an effective tool [249].
- Blockchain Technology: Since the success of Bitcoin, a cryptocurrency [250], blockchain has disrupted conventional IT industry. The inherent cryptographic security of blockchain protects against most of the data forgery, modification, replay and authentication threats. It also provides a transparent log of events that facilitates system audit at any time [251].
- Role-based Access Control: Issues related to the security and privacy of data and unauthorized access to the network services can be prevented by deploying role-based access controls [206].
- Secure Remote Access: Not only in private sector but in public organizations as well, sometimes the users are required to work from home. Hence, there should be a mechanism of remotely connecting users at their homes with the organization networks and systems. For example, use of a Virtual Private Network (VPN) service can protect against attacks on corporate networks and threats to sensitive Business Intelligence (BI) [252].
- Key Management: Secure management of cryptographic keys including generation, distribution, storage, revocation, and update is an essential requirement to protect against masquerading attacks and exposure of critical information.
- Network Segmentation: To curtail the effects of network or a node compromise using network segmentation is recommended to be an effective approach. Network segmentation can be achieved by defining de-militarized zones, physical isolation, VLANs, software-defined perimeter, application firewalls, and content-based filtering [253].
- Software-defined Networking (SDN) based Virtual Security: Network Virtualization using SDN can augment IoT device-level protection by implementing security at the network level, hence, reducing cost and add-ons for low-end devices [254].
- Use of self-encrypting drives/devices: Data privacy is one of the fundamental issues in this age of internet and smart technologies. Therefore, it is believed that use of self-encrypting drives and on-chip flash memories may provide requisite security by design against unauthorized disclosure of private user data [243].
- Security Awareness: In the tech savvy world, it is very crucial that organizations should invest in educating their employees on security concerns. It can be achieved through various workshops, seminars and periodic lectures on cyber threats and requisite precautionary measures.

c) Detective Measures: As the name suggests, even if an attacker is successful in gaining an initial foothold into any IoT system, the detective measures will help in identifying any malicious activity. Some of these measures may include:

- Secure Log Management: Most of the attackers/hackers try to wipe off their footprints after an unauthorized intrusion into a critical system. Hence, keeping a secure log of all activities in the network helps to expose any unusual activity or a security breach.
- Network Security Analysis: CISCO [255], and IBM [256] have developed various network security analysis tools that are helpful in detecting numerous

anomalies, malfunctions and security breaches.

- Edge Security Analysis: In addition to the network security analysis, edge security analytics facilitates isolation of security events at the source and limit attack spectrum [242].
- Network-level Security Measures: Network-level security measures to enforce cross-device security policies can easily detect manipulation of actuator actions based on malicious/modified sensors data [257].
- Device Attestation: If possible, there should be some mechanism of performing runtime IoT device code attestation to check for the presence of any malicious payload or modification in the original code. The successful code verification is expected to shrink the attack surface [258].
- Penetration Testing and Vulnerability Assessment: Periodic network penetration testing is always helpful in detecting weaknesses in all the layers of IoT architecture, web UI/APIs, and servers to initiate respective counter/response measures.

d) Responsive Measures: The best way an organization can respond to a cyber security incident is by preparing an effective incident response plan. Mostly, these plans are rolled out by a team usually called as Computer Emergency Response Team (CERT). These teams comprise skilled professionals including cyber security experts, information security auditors, legal experts, IT administrators and other specialized members. The primary objective of CERT is to develop and practice a diligent response plan against any security breach so that all the team members are clear about their responsibilities. The response measures are often termed as after-incident reactive measures, which include:

- Disconnect the affected system from the Internet.
- Isolation of the compromised devices/parts of the system allowing rest of the system to continue uninterrupted operation.
- Revocation and blacklisting of malicious nodes.
- Initiation of anti-tamper mechanism, in which, as soon as the hardware of the node is interfered with, the memory of the node that contains firmware and code should immediately be wiped off, and the node should only join the network after being physically activated instead of OTAA (Over-The-Air-Activation).
- Recover important business and personal data from the backup.

e) Corrective Measures: Once a security event has occurred and the compromised devices/parts of the system are identified and isolated, they need to be recovered to operational condition. There are two known methods of node restoration, i.e., self-recovery and remote attestation. In self-recovery, the faulty device performs integrity check of the code running on it and the last best configuration stored in read-only memory. If the validation fails, the device deletes the current code and re-installs the last best configuration. The device then restarts and performs validation of all its modules. Whereas, in the later method, the compromised/faulty device sends integrity report to the controller/gateway device for remote validation [243]. If the validation fails, a secure firmware update process is initiated by the verifier.

To conclude, Table 10 summarizes threats at different layers of IoT architecture, including physical, network, fog/edge, data orchestration/cloud, application, and business layer. Similarly, Table 11 highlights the essentials of defense-in-depth approach to secure IoT systems.

IX. IOT SUSTAINABILITY

While IoT technology has gone through a significant level of advancements in recent years, there are still a number of constraints associated with battery dependency, limited lifetime, and environmental pollution of these portable devices. Until now, energy has been one of the barriers to large-scale adoption and deployments in IoT devices. Integrating EH systems with IoT devices extend their lifetime, decrease energy costs, and reduce environmental pollution by using green energy sources [259]. Hence, self-powered IoT devices that can operate autonomously are an emerging topic of interest among researchers [260, 261]. Energy harvesting is a sustainable, cost-effective, green energy solution to provide an alternative energy source for remotely deployed IoT devices and sensors. Energy harvesting or scavenging is the process of collecting energy from freely available ambient sources, and EH is a device that converts ambient energy into DC power to supply Wireless Sensor Networks (WSNs), biosensors and IoT devices [262, 263, 264, 265, 266].

Depending on the type of energy available, there are a number of techniques for energy scavenging from ambient sources such as solar, thermal, mechanical sources (for example, wind, kinetic, vibration) and radio frequency (RF) waves. These sustainable sources are all in abundance and are produced in a pure form on our planet [266]. Harvested energy is often used for WSN, wearable electronics, and portable IoT devices [259, 267]. However, not all ambient sources are appropriate for energy harvesting in IoT applications.

Basically, the energy harvester (EH) integrated with IoT devices should produce at least milliwatts of power from the environment. Figure 19 shows generated DC power of different energy harvesting technologies and the power consumption of different electronic devices to demonstrate the usefulness of energy harvesting techniques for these devices [259].

A. ENERGY HARVESTER SYSTEMS IN IOT DEVICES

EH system converts ambient energy, such as solar energy, thermal, vibrational, or RF energy into usable electrical energy. According to Figure 20, an EH consists of three main components: power transducer, storage (bat-

TABLE 10. Threats to IoT

IoT Layer	Threats	References
Physical layer	Eavesdropping	[218]
	Hardware failure	[187, 188]
	Malicious data injection	[189]
	MITM	[218]
	Sybil attack	[190]
	Loss of power	[218]
	Information disclosure	
	Side-channel attacks	[191]
	Device compromise and node cloning	[192, 193, 194]
	Invasive/semi-invasive intrusions	[195]
Network layer	Unfairness and impersonation attacks	[197, 198, 199]
	Sybil attack	
	Interrogation attacks	
	Channel congestion and collision attacks	[200, 201, 202, 203]
	Battery exhaustion attacks	
	Hello flood attacks	[200, 187]
	Selective forwarding attack	
	Wormhole and blackhole attacks	
	Storage attacks	
	CSMA attack	[202, 201]
	PANId conflicts	
	MITM, eavesdropping and spoofing attacks	[204, 205, 189, 200]
	Remote device compromise	[187]
	Node replication	[197]
	Insertion of rogue devices	[206]
Fog/Edge layer	Issues concerning device authentication	[207, 208]
	Lack of trust mechanism	
	Threats to IoT device integrity	
	Vulnerability to insider and external attacks	
Cloud layer	Single point of failure	[189]
	Data manipulation	[211, 212]
	Threats to the availability of cloud services	
	Risk of unauthorized data sharing	
Application layer	Information disclosure	[187]
	Elevation of privileges and data tampering	
	Threat of botnets	
	Code substitution or code extension attacks	[215]
	Injection flaws in SQL/noSQL Databases, OS and LDAP	[217]
	Session hijacking	[219]
	Security misconfiguration	[218]
	XSS	[217, 220]
	Plain-text recovery attacks	[221]
	Resource constraints	[222]
Business layer	Unauthorized sharing of data/information	[223]
	Threats to user privacy	

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

TABLE 11. IoT Defense-in-Depth Approach

Defense Category	Security Measures	References
Risk assessment	Identify critical assets	[238, 239]
	Vulnerability assessment	
	Risk treatment and mitigation strategy	
Protective measures	Security by design	[240, 241]
	Identity management	[242]
	Tamper-proofing	[243, 244]
	Use of pseudonymous identities	[245]
	Identity-based authenticated encryption and mutual authentication	[246, 247, 248]
	Homomorphic encryption	[249]
	Blockchain technology	[250, 251, 206]
	Role-based access control	[206]
	Secure remote access	[252]
	Key management	[218]
	Network segmentation	[253]
	SDN	[254]
	Self-encrypting devices	[243]
	Security training and awareness	
	Secure log management	
Detective measures	Network security analysis	[255, 256]
	Edge security analysis	[242]
	Network-level security measures	[257]
	Device attestation	[258]
	Penetration testing and vulnerability assessment	[218]
Responsive measures	Establishment of CERT	[218]
	Preparation of incident response plan	
	Self recovery of nodes	
Corrective measures	Remote attestation	[243]
	Device replacement/reconfiguration	
	Review and updating security policies	

tery/supercapacitor), and power management unit (interface) [268].

Transducers convert ambient energy into electrical DC power and commonly referred to an "energy harvester." In addition, the battery/supercapacitor collects cumulative DC power over a period of time, and the power management unit transfers maximum energy from the battery/supercapacitor to the IoT device.

Since energy supply and demand may come at different times, in practice, a temporary energy buffer (for example, supercapacitor) and power management unit are necessary to deliver harvested energy to the IoT device effectively. Therefore, the power interface (power management unit) makes the produced energy feasible to the load using various adjustments such as voltage regulation (DC/DC convertor) and power management functions [269]. Supercapacitors have been investigated as an alternative green energy storage due to their advantages compared to batteries [270]. They have quicker charge time (∼1000 times over batteries), larger operating temperature range (-40∼+85°C), ability to withstand millions of charge/discharge cycles, nearly infinite shelf life and lack of toxic heavy metals [271]. Although nearly perfect for IoT applications, a supercapacitor has its own disadvantages such as lower energy density (10 times smaller than batteries) and unstable output voltage over long time-span. To address the quick charging and long-lasting requirements of IoT systems, and to overcome the inherent disadvantages of supercapacitors, an overall power management solution is proposed using supercapacitor management integrated circuits (ICs) [272, 273].

Recently, supercapacitors with very low equivalent series resistance (ESR) much less than 0.1 ohm have been presented which are capable to work efficiently over a wide temperature range of -40° to 85°C [274]. Further, they can be discharged at high current level up to 10 A which make them a suitable candidate for IoT applications and large-scale WSNs in precision agriculture (for example, plant and soil sensors) [275].

In addition, supercapacitor has an excellent reliability in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

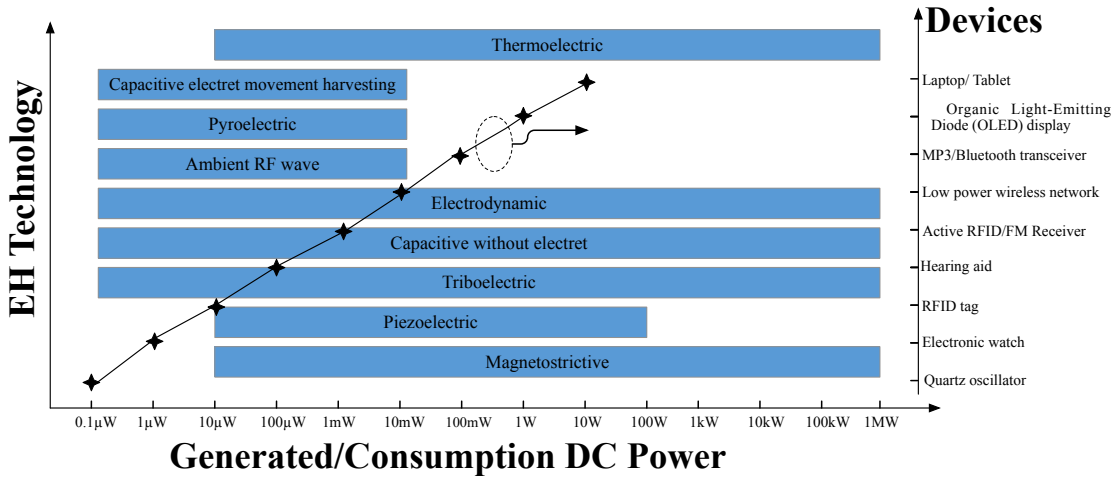

FIGURE 19. Generated power using various energy harvesting technologies and typical power consumption of devices.

FIGURE 20. General block diagram of an energy harvesting system.

comparison with battery in the market. High durability guarantees less degradation and a longer working time under high temperature condition [274]. Table 12 exhibits key benefits of supercapacitor relative to battery. The application of supercapacitors in micro-satellites has been also investigated [276] as supercapacitor cells are capable of surviving in harsh environments (for example, space applications).

Finally, supercapacitors are ideal storage candidate when a quick charge is required to address a short-term power need; whereas batteries are chosen to provide long-term energy storage. Therefore, combining supercapacitors with batteries in a hybrid mode provide an optimum solution which satisfies both requirements. This reduces battery stress, resulting in a longer service life [277].

EH systems for IoT devices should fulfill certain requirements, such as power range, cost, and dimension. A low profile, compact, maintenance-free, low-cost, and highly efficient EH is suitable for IoT devices. Recent advancements in integrated circuit architecture have created the potential to integrate multiple features into one chip (for example, monolithic microwave integrated circuit technologies). Hence, IoT size is not a bottleneck anymore. Moreover, employing RF technologies has allowed for size and cost reductions in integrated IoT devices with EH [278]. Sustainable IoT devices driven by EH have been attracting significant interest from different sectors such as smart cities, health care, and precision agriculture [259]. Table 13 presents an overview

TABLE 12. Comparison table of supercapacitor vs battery.

Parameter	Battery	Supercapacitor
Energy Density (Wh/Kg)	100	10
Power Density (KW/Kg)	1	10
Efficiency (%)	<80	>90
Cyclability	400–2500	1000000
Calendar Life (Years)	4–6	>15
Low Temperature (°C)	-20	-40
High Temperature (°C)	+60	+85 to +100
Death	Sudden	Predictable
Cost ($/KWh/Cycle)	0.07–0.2	0.006

of different sensor types and their maximum power demand. Moreover, in each sensor type, a typical sensor and its power consumption are presented. Table 14 and 15 present some examples of industrial IoT devices powered by integrated EH systems.

1) RF Energy Harvesting

RF energy scavenging has experienced rapid development recently due to the increasing number of RF transmitter sources, which are producing an abundant ambient electromagnetic energy [267]. A prominent advantage of RF harvesting is the capability to transform dissipated microwave energy into usable electrical power during day and night, both indoor and outdoor. Further, penetrations of RF signals inside structures (for example, walls, bridges, tunnels) and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

TABLE 13. Overview of Different Sensor Types and their Power Demand.

Sensor Type	Max Power Consumption	Typical Sensor Model	Company	Typical Sensor Power Consumption
Pressure	20 mW	BMP280	Bosch	100 μW
Acceleration	35 mW	ADXL345	Analog Devices	100 μW
		MPU-6050	InvenSense	1650 μW
		LIS2DS12TR	STMicroelectronics	270 μW
Temperature	3.5 mW	TMP006	Texas Instruments	792 μW
		D6T-44L-06	Omron	25 μW
Humidity	3 mW	HDC1000	Texas Instruments	2.46 μW
Gas	800 mW	Grove - Gas Sensor (MQ2)	Seeed Studio	800 mW
Displacement	1 mW	SP1-50	TE Connectivity	0.5 mW

underground allow for RF energy harvesting and wireless power charging where other energy sources (for example, solar, wind) are not available [268, 278, 301]. RF energy harvesting offers a novel approach to develop environmentally sustainable IoT devices by employing ambient energy and converting electromagnetic resources to electricity. To this end, receiving antennas is integrated with rectifying circuits (rectifying antenna or rectenna) to harvest RF energy from a focused beam (Wireless Power Transfer/ WPT) and other freely available sources in the environment (Ambient RF Energy Scavenging).

RF energy harvesting system eliminates the need for returning IoT devices to base for recharging. These devices could be powered through ambient energy sources or wireless power transmission. This is of paramount importance for autonomous systems in remote or harsh areas where accessibility is a problem [262]. From a practical perspective, efficiency, sensitivity, and compactness are key factors of EH, as RF energy harvesting in free space suffers from a large propagation loss [302]. Enabling simultaneous multi-band and multi-tone signals in the input of an EH system and taking advantage of the RF combining method, the rectifier sensitivity and generated output power can be enhanced [261, 262, 303]. Further, RF technology allows for size reduction using metamaterials in applications where miniaturization is required [303, 304, 305].

2) Spaceborne Energy Harvesting

Another method of generating an alternative energy source for ground-based IoT devices is using Sun-synchronous satellites. Sun-synchronous orbit (SSO) is a particular kind of polar orbit. Satellites in SSO, traveling over the Polar Regions, are synchronous with the Sun. This means they are synchronized to always be in the same "fixed" position relative to the Sun. Hence, the satellite will always observe a point on the Earth at the same time of the day, which creates a number of applications [306]. One of the key applications of this system is providing DC power for ground-based IoT devices, as depicted in Figure 21.

Space satellites collect sunlight using solar cells which transform the absorbed energy into DC power (Figure 21). Subsequently, the high voltage DC power is supplied to RF generators, i.e., magnetron generates RF power which can be transferred to a ground station or IoT devices, directly [307]. The receiving ground-based antenna integrated with rectifier (RF to DC convertor) regenerates DC power from RF power. In this method, energy is directed from space to the Earth to support large-scale WSNs with sufficient power sources.

B. SIMULTANEOUS WIRELESS INFORMATION AND RF POWER TRANSFER

High data rate, small dimension, and low-cost are important metrics in the next generation IoT devices and communication technologies. Hence, the use of simultaneous wireless information and power transfer (SWIPT) is investigated to improve energy efficiency as well as information transfer of the network [308, 309].

It has been proven that RF power transfer allows wireless nodes to recharge their batteries from receiving RF signals, leading to the fifth-generation green communication technologies [259, 310].

Moreover, conventional forms of SWIPT systems such as time splitting, power splitting, antenna switching, and partial switching are suitable for IoT networks [308].

In [311], a new concept and design of a three-dimensional antenna array is addressed. The purpose of this paper is to enhance efficiency of SWIPT systems when integrated into WSN architectures. Using 3D antenna, an omnidirectional radiation pattern can be achieved with considerable gain and low power losses [312]. Consequently, 3D arrays prove to be a reliable solution to feed low power WSNs that are placed over the 360 azimuth angles in a smart grid farm. Moreover, several pioneers working on SWIPT have attempted to focus the energy of the electromagnetic wave

TABLE 14. Overview of Embedded Energy Harvester Used in IoT Applications.

Ref.	Product	Company	Energy Source	EH Technology	Country
[279]	Thermostat	Kieback&Peter	Thermal	TEG	Germany
[280]	Wireless Magnet Contact	EnOcean	Light/Solar	Photovoltaic	Germany/USA
[281]	Wireless Light Switch	EnOcean	Kinetic Energy (pressure)	Electrodynamic/ Piezoelectric	Germany/USA
[282]	Key Card Switch	EnOcean	Kinetic Energy (pressure)	Electrodynamic/ Piezoelectric	Germany/USA
[283]	Occupancy Sensor	EnOcean	Indoor Light	Photovoltaic	Germany/USA
[284]	Room Thermmostat	Peha-Honeywell	Indoor Light	Photovoltaic	Germany/USA
[285]	Remote Control	Arveni	Kinetic Energy (pressure)	Piezoelectricity	France
[286]	Smart Charging at Home	Energous Corp.	RF Energy	RF to DC	USA
[287]	Fleet Tracking	Perpetuum	Kinetic Energy (Vibration)	Piezoelectricity	England
[288]	Roads/Sidewalks	Pavegen	Kinetic Energy (Vibration)	Piezoelectricity/ Induction	USA
[289]	Street Lights	EnGoPlanet	Kinetic Energy (Pressure)	Solar: Day, Piezo: Night	USA
[290]	Outdoor Temperature Sensor	Thermokon	Light/Solar	Photovoltaic	Germany
[291]	Pipeline/Industry Monitoring	Perpetua	Thermal Energy	TEG	USA
[292]	Sewer Level Monitoring System	NTT Data	Thermal Energy	TEG	Japan
[293]	Smart Watch	Matrix Ind.	Thermal Energy	TEG	USA
[294]	Solar Lamp	Ningbo Yongjiang Shenzhou Photovoltaic Co., Ltd.	Solar	Photovoltaic	China

as much as possible in order to increase the efficiency of power and data transfer [313, 314]. Nevertheless, the most interesting aspect regarding the architecture of SWIPT is how to concentrate electromagnetic power based on the location of the sensor. Simple beam scanning approach is suggested to identify the location of wireless sensors and concentrating microwave power using beam-steering method according to a preset look-up table [315]. Recently, a novel analog real-time spectrum analyzer (RTSA) was suggested and experimentally tested on the basis of the spectral-spatial decomposition property of the composite right and left handed (CRLH) leaky wave antenna (LWA) [316, 317, 318] which can be used as a beam-steering configuration to feed sensors in a smart grid field (for example, large-scale farms). According to Figure 22, a leaky wave antenna array is used to feed a variety of agriculture sensors in each beam direction.

X. IOT INTEROPERABILITY

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

TABLE 15. Overview of External Mounted Energy Harvester Used in IoT Applications.

Ref.	Product	Company	Energy Source	EH Technology	Country
[295]	Solar Harvester	KCF Technologies	Light/Solar Energy	Photovoltaic	USA
[296]	Libelium Waspmote Plug and Sense	Libelium	Solar	Photovoltaic	Spain
[297]	Vibration Energy Harvester	Perpetuum	Vibration	Piezoelectric	England
[298]	Powerharvester	Powercast	RF	RF to DC	USA
[299]	Ultra low power energy harvester and battery charger	STMicroelectronics	Thermal	TEG	USA
[300]	Marlow EHAL37L37-R01-L1	Marlow	Thermal	TEG	USA

A. INTEROPERABILITY BETWEEN STANDARDS

IoT networks are created with massive heterogeneous devices. The communication of these different devices is a key problem. To solve this problem, different standards are created to standardize the information exchanging process within IoT networks. The authors of [319] summarized all these standards and categorize them into communication, RFID, Data content and encoding, electronic product code, sensor, network management, middle, and quality of service. Apart from these protocols, there are also standards designed to fit the IoT use cases, such as, IoT6 [320]. With all these standards and protocols aiming for different scenarios, inter-communication between standards is an issue. This introduces interoperability problems of IoT. In Table 16, the authors of [186] classified interoperability problem into device interoperability, network interoperability, syntactical interoperability, semantic interoperability, and platform interoperability. The authors from [186] also aggregated different works and form seven approaches tackling the problem of interoperability. As the first approach, adapters and gateways are utilized as an intermediate bridge between different standards and specifications [186]. The intermediate device is compatible with multiple standards and specifications. Therefore, such a device can communicate with different IoT devices by converting messages between different protocols. However, this method assumes TCP/IP support on devices and does not account for the limitation of resources of IoT devices. Also, scalability is a problem as the message conversion process needs to be defined between all IoT protocols. The second approach is using a virtualized network overlay layer above physical networks. This approach supports end-to-end communication using different protocols. Unfortunately, scalability issues induced by different protocols persist.

The third approach in [186] consists of four different network technologies. The first technology is TCP/IP. Interoperability is implemented by embedding the TCP/IP stack on smart devices. Therefore, these devices can communicate with standard network protocols. The second technology is SDN. This programmable network technology provides intelligence, efficiency, security, and scalability to IoT networks. This can also be achieved with NFV, where virtual networks separate network functions with the physical equipment. Furthermore, physical equipment can be shared between different network functions. The final technology is fog computing. Fog computing relies on fog servers to preprocess raw data from the end devices and preparing these data to be interoperable for other applications [186].

The fourth approach is using open APIs [186]. A commonly used example is the REST API. Open APIs provide standard methods to access data or services. This provides cross-platform and cross-domain interoperability. A future direction is a generic API for uniform resource access.

A service-oriented architecture is implemented above the network layer as the fifth approach to achieve interoperability. The aim of this architecture is to package the IoT device resource as standard services. Therefore, device data can be standardized into services, providing syntactic interoperability [186]. The IoT6 standard is an example of this approach. IoT6 is an IPv6-based service-oriented architecture that provides interoperability between heterogeneous system components [320].

The last two approaches to achieving IoT interoperability are semantic web technologies and open standards. Both of these approaches require a recognized organization to provide common definitions [186]. Semantic web technologies define a common understanding of the various entities. Once a common vocabulary of standard, data and format is agreed, semantic interoperability can be achieved. The final approach is the establishment of open standards. These standards are provided by recognized organizations to achieve interoperability with IoT networks implementing these standards. An example is the AllSeen Alliance, defining the AllJoyn for device interoperability and the oneM2M for platform interoperability [186]. The ISO also developed a framework (ISO/IEC NP 21823) for IoT interoperability [321]. They established standards on semantic interoperability and network connectivity.

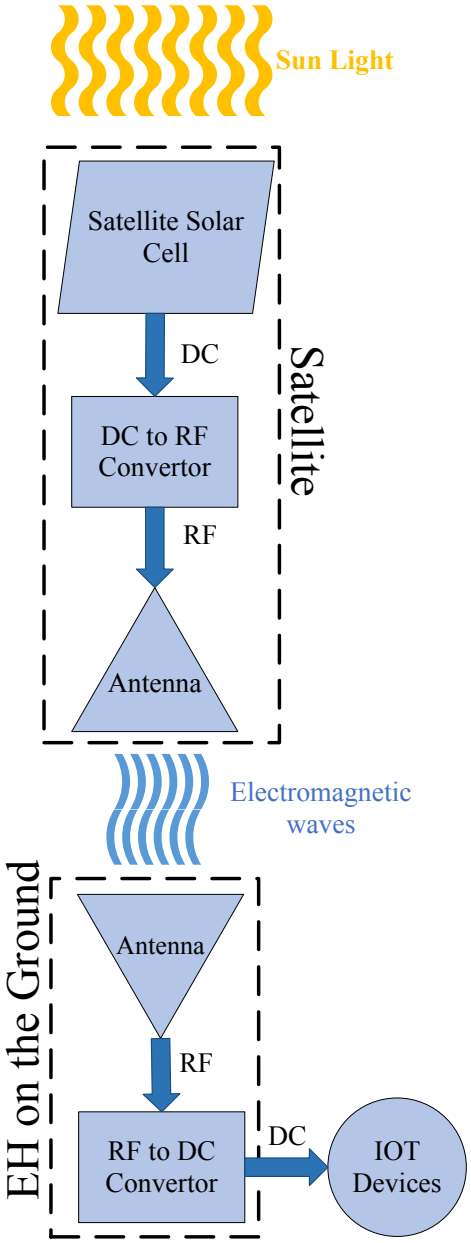

FIGURE 21. Block diagram of an energy harvesting system.

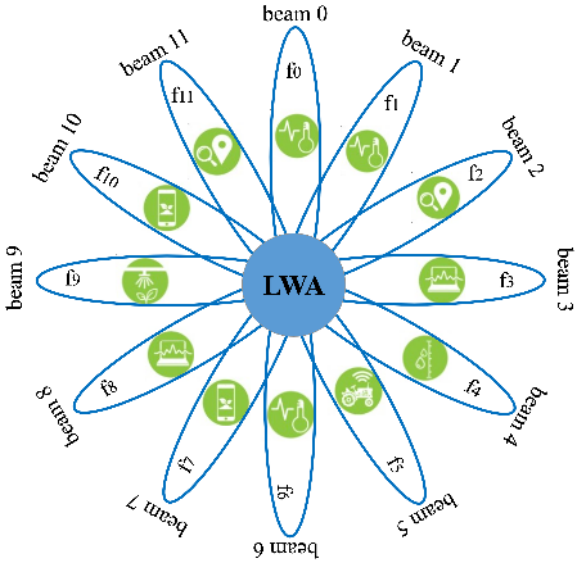

FIGURE 22. Beam-steering configuration for feeding sensors (SWIPT application) in a smart grid field.

TABLE 16. Types of IoT interoperability. [186]

Type of Interoperability	Definition
Device Interoperability	The exchange of information between heterogeneous devices and heterogenous communication protocols;The ability to integrate new devices into different IoT platforms.
Network Interoperability	Interact between different system accounting routing, resource optimization, security, quality of service and mobility.
Syntactical Interoperability	Interoperation of data structure in exchanged information.
Semantic Interoperability	Descriptions or understandings of resource, operational procedures, data models and information models between different entities.
Platform Interoperability	Interoperability required for barriers created by different IoT stacks consist of different operating systems, programming languages, data structures, architectures and access mechanisms for things and data.

XI. USER FRIENDLY IOT

This section provides insights into the usability of IoT 2.0. The purpose is to create a vision of future IoT that aims to lower the entry barrier of IoT services for non-expert users. This vision starts with exploring the previous technologies of lowering entry barriers for non-expert users. These technologies are cloud computing-based services, which are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The usability of these technologies is created by increasing accessibility, increasing scalability and flexibility, the use of virtualization, reducing cost on maintenance, and standardization [322, 323]. Accessibility is created by the feature of the cloud, where users can easily access the services through the Internet. Scalability and flexibility are induced by the virtualization of hardware and software resources [323]. Therefore, users do not need to directly configure these resources, as a standardized interface can reduce the complexity of resource configuration

[322]. Finally, as maintenance is mostly done by the service providers, the cost of maintenance is reduced on the user side [322].

The authors of [324] offered the five features to ensure the usability of IoT systems. These features are Plug & Play, interoperability, the ability for remote control and monitor, cost effectiveness, and open source, open architecture. Also, by deduction from the cloud computing services, a standardized interface can increase the usability of systems and fulfill the features of remote control and interoperability. However, due to the heterogeneity of IoT devices, a solution is to adopt modularization. The authors from [325] proposed Internet of Things as a service (iTaaS). iTaaS utilizes service oriented architecture, which is built with modular and reusable service modules. Thus, this architecture reduces the time of service development, service deployment, and service configuration.

iTaaS only reduces complexity and interoperability issues for software deployment. Different from cloud computing services, IoT devices are heterogeneous and deployed in complex environments. Therefore, the customization of IoT devices is important to support different use cases [326]. The authors from [326] also emphasized that the modularization of IoT devices can reduce cost and complexity for non-technical personnel. Therefore, modularization increases the cost effectiveness and usability of IoT systems.

To reduce the cost of maintenance, IoT devices must operate in a self-organized, secure manner and avoid extra human intervention. The authors of [327] mentioned that self-organized IoT networks should contain the following features: cooperative communication model to support communication across different layers with suitable resource control, situational awareness to monitor neighbor devices and faults, and automated load-balancing to extend the overall lifetime of the whole system. A possible solution is the SONs mentioned in the sections above. SONs provide machine learning-driven self-configuration, self-optimization, and self-healing functionalities [111].

Finally, as a vision towards the future, industry level standardization and efficient device deployment method is required for IoT systems. The authors from [328] pointed out that standardization drives standard testing and manufacturing procedures. Thus, this provides end users with more trust and confidence in IoT products. Another problem with current IoT systems is device deployment. Most work on IoT deployment focuses on software deployment and topology [324]. However, most devices are still deployed by humans. Novel device deployment methods should be invented to automate this process.

XII. IOT APPLICATIONS

This section starts with presenting some existing applications of IoT systems. These applications are categorized into smart home applications, smart city applications, healthcare applications, and smart farm applications. Then, a vision of possible applications of Industry 4.0 and Tactile Internet is revealed.

A. SMART HOME APPLICATIONS

Smart home applications leverage IoT devices and sensors to provide people convenience. The majority of smart home applications are home automation systems, which use the result of analyzing sensor data to automate a certain activity [329]. In [329] Healthcare system for elders and people with disabilities is a type of home automation system. These systems collect data from CCTV, motion sensors, and body sensor networks to perform analytics and push medical reminders. Another application is the pet care system. Temperature sensors are attached to a pet dog to monitor its body temperature. When the temperature sensor detects any anomaly, the air conditioner is automatically switched on to comfort the pet.

The authors of [330] explored the smart grid as another major field of smart home applications. This field of applications leverages smart meters, smart appliances, and smart power outlets. The aim of smart grid applications is to monitor and control power production and consumption to achieve a balance between production and consumption. Furthermore, it reduces the waste of power induced by overproduction. Applications under the smart grid field are real-time generation monitoring, power plants controlling, alternative energy source controlling, and residential production controlling [330].

B. SMART CITY APPLICATIONS

Smart city applications solve problems and issues in the public sector. The authors of [331] and [332] both summarized smart city applications in their works (Table 17). In their work, smart home applications are viewed as a part of the smart city applications. Other applications include smart parking, augments maps, logistics, smart water supply, smart cars, smart grid, weather monitor, pollution monitor, surveillance systems, traffic monitor, and healthcare.

C. HEALTHCARE APPLICATIONS

=Compared to traditional and manual health monitoring systems, IoT healthcare systems have a few advantages [333]. First, IoT devices are relatively portable. These devices can be worn by the patients to provide constant monitoring [333]. Also, with IoT devices, voluminous data can be accessed remotely in a quicker pack compared to the traditional methods [333]. These advantages attracted the development of different IoT healthcare applications. The authors of [334] classified IoT healthcare applications into home healthcare, mobile health and electronic health, and hospital management. Home healthcare IoT applications move the setting from a hospital to the homes of people. It is achieved through remote monitoring through IoT devices [334]. Similarly, mobile health and electronic health also rely on remote monitoring of patients. However, it focuses more on wearable sensors [334]. The above two types of applications involve single condition applications such as diabetes glucose level sensing designed for specific diseases; and cluster condition applications such as rehabilitation systems that can help treat

TABLE 17. IoT Smart City Applications. [331, 332]

Application	Description
Smart Home	Using sensors to monitor the environment and control environmental parameters using heaters, air conditioners, fans, etc.
Smart parking	Using sensors to monitor arrival and departure of cars providing information of available spaces.
Augments maps	Near field communication tags provides tourists information by connecting phones to web services.
Logistics	Leverage Radio Frequency Integrated Circuit (RFIC) to monitoring and track every step of the inventory.
Smart water supply	Pipe leakage detection and water quality monitoring.
Smart cars	Driverless cars
Smart grid	Prediction and scheduling of power supplying and production. Also self-healing functionality induced by defect detection.
Weather monitor	Monitoring temperature, rain, wind speed, and pressure.
Pollution monitor	Environmental monitoring and report for human health.
Surveillance systems	Video camera systems for security and crime detection.
Traffic monitor	Congestion monitoring. Providing analytics for arrival time Prediction.
Healthcare	Remote health monitoring.

different diseases together [335]. As the final type of IoT healthcare applications, hospital management applications are responsible for the management and improvement of various hospital services [334]. For example, safety and violence detection systems using cameras and biometric sensors could track staff, patients, and visitors, and detect signs of aggression or stress [336]. Equipment tracking and maintenance systems can manage scarce shared equipment, and remind staff for requirements of equipment refill or calibration [336].

D. SMART FARM APPLICATIONS

The two major types of smart farm applications are crop monitoring and animal monitoring. The authors of [337] reviewed several different crop monitoring systems. These monitoring systems usually trigger actuator actions. In [337], one example is the irrigation system. Humidity, temperature, and weather data are collected to make the decision of irrigation. Another example is weed detection. In the application of weed detection, images are passed through a CNN model to detect weed. If weed is detected, a smart herbicide sprayer robot is activated to spray herbicide.

Animal monitoring applications aim to use sensors data to monitor and predict animal behavior. The authors from [337] described a smart beehive application. The smart beehive monitors oxygen, carbon dioxide, pollutant levels, temperature, and humidity to determine the health status of the bee colony. The authors of [338] reviewed machine learning-based animal monitoring applications. This work focuses on animal welfare. The first application of this work detects dietary changes and mating periods of cattle using ensemble learning based on data from magnetometers and three-axis accelerometers. The second application identifies and classifies chewing patterns in calves with DT leveraging optical sensor data. The authors from [339] created a full system of smart animal farm. This smart animal farm consists of four major applications. The first application detects biogases with a gas sensor. When the gas reaches a certain level, it emits the gas to prevent harm to the animals. The second application is auto-feeding. This application uses ultrasonic sensors to detect the level of food in storage and automatically add food using a valve. The third application is water level detection. Similar to auto-feeding, a water level sensor is used to open the water pump if the water is below a certain level. Finally, the incubator control system reads data from the humidity sensor and temperature sensor to control environmental parameters using a heater and a fan [339].

E. INDUSTRY 4.0 APPLICATIONS

Industry 4.0 applications focus on CPSs in production and manufacture. The authors of [340] determined three important characteristics of industrial applications. The first characteristic is cycle time determined by the round-trip time between the control center and end device. The second characteristic is the number of nodes determined by the size of the system. The final characteristic is reliability determined by the quality of information transmission. The authors of [340] also separated Industry 4.0 applications into process automation and factory automation. Process automation is characterized by an industrial process operated by sensors for data collection, controllers for controlling, and actuators for actuating the controller decision. The cycle time of process automation should be 100 ms with medium quality of information transmission. A more critical scenario is factory automation, which is the automation of the manufacturing process [340]. Therefore, it requires frequent collaboration between multiple robotics and assembly line machinery. Hence, a short latency of 1 ms with high reliability is required [340].

F. TACTILE INTERNET APPLICATIONS

The feature of low latency and ultra-high reliability of Tactile Internet attract applications like self-driving vehicles and industrial automation. For example, V2X communication requires real-time communication with latency less than 10 ms, and CPSs with mobile robot collaboration requires high reliability and real-time communication in manufacturing

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3078549, IEEE Access

applications [341]. However, the core of Tactile Internet application should be based on haptic communications.

The authors from [342] defined haptic architecture into the master domain, the network domain, and the slave domain. The master domain is usually a haptic device controlled by a human. The haptic device can control the slave domain through the network domain. Then, the slave domain returns environmental data and responds through the network domain back to the haptic device. Finally, the haptic device receives the data and simulate a virtual environment of the slave domain for the human to touch and feel.

The authors of [341] explored four domains of haptic communication applications. The first domain is Tele-medicine. Robust and reliable networks allow physicians to perform telesurgery and tele-diagnostic using a remote slave robot. The second domain is AR and VR. Haptic communications could provide extra reality with the sense of touch. The third domain is serious gaming. This requires real-world simulations to solve a certain problem. Haptic communications could induce real-world experiences for problem solving within serious gaming. Finally, unmanned autonomous and remotely controlled systems provide safety for operations in dangerous and difficult-to-reach environments. These operations usually involve high precision. Utilizing Haptic communications could perform these operations remotely without any delays.

XIII. RESEARCH CHALLENGES OF IOT 2.0

This section summarizes the possible future development of IoT 2.0. Some of these development are IoT global connectivity, IoT security architecture, ubiquitous IoT devices, energy harvesting-based energy efficiency, IoT reliability, and considerations in usability.

A. IOT GLOBAL CONNECTIVITY

As current IoT architectures evolved with edge computing layers, future IoT architectures focus with IoT global connectivity. We believe that the development of 6G networks provides a platform for IoT global connectivity. In [343], the 6G networks evolve in the space, time, and frequency dimensions. In the space dimension, more transceivers will be deployed to increase multipath communication [343]. In the time dimension, there will be more fine-grained time slot units to satisfy latency-sensitive applications [343]. Finally, in the frequency dimension, 6G will operate in a higher frequency spectrum to fulfill higher data rate requirements [343]. Also, the increase of frequency range is a basis of integrating the satellite system into mobile networks to create a space-air-ground integrated architecture [343]. As completion of a network providing full coverage, the authors of [344] extended the space-air-ground architecture with the vision of underwater networks and specified four tiers within the space-air-ground-underwater networks (Table 18). On the commercial side, ground to satellite communications widening the system coverage have already emerged. IoT devices can communicate with Low Earth orbit (LEO) satellites through VHF and UHF transmissions [345]. However, there are latencies up to three hours due to coverage gaps between LEO movements [345, 346]. Compared to LEO satellites, IoT data transmissions to Geosynchronous Earth orbit (GEO) satellites have a lower latency around two minutes [346]. These satellite systems initiate the exploration of the future space tier IoT network. Previous network coverage, network types, wireless spectrums, communication mediums, interactive functions, core services, and layers will be integrated to support the 6G architecture [347]. The 6G networks will be providing services to new mobile terminals such as smart cars and robots with disruptive communication technologies and distributed, intelligent base stations [348].

TABLE 18. Space-air-ground-underwater networks tiers [344]

Tier	Base Station/Devices	Communication Method
Space	Low-Earth orbit, medium-Earth-orbit, and geostationary satellites	mm-wave and laser communication between satellites.
Air	Flying base stations (UAV), floating base stations	Low frequency, microwave, and mm-wave bands.
Terrestrial	Ultra-dense network with small base stations	Low frequency, microwave, mm-wave, and THz bands.
Underwater	Underwater military and commercial devices	Acoustic and laser communications.

Table 19 outlines the network performance requirements as a foundation of the 6G vision and future applications. Despite the performance requirements, there are also various service requirements. These services requirements are high security, secrecy and privacy, high affordability and customization, and finally, high intelligence [349].

To fulfill the 6G requirements, the relevant technologies will evolve with three different directions: communication technology, network architecture, and network intelligence integration [350]. The authors of [348] promoted two candidates for 6G communication technology improvement. The first is photonic-defined radio. As a vision, 6G could leverage photonic technology to create a multipurpose network, converging different previous network types with full-spectral support [348]. The second candidate is laser mm wave. This technology supports 100 Gb/s communication for communication between space and terrestrial networks [348]. The authors of [343] also provided two higher spectrum technologies as an extension to the current 5G paradigm. These technologies are terahertz communications and visible light communications. To support communication in higher

TABLE 19. 6G network performance requirements [344].

Network Property	Requirement
Wireless backhaul fronthaul data rate	1 - 10 Tb/s
User experienced data rate	1 - 10 Gb/s
Over-the-air latency	10 - 100 μs
Support high mobility	>1000 km/h
Connectivity density	$10^7 devices/km^2$
Area traffic capacity	1 $Gb/s/m^2$
Energy efficiency	10 - 100 times of 5G
Spectrum efficiency	5 - 10 times of 5G

frequency spectrum, full-duplex communication stack enabling simultaneous signal transmission and reception, and novel channel estimation technologies to improve bandwidth efficiency are required to handle the high usage demands of 6G networks [350].

With the novel communication technologies and limitations of 5G networks, new network architectures need to be established to support 6G communications and applications. In [348], there are four 6G network architectures, including the hyperspectral space-terrestrial integration network discussed above as part of the 6G vision. Subsequently, an all-photonic radio access network leveraging photonic engines with all-photonic arrayed antenna units to break through the bandwidth and latency limitations of 5G networks [348]. The third architecture, holographic radio, and photodiode-coupled antenna arrays exploiting interference to improve the spectrum efficiency and enhance the service quality [348]. Finally, the cognitive radio based on AI and photonics aims to further strengthen the current network performance with all-photonic arrayed antenna units, and AI is optimizing the network layers and services [348]. The evolution of AI in 6G will be discussed next.

As discussed in section IV above, AI and machine learning can be embedded in most layers of the communication network. In [351], applying AI in 6G networks is inevitable as the vast and complex network topology cannot simply be managed by humans. Also, AI simplifies the network model and portraits the unknown non-linearity [351]. Moreover, in [348], AI and machine learning can be combined with photonics-based cognitive radio to form a novel 6G network architecture. In this architecture, AI is used for network deployment tasks such as precise capacity forecasts, coverage auto-optimization, network resource scheduling, and network slicing [348]. To optimize the AI models for these tasks, cross-layer models providing intralayer and interlayer functions are more suitable than the current layered designs [344].

B. MACHINE LEARNING MODELS

This article reviewed machine learning implementations from the physical layer to the cloud layer. On the physical layer, the development of end-to-end machine learning models could reduce operation complexity. Thus, improving the physical layer efficiency [344]. The network layer applications provide services such as routing, traffic analytics and control, network management, network security, and network configuration. These services lead to the achievement of SONs. However, the generalization of these machine learning models is questionable, as most of these models are constructed using data generated from only one or a few networks. The generalization of network layer machine learning models on IoT networks could be a future direction. Furthermore, each implementation of machine learning in IoT presented in Section IV is only providing services within a single layer of the IoT network architecture. From [344], compared to current layered designs, cross-layer models are necessary to provide optimal performance. Therefore, cross-layer models should be investigated for future IoT networks.

C. IOT SECURITY ARCHITECTURE

Due to diverse IoT applications supporting heterogeneous IoT devices, there are numerous security challenges that require further investigation. Some of these significant issues are discussed here.

1) Vulnerability of Machine Learning and AI Technologies

Since machine learning and AI are dominant technologies in future networks [350], it is essential to provide extra security on the data. Therefore, federated learning should be promoted to preserve the privacy of multiple edge and end devices [351, 352]. On the other hand, if cross-layer machine learning models are the mainstream of future IoT networks, future IoT security architectures could also evolve towards cross-layer security and benefit from cross-layer machine learning models to ensure safer network services. However, machine learning and deep learning based IoT systems are susceptible to "Butterfly Effect." Where a minute change in the data being input to the learning system adversely affects the output (learned model). Hence, attackers can maliciously change the input data to make the system unstable [353]. Such attacks are difficult to protect against since the attackers do not need access to the system itself. Correspondingly, there is a need to devise a mechanism to ensure data integrity for different machine learning-based IoT applications.

2) Post-Quantum IoT Security

As we are near the beginning of the era of quantum computing, research into the application of post-quantum cryptography on IoT is necessary. In this regard, classical cryptography could be vulnerable to quantum computers [354]. Moreover, quantum computing threatens the asymmetric encryption algorithms, including RSA, ECDSA, elliptic Curve DH (ECDH), and Digital Signature Algorithm (DSA). Most of which can be solved swiftly with Shor's algorithm [355,

356] on a powerful quantum computer. Similarly, quantum computers can also speed up the brute force attacks on symmetric encryption ciphers by a quadratic factor using Grover's algorithm [357]. However, irrespective of the recent research efforts in post-quantum cryptography by PQCrypto and SAFECrypto projects, very little focus has been on addressing the challenges in implementing the post-quantum schemes on resource-constrained (especially low power) IoT devices [356].

3) Real-time Updates

The estimated increase in the use of IoT devices to a Billion devices in the near future, affirms the need for a secure software/firmware update mechanism. However, it seems challenging since not all the devices support OTA (Over The Air) updates. Consequently, IoT devices are to be manually updated, which is not feasible for real-time IoT applications [358]. Therefore, there is a requirement of developing an intelligent and secure protocol to enable IoT devices to periodically poll for software/firmware updates so that they are protected against the latest threats/attacks.

D. UBIQUITOUS IOT DEVICES

Ubiquitous IoT refers to the coverage of different IoT services in different scale of management [359]. This includes local IoT maintained by regional management platforms, industrial IoT managed by particular industries, national IoT controlled by national level management unit, and global application IoT coordinated by a global coordinator. With this massive number of devices interacting with each others on these different scales, energy consumption and management could be issues [359]. To address the issues of energy consumption and management, in a future vision, ubiquitous IoT devices should conduct autonomous operations with no human intervention or maintenance and able to adapt to different scales of operations [360]. To achieve such autonomy, AI and machine learning models could be a vehicle automating many management and communication operations [361]. This automation can also be achieved from the SON methods mentioned in Section IV. On the other hand, energy harvesting methods are also an important solution reducing energy consumption and management costs. Other than these two important aspects of IoT, the authors of [360] concluded some major directions of ubiquitous IoT devices. One direction is multiservice IoT, which extends the idea of single service on single nodes towards multiple services on single nodes. This aims to increase the value of single IoT nodes. Another important direction is the ability of devices to deal with extreme conditions. This includes the prediction of energy consumption (and harvesting). Also, low energy communication methods technologies will support the development of battery-less devices with the aid of energy harvesting methods [360]. Finally, as energy harvesting methods are also an important aspect of ubiquitous IoT, the limitations and future development of energy harvesting techniques are presented in the next subsection.

E. ENERGY HARVESTING-BASED ENERGY EFFICIENCY

Sensors and IoT devices have now become an integral part of the tool-set used to ensure effective monitoring and to maintain safety in societies. However, the dependency of these portable devices on batteries limits their operation time and range. Energy harvesting is a promising solution to provide a sustainable and cost-effective alternative energy source to extend the lifetime of IoT devices and reduce energy costs [362, 363]. As the number of IoT devices grows, deploying environmentally sustainable IoT devices integrated with EHs will lead to the long-term conservation of the environment and the global economy. Further, EH techniques can introduce more robust and trusted autonomous monitoring systems in the future [364].

The main challenge of implementing EHs in IoT networks is the low produced output power (for example, RF and piezo), which can be improved through well-designed structures and also applying hybrid techniques. Further, ambient sources may always not be available, hence, using Sun-synchronous satellites is a key solution to develop the next generation of sustainable IoT.

Moreover, WPT concept is extended to the simultaneous wireless information and power transfer (SWIPT), which allows data and RF power to be transmitted via the same electromagnetic (EM) wave. However, the low efficiency of a SWIPT system is the main drawback in SWIPT system and can be improved by using novel solutions, such as 3D printed antenna array and beam steering based on the LWA. In the former, the radiation pattern of the antenna array is optimized on behalf of the efficiency and in the later, the beam direction of the antenna is managed according to the sensor location.

In addition, many recent dispersion-engineered analog signal processing (ASP) systems have been introduced based on CRLH Transmission Line (CRLH TL) metamaterial-inspired structures [365]. Dispersion engineering involves manipulating the electromagnetic wave pathway to handle signals in an analog manner, contributing to applications such as real-time Fourier transformers, pulse shapers, and etc. Furthermore, several new dispersion-engineered CRLH TL metamaterial analog signal processing systems, exploiting the wideband dispersive features and design flexibility of CRLH TLs, have been presented [366].

This approach is particularly useful in applications where low-cost and low profile systems are needed or digital solutions are not available, as for instance in very high frequency and high speed ultra-wideband microwave systems, such as 6G technology [367]. These new methods will support large-scale WSNs and IoT devices in next generation smart grid field applications (for example, smart cities, and precision agriculture).

F. IOT RELIABILITY

The reliability in mission critical applications are discussed in Section V of this article. The integration of SDN and NFV in mission critical communication networks are also

discussed. Other than these aspects, IoT communication reliability can also be enhanced through advance error coding schemes, and network coding [368]. Advance error coding schemes such as polar codes can ensure communication reliability due to its ability of error correction [369]. This error correction functionality can operate with low computational complexity and decoding latency. Network coding gives intermediate nodes within a network processing ability to encode coming traffic [370]. With such ability, there are less packet re-transmissions and thus improving the reliability of IoT networks. Finally, IoT fault tolerance methods leveraging the concept of graceful degradation could also be enhanced for IoT reliability [368].

Achieving the desired requirements of mission critical communication in a dynamic environment is very challenging. In this regard, the knowledge available at the device level can also be utilized to reduce the computation burden at the base station, resulting in overall latency reduction [170]. The intelligence at the edge devices can enable them to adapt to the network dynamics without relying much upon the base station. Promising theoretical enablers for intelligence at the edge devices are presented in [371], which can be used to design mission critical communication systems.

G. TRADEOFF IN USABILITY

As future IoT networks promote full coverage and integration [348, 372], IoT scalability and interoperability between different devices and protocols should also be promoted to connect IoT as part of the network ecosystem. Using 6G networks as a platform, IoT system performance can be enhanced by 6G infrastructures, such as the coverage enhancement from satellites to provide better accessibility [372]. With the aid of machine learning and AI, managing these network connections and autonomous devices should not require much user attention and labor [351]. Therefore, this increases the usability of the system. On the other hand, the authors of [349] pointed out that the usage of AI reduces the magnitude of system customization. Thus, AI could decrease the usability for users with special requirements and preferences. In conclusion, the degree of system intelligence should be carefully designed in the future to satisfy general users and users with other system preferences.

XIV. CONCLUSION

The definition of IoT remains unchanged since the birth of the concept. As we are on the brink of the 5G era, the concept of IoT should follow this evolution towards IoT 2.0. This article summarizes the recent advancement of IoT technologies and defines it as IoT 2.0. First, a general architecture of IoT 2.0 is compared with previous architectures. From these architectures, edge computing is the driving force of architectural evolution. Current IoT technology is then discussed in seven dimensions as machine learning intelligence, mission critical communication, IoT scalability, IoT security, IoT sustainability, IoT interoperability, and user friendly IoT. The usage of machine learning algorithms is revealed in different layers of IoT applications. Then, mission critical communication systems are introduced, focusing on physical layer considerations and programmable mission critical communication networks. After that, hardware, network and service scalability is explored and lead to the discussion of SDN induced scalability. Security is an important aspect of IoT systems. In this article, security at different layers is analyzed. Followed by security, sustainability of IoT systems is also an essential component. Therefore, energy harvesting technologies providing longer lifetimes are evaluated. After that, due to the increase of device types and standards, interoperability and usability of IoT components are covered. The discussion of recent advancements ends with the outline of existing IoT applications. This whole discussion leads to the future directions of IoT, portrayed by the vision of future 6G networks.

REFERENCES

[1] Y. Zhang, "Technology framework of the internet of things and its application," in *Proc. 2011 International Conference on Electrical and Control Engineering*, Bandung, Indonesia, Sep. 2011, pp. 4109–4112.
[2] *Overview of the Internet of things*, ITU Std. Y.4000/Y.2060, 2012.
[3] V. Cisco, "Cisco visual networking index: Forecast and trends, 2017–2022," *White Paper*, vol. 1, 2018.
[4] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
[5] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *Journal of Industrial Information Integration*, vol. 6, pp. 1 – 10, Jun. 2017.
[6] G. Sun, V. Chang, S. Guan, M. Ramachandran, J. Li, and D. Liao, "Big data and internet of things–fusion for different services and its impacts," *Future Generation Computer Systems*, vol. 86, pp. 1368 – 1370, Sep. 2018.
[7] Techiexpert. (2017) What is coming in IoT 2.0? Techiexpert. [Accessed: September 16, 2020]. [Online]. Available: https://www.techiexpert.com/what-is-coming-in-iot-2-0/
[8] J. Goldfein. (2019) The Internet of Things 2.0 – the technology revolution. Mercury. [Accessed: September 16, 2020]. [Online]. Available: https://mercury.one/online-business/internet-things-2-0-technology-revolution/
[9] D. Litwin. (2020) Industrial IoT: How IoT has evolved and moved into the IoT 2.0 era. MarketScale. [Accessed: September 16, 2020]. [Online]. Available: https://marketscale.com/industries/industrial-iot/iot-2-0-era/
[10] J. Gomez. (2020) IoT 2.0: The intelligence of things. Koombea. [Accessed: September 16, 2020]. [Online]. Available: https://www.koombea.com/blog/iot-2-0-the-intelligence-of-things/
[11] J. Carter. (2017) A closer look at the Internet of Things 2.0 – and why it's inevitable. TechRadar. [Accessed: September 16, 2020]. [Online]. Available: https://www.techradar.com/news/a-closer-look-at-the-internet-of-things-20-and-why-its-inevitable
[12] Web Summit. (2018) IoT2.0. Youtube. [Accessed: September 16, 2020]. [Online]. Available: https://www.youtube.com/watch?v=00K0AWbMe_U
[13] M. Abbas. (2018) IoT 2.0: Revolutionize Internet of Things (IoT 2.0) Using Blockchain. IoTWorld. [Accessed: September 16, 2020]. [Online]. Available: https://iotworld.co/2018/01/iot-2-0-revolutionize-internet-of-things-using-blockchain/
[14] Samsung. (2019) IoT 2.0: The next phase of SmartThings engagement and growth. Youtube. [Accessed: September 16, 2020]. [Online]. Available: https://www.youtube.com/watch?v=8hGkB6AQA38
[15] S. Nativi, A. Kotsev, P. Scudo, K. Pogorzelska, I. Vakalis, A. Dalla Benetta, and A. Perego, "IoT 2.0 and the internet of transformation," 2020.
[16] J. Mongay Batalla, M. Gajewski, and K. Sienkiewicz, "Concept of IoT 2.0 platform," in *Ad-hoc Networks and Wireless*, M. Garcia Pineda, J. Lloret, S. Papavassiliou, S. Ruehrup, and C. B. Westphall, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 27–34.

[17] N. K. Narang, "Standards matters/mentor's musings on IoT 2.0: IoT coming of age," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 10–11, Jun. 2020.

[18] B. Montgomery, "Future shock: IoT benefits beyond traffic and lighting energy optimization." *IEEE Consumer Electronics Magazine*, vol. 4, no. 4, pp. 98–100, Oct. 2015.

[19] T. García Ferrari, A. Hinze, and J. Bowen, "An IoT for everyone: fact or fiction?" in *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32*, 2018, pp. 1–5.

[20] J. Park, Y. Son, D. Park, J. Cho, M. Bae, M. Han, H. Lee, J. Choi, H. Kim, and S. Hwang, "IoT based distributed intelligence technology for hyper-connected space," *Electronics and Telecommunications Trends*, vol. 33, no. 1, pp. 11–19, 2018.

[21] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in internet of things: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1–27, Feb. 2018.

[22] S. Li, L. D. Xu, and S. Zhao, "5G internet of things: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1 – 9, Jun. 2018.

[23] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN–key technology enablers for 5G networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2468–2478, Nov. 2017.

[24] H. Ramazanali, A. Mesodiakaki, A. Vinel, and C. Verikoukis, "Survey of user association in 5G HetNets," in *Proc. 2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, Medellin, Colombia, Nov. 2016, pp. 1–6.

[25] A. Morgado, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, "A survey of 5G technologies: regulatory, standardization and industrial perspectives," *Digital Communications and Networks*, vol. 4, no. 2, pp. 87 – 97, Apr. 2018.

[26] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, "The tactile internet: vision, recent progress, and open challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 138–145, May 2016.

[27] G. P. Fettweis, "5G and the future of IoT," in *Proc. ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, Lausanne, Switzerland, Sep. 2016, pp. 21–24.

[28] S. M. A. Oteafy and H. S. Hassanein, "Leveraging tactile internet cognizance and operation via iot and edge technologies," *Proceedings of the IEEE*, vol. 107, no. 2, pp. 364–375, Feb. 2019.

[29] G. P. Fettweis, "The tactile internet: Applications and challenges," *IEEE Vehicular Technology Magazine*, vol. 9, no. 1, pp. 64–70, Mar. 2014.

[30] M. Alrowaily and Z. Lu, "Secure edge computing in IoT systems: Review and case studies," in *Proc. 2018 IEEE/ACM Symposium on Edge Computing (SEC)*, Bellevue, WA, Oct. 2018, pp. 440–444.

[31] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *Proc. 2017 Global Internet of Things Summit (GIoTS)*, Geneva,Switzerland, Jun. 2017, pp. 1–6.

[32] F. S. Abkenar and A. Jamalipour, "Eba: Energy balancing algorithm for fog-iot networks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6843–6849, Aug. 2019.

[33] F. Shirin Abkenar and A. Jamalipour, "Energy optimization in association-free fog-iot networks," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 2, pp. 404–412, Jun. 2020.

[34] F. S. Abkenar and A. Jamalipour, "A reliable data loss aware algorithm for fog-iot networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5718–5722, May 2020.

[35] D. Lukač, "The fourth ICT-based industrial revolution "Industry 4.0" - hmi and the case of cae/cad innovation with eplan p8," in *Proc. 2015 23rd Telecommunications Forum Telfor (TELFOR)*, Belgrade, Serbia, Nov. 2015, pp. 835–838.

[36] S. Trinks and C. Felden, "Edge computing architecture to support real time analytic applications : A state-of-the-art within the application area of smart factory and industry 4.0," in *Proc. 2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, Dec. 2018, pp. 2930–2939.

[37] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the internet of things (IoT)," in *Proc. 2017 Eleventh International Conference on Sensing Technology (ICST)*, Sydney, NSW, Dec. 2017, pp. 1–5.

[38] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: a survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161 – 175, Aug. 2018.

[39] M. Z. Alom, T. M. Taha, C. Yakopcic, S. Westberg, P. Sidike, M. S. Nasrin, B. C. Van Esesn, A. A. S. Awwal, and V. K. Asari, "The history began from alexnet: A comprehensive survey on deep learning approaches," *arXiv:1803.01164 [cs]*, Sep. 2018.

[40] T. Hastie, R. Tibshirani, and J. Friedman, "Introduction," in *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. New York, NY: Springer New York, 2009, ch. 1, pp. 1–8.

[41] R. S. Sutton and A. G. Barto, "Finite markov decision processes," in *Reinforcement learning: An introduction*. MIT press, 2018, ch. 3, pp. 47–72.

[42] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, pp. 251 – 279, Jan. 2019.

[43] H. Rahimi, A. Zibaeenejad, and A. A. Safavi, "A novel IoT architecture based on 5G-IoT and next generation technologies," in *Proc. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, Canada, Nov. 2018, pp. 81–88.

[44] G. Peralta, M. Iglesias-Urkia, M. Barcelo, R. Gomez, A. Moran, and J. Bilbao, "Fog computing based efficient iot scheme for the Industry 4.0," in *Proc. 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM)*, San Sebastian, Spain, May 2017, pp. 1–6.

[45] L. Carnevale, A. Celesti, A. Galletta, S. Dustdar, and M. Villari, "From the cloud to edge and iot: a smart orchestration architecture for enabling osmotic computing," in *Proc. 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Cracow, Poland, May 2018, pp. 419–424.

[46] 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, Jan. 2018.

[47] R. Shahzadi, A. Niaz, M. Ali, M. Naeem, J. J. P. C. Rodrigues, F. Qamar, and S. M. Anwar, "Three tier fog networks: Enabling IoT/5G for latency sensitive applications," *China Communications*, vol. 16, no. 3, pp. 1–11, Mar. 2019.

[48] N. Kalatzis, M. Avgeris, D. Dechouniotis, K. Papadakis-Vlachopapadopoulos, I. Roussaki, and S. Papavassiliou, "Edge computing in IoT ecosystems for UAV-enabled early fire detection," in *Proc. 2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, Sicily, Italy, Jun. 2018, pp. 106–114.

[49] B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas, and Q. Zhang, "Edge computing in IoT-based manufacturing," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 103–109, Sep. 2018.

[50] H. Guo, J. Ren, D. Zhang, Y. Zhang, and J. Hu, "A scalable and manageable IoT architecture based on transparent computing," *Journal of Parallel and Distributed Computing*, vol. 118, pp. 5 – 13, Aug. 2018.

[51] A. Giri, S. Dutta, S. Neogy, K. Dahal, and Z. Pervez, "Internet of things (IoT): A survey on architecture, enabling technologies, applications and challenges," in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, Liverpool, United Kingdom, 2017, pp. 7:1–7:12.

[52] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.

[53] U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu, and M. Stanley, "A brief survey of machine learning methods and their sensor and IoT applications," in *Proc. 2017 8th International Conference on Information, Intelligence, Systems Applications (IISA)*, Larnaca, Cyprus, Aug. 2017, pp. 1–8.

[54] M. Mahmud, M. S. Kaiser, A. Hussain, and S. Vassanelli, "Applications of deep learning and reinforcement learning to biological data," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 6, pp. 2063–2079, Jun. 2018.

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

[56] A. S. Ali, "Support vector machine: Itself an intelligent systems," in *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications*, M. R. Syed and S. N. Syed, Eds. IGI Global, 2009, pp. 501–522.

[57] X. Su, X. Yan, and C.-L. Tsai, "Linear regression," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 4, no. 3, pp. 275–294, Feb. 2012. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/wics.1198

[58] T. P. Ryan, "Logistic regression," in *Modern Regression Methods*, 2nd ed. John Wiley & Sons, 2009, ch. 9, pp. 312–384.

[59] S. R. Safavian and D. Landgrebe, "A survey of decision tree classifier methodology," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 21, no. 3, pp. 660–674, May 1991.

[60] A. Navada, A. N. Ansari, S. Patil, and B. A. Sonkamble, "Overview of use of decision tree algorithms in machine learning," in *Proc. 2011 IEEE Control and System Graduate Research Colloquium*, Jun. 2011, pp. 37–42.

[61] O. Sagi and L. Rokach, "Ensemble learning: A survey," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 8, no. 4, p. e1249, Feb. 2018. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/widm.1249

[62] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, Oct. 2001.

[63] P. Cichosz, "Naïve bayes classifier," in *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications*, M. R. Syed and S. N. Syed, Eds. John Wiley & Sons Incorporated, 2015, pp. 118–133.

[64] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian network classifiers," *Machine Learning*, vol. 29, no. 2, pp. 131–163, Nov. 1997.

[65] T. N. Phyu, "Survey of classification techniques in data mining," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, Hong Kong, China, Mar. 2009, pp. 18–20.

[66] M. Scanagatta, A. Salmerón, and F. Stella, "A survey on bayesian network structure learning from data," *Progress in Artificial Intelligence*, May 2019.

[67] M. Tsagris, "Bayesian network learning with the PC algorithm: An improved and correct variation," *Applied Artificial Intelligence*, vol. 33, no. 2, pp. 101–123, Oct. 2019.

[68] K. Fukumizu, L. Song, and A. Gretton, "Kernel bayes' rule: Bayesian inference with positive definite kernels," *The Journal of Machine Learning Research*, vol. 14, no. 1, pp. 3753–3783, Jan. 2013.

[69] E. Schulz, M. Speekenbrink, and A. Krause, "A tutorial on gaussian process regression: Modelling, exploring, and exploiting functions," *Journal of Mathematical Psychology*, vol. 85, pp. 1 – 16, Aug. 2018.

[70] T. A. Kerkiri and D. Konetas, "Collaborative filtering: Inference from interactive web," in *Semantic Web Personalization and Context Awareness: Management of Personal Identities and Social Networking*. IGI Global, 2011, pp. 151–163.

[71] I. Goodfellow, Y. Bengio, and A. Courville, "Deep feedforward networks," in *Deep learning*. MIT press, 2016, ch. 6, pp. 163–220.

[72] ——, "Convolutional networks," in *Deep learning*. MIT press, 2016, ch. 9, pp. 321–362.

[73] ——, "Sequence modeling: Recurrent and recursive nets," in *Deep learning*. MIT press, 2016, ch. 10, pp. 363–408.

[74] J. Chung, Ç. Gülçehre, K. Cho, and Y. Bengio, "Empirical evaluation of gated recurrent neural networks on sequence modeling," *CoRR*, vol. abs/1412.3555, 2014. [Online]. Available: http://arxiv.org/abs/1412.3555

[75] H. Bakırcıoğlu and T. Koçak, "Survey of random neural network applications," *European Journal of Operational Research*, vol. 126, no. 2, pp. 319 – 330, Oct. 2000.

[76] M. A. Alsheikh, S. Lin, D. Niyato, and H. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1996–2018, Fourthquarter 2014.

[77] T. Hastie, R. Tibshirani, and J. Friedman, "Unsupervised learning," in *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. New York, NY: Springer New York, 2009, ch. 14, pp. 485–585.

[78] E. Schubert, J. Sander, M. Ester, H. P. Kriegel, and X. Xu, "DBSCAN revisited, revisited: Why and how you should (still) use DBSCAN," *ACM Trans. Database Syst.*, vol. 42, no. 3, Jul. 2017. [Online]. Available: https://doi.org/10.1145/3068335

[79] L. Rokach, "A survey of clustering algorithms," in *Data Mining and Knowledge Discovery Handbook*, O. Maimon and L. Rokach, Eds. Boston, MA: Springer US, 2010, pp. 269–298.

[80] G. Molenberghs and M. G. Kenward, "The expectation-maximization algorithm," in *Missing Data in Clinical Studies*. John Wiley & Sons, Ltd, 2007, ch. 8, pp. 93–104.

[81] C. M. Bishop, *Pattern recognition and machine learning*. springer, 2006.

[82] T. Howley, M. G. Madden, M.-L. O'Connell, and A. G. Ryder, "The effect of principal component analysis on machine learning accuracy with high dimensional spectral data," in *Applications and Innovations in Intelligent Systems XIII*, A. Macintosh, R. Ellis, and T. Allen, Eds. London: Springer London, 2006, pp. 209–222.

[83] A. Datta, S. Ghosh, and A. Ghosh, "PCA, kernel PCA and dimensionality reduction in hyperspectral images," in *Advances in Principal Component Analysis*. Springer, 2018, pp. 19–46.

[84] I. Borg and P. J. Groenen, "The four purposes of multidimensional scaling," in *Modern Multidimensional Scaling: Theory and Applications*. Springer, 2005, ch. 1, pp. 3–18.

[85] A. N. Gorban, B. Kégl, D. C. Wunsch, A. Y. Zinovyev *et al.*, *Principal manifolds for data visualization and dimension reduction*. Springer, 2008, vol. 58.

[86] I. Borg and P. J. Groenen, "Classical scaling," in *Modern Multidimensional Scaling: Theory and Applications*. Springer, 2005, ch. 12, pp. 261–267.

[87] R. R. Coifman and S. Lafon, "Diffusion maps," *Applied and Computational Harmonic Analysis*, vol. 21, no. 1, pp. 5 – 30, 2006, special Issue: Diffusion Maps and Wavelets.

[88] J. De la Porte, B. Herbst, W. Hereman, and S. Van Der Walt, "An introduction to diffusion maps," in *Proceedings of the 19th Symposium of the Pattern Recognition Association of South Africa (PRASA 2008)*, Cape Town, South Africa, 2008, pp. 15–25.

[89] D. Schweizer, M. Zehnder, H. Wache, H. Witschel, D. Zanatta, and M. Rodriguez, "Using consumer behavior data to reduce energy consumption in smart homes: Applying machine learning to save energy without lowering comfort of inhabitants," in *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, Miami, FL, USA,, Dec. 2015, pp. 1123–1129.

[90] I. Goodfellow, Y. Bengio, and A. Courville, "Autoencoders," in *Deep learning*. MIT press, 2016, ch. 14, pp. 493–516.

[91] Chang Wook Ahn and R. S. Ramakrishna, "QoS provisioning dynamic connection-admission control for multimedia wireless networks using a hopfield neural network," *IEEE Transactions on Vehicular Technology*, vol. 53, no. 1, pp. 106–117, 2004.

[92] J. J. Hopfield, "Neural networks and physical systems with emergent collective computational abilities," *Proceedings of the National Academy of Sciences*, vol. 79, no. 8, pp. 2554–2558, 1982.

[93] T. Kohonen, T. Huang, and M. Schroeder, *Self-Organizing Maps*, ser. Physics and astronomy online library. Springer Berlin Heidelberg, 2001.

[94] H. A. A. Al-Rawi, M. A. Ng, and K.-L. A. Yau, "Application of reinforcement learning to routing in distributed wireless networks: a review," *Artificial Intelligence Review*, vol. 43, no. 3, pp. 381–416, Mar. 2015.

[95] R. S. Sutton and A. G. Barto, "Temporal-difference learning," in *Reinforcement learning: An introduction*. MIT press, 2018, ch. 6, pp. 119–140.

[96] ——, "Policy gradient methods," in *Reinforcement learning: An introduction*. MIT press, 2018, ch. 13, pp. 321–338.

[97] M. G. Lagoudakis and R. Parr, "Least-squares policy iteration," *J. Mach. Learn. Res.*, vol. 4, pp. 1107–1149, Dec. 2003.

[98] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 10, pp. 1345–1359, 2010.

[99] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, Jan. 2019.

[100] M. Chincoli, S. Stavrou, and A. Liotta, "Density and transmission power in intelligent wireless sensor networks," in *Proc. 2018 14th International Wireless Communications Mobile Computing Conference (IWCMC)*, Limassol, Cyprus, Jun. 2018, pp. 1518–1523.

[101] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 563–575, Dec. 2017.

[102] F. K. Shaikh and S. Zeadally, "Energy harvesting in wireless sensor networks: A comprehensive review," *Renewable and Sustainable Energy Reviews*, vol. 55, pp. 1041 – 1054, Mar. 2016.

[103] D. Ventura, D. Casado-Mansilla, J. López-de Armentia, P. Garaizar, D. López-de Ipiña, and V. Catania, "ARIIMA: A real IoT implementation of a machine-learning architecture for reducing energy consumption," in *Proc. Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services*, R. Hervás, S. Lee, C. Nugent, and J. Bravo, Eds. Belfast, UK: Springer International Publishing, Dec. 2014, pp. 444–451.

[104] M. Zehnder, H. Wache, H. Witschel, D. Zanatta, and M. Rodriguez, "Energy saving in smart homes based on consumer behavior: A case

study," in *Proc. 2015 IEEE First International Smart Cities Conference (ISC2)*, Guadalajara, Mexico, Oct. 2015, pp. 1–6.

[105] J. S. Jang, Y. L. Kim, and J. H. Park, "A study on the optimization of the uplink period using machine learning in the future IoT network," in *Proc. 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, Sydney, NSW, Mar. 2016, pp. 1–3.

[106] S. Dharur, C. Hota, and K. Swaminathan, "Energy efficient IoT framework for smart buildings," in *Proc. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Coimbatore,India, Feb. 2017, pp. 793–800.

[107] W. Song, N. Feng, Y. Tian, and S. Fong, "An IoT-based smart controlling system of air conditioner for high energy efficiency," in *Proc. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Devon, UK, Jun. 2017, pp. 442–449.

[108] A. Javed, H. Larijani, and A. Wixted, "Improving energy consumption of a commercial building with IoT and machine learning," *IT Professional*, vol. 20, no. 5, pp. 30–38, Sep. 2018.

[109] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano, and O. M. Caicedo, "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," *Journal of Internet Services and Applications*, vol. 9, no. 1, p. 16, Jun. 2018.

[110] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for internet of things," *International Journal of Machine Learning and Cybernetics*, vol. 9, no. 8, pp. 1399–1417, Aug. 2018.

[111] S. Mwanje, G. Decarreau, C. Mannweiler, M. Naseer-ul-Islam, and L. C. Schmelz, "Network management automation in 5G: Challenges and opportunities," in *Proc. 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Valencia, Spain, Sep. 2016, pp. 1–6.

[112] B. Keshavamurthy and M. Ashraf, "Conceptual design of proactive SONs based on the big data framework for 5G cellular networks: A novel machine learning perspective facilitating a shift in the son paradigm," in *Proc. 2016 International Conference System Modeling Advancement in Research Trends (SMART)*, Moradabad, India, Nov. 2016, pp. 298–304.

[113] J. Ali-Tolppa, S. Kocsis, B. Schultz, L. Bodrog, and M. Kajo, "Self-healing and resilience in future 5G cognitive autonomous networks," in *Proc. 2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K)*, Santa Fe, Argentina, Nov. 2018, pp. 1–8.

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

[115] P. V. Klaine, M. A. Imran, O. Onireti, and R. D. Souza, "A survey of machine learning techniques applied to self-organizing cellular networks," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2392–2431, Fourthquarter 2017.

[116] J. Moysen and L. Giupponi, "From 4G to 5G: Self-organized network management meets machine learning," *Computer Communications*, vol. 129, pp. 248 – 268, Sep. 2018.

[117] R. Amiri and H. Mehrpouyan, "Self-organizing mm wave networks: A power allocation scheme based on machine learning," in *Proc. 2018 11th Global Symposium on Millimeter Waves (GSMM)*, Boulder, CO, May 2018, pp. 1–4.

[118] L. Le, D. Sinh, L. Tung, and B. P. Lin, "A practical model for traffic forecasting based on big data, machine-learning, and network kpis," in *Proc. 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Las Vegas, USA, Jan. 2018, pp. 1–4.

[119] L. Le, B. P. Lin, L. Tung, and D. Sinh, "SDN/NFV, machine learning, and big data driven network slicing for 5G," in *Proc. 2018 IEEE 5G World Forum (5GWF)*, Silicon Valley, CA, Jul. 2018, pp. 20–25.

[120] Nvidia. (2019) Hardware for every situation. Nvidia. [Accessed: May 28, 2019]. [Online]. Available: https://developer.nvidia.com/embedded/develop/hardware

[121] Intel. (2018) Product brief Intel Movidius Myriad X VPU enhanced visual intelligence at the network edge. Intel. [Accessed: May 28, 2019]. [Online]. Available: https://movidius-uploads.s3.amazonaws.com/1532110136-MyriadXVPU_ProductBrief_final_07.18.pdf

[122] ——. (2019) Intel neural compute stick 2. Intel. [Accessed: May 28, 2019]. [Online]. Available: https://software.intel.com/en-us/neural-compute-stick

[123] Google. (2019) Dev board datasheets. Google. [Accessed: May 28, 2019]. [Online]. Available: https://coral.withgoogle.com/docs/dev-board/datasheet/

[124] ——. (2019) Edge TPU performance benchmarks. Google. [Accessed: May 28, 2019]. [Online]. Available: https://coral.withgoogle.com/docs/edgetpu/benchmarks/

[125] ——. (2019) USB accelerator datasheet. Google. [Accessed: May 28, 2019]. [Online]. Available: https://coral.withgoogle.com/docs/accelerator/datasheet/

[126] Qualcomm. (2019) Qualcomm Snapdragon 855 mobile platform product brief. Qualcomm. [Accessed: May 28, 2019]. [Online]. Available: https://www.qualcomm.com/media/documents/files/snapdragon-855-mobile-platform-product-brief.pdf

[127] HiSilicon. (2019) Kirin. HiSilicon. [Accessed: May 28, 2019]. [Online]. Available: http://www.hisilicon.com/en/Products/ProductList/Kirin

[128] Samsung. (2019) Exynos 9820 the next-level processor for the mobile future. Samsung. [Accessed: May 28, 2019]. [Online]. Available: https://www.samsung.com/semiconductor/global.semi.static/minisite/exynos/file/solution/MobileProcessor-9-Series-9820.pdf

[129] MediaTek. (2019) Mediatek Helio P90 product brief. MediaTek. [Accessed: May 28, 2019]. [Online]. Available: https://d86o2zu8ugzlg.cloudfront.net/mediatek-craft/documents/mediatek-helio-p90/MediaTek-Helio-P90-Product-Brief-0119.pdf

[130] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, "Artificial intelligence for vehicle-to-everything: A survey," *IEEE Access*, vol. 7, pp. 10 823–10 843, 2019.

[131] H. Jeong, I. Jeong, H. Lee, and S. Moon, "Computation offloading for machine learning web apps in the edge server environment," in *Proc. 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, Jul. 2018, pp. 1492–1499.

[132] K. Portelli and C. Anagnostopoulos, "Leveraging edge computing through collaborative machine learning," in *Proc. 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Prague, Czech Republic, Aug. 2017, pp. 164–169.

[133] C. Liu, Y. Cao, Y. Luo, G. Chen, V. Vokkarane, M. Yunsheng, S. Chen, and P. Hou, "A new deep learning-based food recognition system for dietary assessment on an edge computing service infrastructure," *IEEE Transactions on Services Computing*, vol. 11, no. 2, pp. 249–261, Mar. 2018.

[134] K. Kim and Y. Hong, "Autonomous network traffic control system based on intelligent edge computing," in *Proc. 2019 21st International Conference on Advanced Communication Technology (ICACT)*, PyeongChang,South Korea, Feb. 2019, pp. 164–167.

[135] Z. Feng, S. George, J. Harkes, P. Pillai, R. Klatzky, and M. Satyanarayanan, "Edge-based discovery of training data for machine learning," in *Proc. 2018 IEEE/ACM Symposium on Edge Computing (SEC)*, Bellevue, WA, Oct. 2018, pp. 145–158.

[136] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "Ubehealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32 258–32 285, 2018.

[137] P. Warden and D. Situnayake, *Tinyml: Machine learning with tensorflow lite on arduino and ultra-low-power microcontrollers*. " O'Reilly Media, Inc.", 2019.

[138] J. Schneible and A. Lu, "Anomaly detection on the edge," in *Proc. MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Baltimore, MD, Oct. 2017, pp. 678–682.

[139] J. Moon, S. Cho, S. Kum, and S. Lee, "Cloud-edge collaboration framework for iot data analytics," in *Proc. 2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, Oct. 2018, pp. 1414–1416.

[140] F. D. Vita, D. Bruneo, A. Puliafito, G. Nardini, A. Virdis, and G. Stea, "A deep reinforcement learning approach for data migration in multi-access edge computing," in *Proc. 2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K)*, Santa Fe, Argentina, Nov. 2018, pp. 1–8.

[141] N. Cheng, F. Lyu, W. Quan, C. Zhou, H. He, W. Shi, and X. Shen, "Space/aerial-assisted computing offloading for iot applications: A learning-based approach," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 5, pp. 1117–1129, May 2019.

[142] R. Ratasuk, A. Prasad, Z. Li, A. Ghosh, and M. A. Uusitalo, "Recent advancements in M2M communications in 4G networks and evolution towards 5G," in *Proc. 2015 18th International Conference on Intelligence in Next Generation Networks*, Paris, France, Feb. 2015, pp. 52–57.

[143] 3GPP, "Study on provision of low-cost machine-type communications (MTC) user equipments (ues) based on lte," 3GPP, Tech. Rep. 36.888, Jun. 2015.

[144] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Communications Surveys Tutorials*, vol. 16, no. 2, pp. 619–641, SecondQuarter 2014.

[145] A. Kumbhar, F. Koohifar, İ. Güvenç, and B. Mueller, "A survey on legacy and emerging technologies for public safety communications," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 97–124, Firstquarter 2017.

[146] T. Doumi, M. F. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, "LTE for public safety networks," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 106–112, Feb. 2013.

[147] K. Gomez, L. Goratti, T. Rasheed, and L. Reynaud, "Enabling disaster-resilient 4G mobile communication networks," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 66–73, Dec. 2014.

[148] L. G. U. Garcia, E. P. L. Almeida, V. S. B. Barbosa, G. Caldwell, I. Rodriguez, H. Lima, T. B. Sørensen, and P. Mogensen, "Mission-critical mobile broadband communications in open-pit mines," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 62–69, Apr. 2016.

[149] A. Orsino, A. Ometov, G. Fodor, D. Moltchanov, L. Militano, S. Andreev, O. N. C. Yilmaz, T. Tirronen, J. Torsner, G. Araniti, A. Iera, M. Dohler, and Y. Koucheryavy, "Effects of heterogeneous mobility on D2D- and drone-assisted mission-critical MTC in 5G," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 79–87, Feb. 2017.

[150] M. Mozaffari, W. Saad, M. Bennis, Y. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys Tutorials*, vol. Early Access, 2019.

[151] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications Surveys Tutorials*, vol. Early Access, 2019.

[152] *5G; Service requirements for next generation new services and markets*, 3GPP Std. TS 22.261, Jul. 2018.

[153] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 5–20, FirstQuarter 2013.

[154] G. J. Sutton, J. Zeng, R. P. Liu, W. Ni, D. N. Nguyen, B. A. Jayawickrama, X. Huang, M. Abolhasan, Z. Zhang, E. Dutkiewicz, and T. Lv, "Enabling technologies for ultra-reliable and low latency communications: From phy and mac layer perspectives," *IEEE Communications Surveys Tutorials*, vol. Early Access, 2019.

[155] G. Durisi, T. Koch, and P. Popovski, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[156] C. She, Z. Chen, C. Yang, T. Q. S. Quek, Y. Li, and B. Vucetic, "Improving network availability of ultra-reliable and low-latency communications with multi-connectivity," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5482–5496, Nov. 2018.

[157] A. Weinand, M. Karrenbauer, J. Lianghai, and H. D. Schotten, "Physical layer authentication for mission critical machine type communication using gaussian mixture model based clustering," in *Proc. 2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Sydney, NSW, Jun. 2017, pp. 1–5.

[158] H. Forssell, R. Thobaben, H. Al-Zubaidy, and J. Gross, "Physical layer authentication in mission-critical mtc networks: A security and delay performance analysis," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 4, pp. 795–808, Apr. 2019.

[159] H. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical iot applications," *IEEE Transactions on Wireless Communications*, vol. 18, no. 5, pp. 2565–2578, May 2019.

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

[161] H. Zhang, N. Liu, X. Chu, K. Long, A. Aghvami, and V. C. M. Leung, "Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, Aug. 2017.

[162] W. Guan, X. Wen, L. Wang, Z. Lu, and Y. Shen, "A service-oriented deployment policy of end-to-end network slicing based on complex network theory," *IEEE Access*, vol. 6, pp. 19 691–19 701, 2018.

[163] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G network slicing for vehicle-to-everything services," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 38–45, Dec. 2017.

[164] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55 765–55 779, 2018.

[165] F. Kurtz, C. Bektas, N. Dorsch, and C. Wietfeld, "Network slicing for critical communications in shared 5G infrastructures - an empirical evaluation," in *Proc. 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, Seoul, South Korea, Jun. 2018, pp. 393–399.

[166] V. Petrov, M. A. Lema, M. Gapeyenko, K. Antonakoglou, D. Moltchanov, F. Sardis, A. Samuylov, S. Andreev, Y. Koucheryavy, and M. Dohler, "Achieving end-to-end reliability of mission-critical traffic in softwarized 5G networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 485–501, Mar. 2018.

[167] F. Kurtz, N. Dorsch, and C. Wietfeld, "Empirical comparison of virtualized and bare-metal switching for SDN-based 5G communication in critical infrastructures," in *Proc. 2016 IEEE NetSoft Conference and Workshops (NetSoft)*, Seoul, South Korea, Jun. 2016, pp. 453–458.

[168] N. T. Hai and D. Kim, "Efficient load balancing for multi-controller in SDN-based mission-critical networks," in *Proc. 2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, Poitiers, France, Jul. 2016, pp. 420–425.

[169] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks based smart grid communication: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. Early Access, 2019.

[170] M. A. Raza, M. Abolhasan, J. Lipman, N. Shariati, and W. Ni, "Statistical learning-based dynamic retransmission mechanism for mission critical communication: An edge-computing approach," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, 2020, pp. 393–396.

[171] T. Akiba, H. Matsukawa, H. Narimatsu, S. Eitoku, and K. Kitamura, "Device functions virtualization architecture," in *Proc. 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE)*, Nagoya, Japan, Oct. 2017, pp. 1–2.

[172] G. Laput, Y. Zhang, and C. Harrison, "Synthetic sensors: Towards general-purpose sensing," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, Denver, CO, Jun. 2017, pp. 3986–3999.

[173] L. Xu, R. Collier, and G. M. P. O'Hare, "A survey of clustering techniques in wsns and consideration of the challenges of applying such to 5G IoT scenarios," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1229–1249, Oct. 2017.

[174] J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the edge: A scalable IoT architecture based on transparent computing," *IEEE Network*, vol. 31, no. 5, pp. 96–105, Aug. 2017.

[175] N. Dandanov, S. R. Samal, S. Bandopadhaya, V. Poulkov, K. Tonchev, and P. Koleva, "Comparison of wireless channels for antenna tilt based coverage and capacity optimization," in *Proc. 2018 Global Wireless Summit (GWS)*, Chiang Rai, Thailand, Nov. 2018, pp. 119–123.

[176] S. Murali and A. Jamalipour, "Mobility-aware energy-efficient parent selection algorithm for low power and lossy networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2593–2601, Apr. 2019.

[177] S. Berger, A. Fehske, P. Zanier, I. Viering, and G. Fettweis, "Online antenna tilt-based capacity and coverage optimization," *IEEE Wireless Communications Letters*, vol. 3, no. 4, pp. 437–440, Aug. 2014.

[178] M. R. Palattella and N. Accettura, "Enabling internet of everything everywhere: LPWAN with satellite backhaul," in *Proc. 2018 Global Information Infrastructure and Networking Symposium (GIIS)*, Thessaloniki, Greece, Oct. 2018, pp. 1–5.

[179] D. Arellanes and K. Lau, "Analysis and classification of service interactions for the scalability of the internet of things," in *Proc. 2018 IEEE International Congress on Internet of Things (ICIOT)*, San Francisco, CA, Jul. 2018, pp. 80–87.

[180] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1617–1634, ThirdQuarter 2014.

[181] M. Abolhasan, M. Abdollahi, W. Ni, A. Jamalipour, N. Shariati, and J. Lipman, "A routing framework for offloading traffic from cellular networks to sdn-based multi-hop device-to-device networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1516–1531, Dec. 2018.

[182] *Network functions virtualisation (nfv): Architectural framework*, ETSI Std. RGS/NFV-002, 2014.

[183] Y. Li and M. Chen, "Software-defined network function virtualization: A survey," *IEEE Access*, vol. 3, pp. 2542–2553, 2015.

[184] D. Bhamare, R. Jain, M. Samaka, and A. Erbad, "A survey on service function chaining," *Journal of Network and Computer Applications*, vol. 75, pp. 138 – 155, Nov. 2016.

[185] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[186] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, Jun. 2019.

[187] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in *Proc. 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 5772–5781.

[188] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[189] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64–71, 2016.

[190] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proc. 3rd ACM International Symposium on Information processing in sensor networks*, 2004, pp. 259–268.

[191] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure Integrated Circuits and Systems*. Springer, 2010, pp. 27–42.

[192] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *Proc. 21st IEEE Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016, pp. 519–524.

[193] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, 2015.

[194] B. Balamurugan and B. Dyutimoy, "Security in network layer of IoT: Possible measures to preclude," in *Security Breaches and Threat Prevention in the Internet of Things*, N., Jeyanthi and R., Thandeeswaran, Ed. IGI Global, 2017, ch. 3, pp. 46–75.

[195] S. Skorobogatov, "Fault attacks on secure chips: from glitch to flash," *Design and Security of Cryptographic Algorithms and Devices (ECRYPT II)*, 2011.

[196] ——, "Flash memory 'bumping' attacks," in *Cryptographic Hardware and Embedded Systems, CHES 2010*, S. Mangard and F.-X. Standaert, Eds. Berlin, Heidelberg: Springer, 2010, pp. 158–172.

[197] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "A dynamic prime number based efficient security mechanism for big sensing data streams," *Journal of Computer and System Sciences*, vol. 83, no. 1, pp. 22–42, 2017.

[198] S. Mohammadi and H. Jadidoleslamy, "A comparison of link layer attacks on wireless sensor networks," *arXiv preprint arXiv:1103.5589*, 2011.

[199] S. Murali and A. Jamalipour, "A lightweight intrusion detection for sybil attack under mobile rpl in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, Jan. 2020.

[200] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of Internet of Things," *arXiv preprint arXiv:1501.02211*, 2015.

[201] V. B. Misic, J. Fang, and J. Misic, "MAC layer security of 802.15.4-compliant networks," in *Proc. IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 2005, pp. 1–8.

[202] A. Reziouk, E. Laurent, and J.-C. Demay, "Practical security overview of IEEE 802.15.4," in *Proc. IEEE International Conference on Engineering & MIS (ICEMIS)*, 2016, pp. 1–9.

[203] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proc. Proceedings of the 3rd ACM workshop on Wireless security*, 2004, pp. 32–42.

[204] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-health IoT applications," in *Proc. 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 276–281.

[205] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in *Proc. ACM workshop on Security, privacy & dependability for cyber vehicles*, 2013, pp. 61–64.

[206] J. Murphy, "Enhanced Security Controls for IBM Watson IoT Platform," *IBM Watson IoT Platform*, 2016. [Online]. Available: https://developer.ibm.com/iotplatform/2016/09/23/enhanced-security-controls-for-ibm-watson-iot-platform/

[207] J. Pan and J. McElhannon, "Future edge cloud and edge computing for internet of things applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 439–449, 2017.

[208] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[209] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[210] W. H. Hassan *et al.*, "Current research on internet of things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

[211] N. Kshetri, "Can blockchain strengthen the internet of things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[212] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," *ePrint*, 2017.

[213] S. Sara and N. Michael, "Facebook has been worried about data leaks like this since it went public in 2012,," 2018. Last accessed 11 September 2018. [Online]. Available: https://www.cnbc.com/2018/04/12/facebook-warned-of-data-breaches-years-ago-when-it-went-public-in-2012.html

[214] K. Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," *New York Times*, 2018. [Online]. Available: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

[215] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1–6.

[216] OWASP. (2017) The Ten Most Critical Web Application Security Risks. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

[217] SQLi. (2016) SQLi, XSS zero-days expose Belkin IoT devices, Android smartphones. [Online]. Available: https://www.csoonline.com/article/3138935/security/sqli-xss-zero-days-expose-belkin-iot-devices-android-smartphones.html

[218] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1636–1675, Secondquarter 2019.

[219] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *Proc. 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 163–167.

[220] XSS. (2018) Cross-site Scripting Attack. [Online]. Available: https://www.acunetix.com/websitesecurity/cross-site-scripting/

[221] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–29, 2019.

[222] R. T. Tiburski, L. A. Amaral, E. de Matos, D. F. de Azevedo, and F. Hessel, "Evaluating the use of TLS and DTLS protocols in IoT middleware systems applied to e-health," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2017, pp. 480–485.

[223] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security issues for cloud computing," *Optimizing Information Security and Advancing Privacy Assurance: New Technologies*, vol. 150, 2012.

[224] S. Boudko and H. Abie, "Adaptive cybersecurity framework for healthcare internet of things," in *In Proceedings of the 13th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, 2019, pp. 1–6.

[225] J. Rajamäki and R. Pirinen, "Towards the cyber security paradigm of ehealth: Resilience and design aspects," in *AIP Conference Proceedings*, vol. 1836, no. 1. AIP Publishing LLC, 2017, p. 020029.

[226] A. Laugé, J. Hernantes, and J. M. Sarriegi, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach," *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 16–23, 2015.

[227] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the internet of things," *Computer Networks*, vol. 129, pp. 444–458, 2017.

[228] S. Plaga, N. Wiedermann, S. D. Anton, S. Tatschner, H. Schotten, and T. Newe, "Securing future decentralised industrial iot infrastructures: Challenges and free open source solutions," *Future Generation Computer Systems*, vol. 93, pp. 596–608, 2019.

[229] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, 2011.

[230] R. Langner, "To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve," 2013. [Online]. Available: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[231] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: a survey, research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2018.

[232] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir computing meets smart grids: Attack detection using delayed feedback networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 734–743, 2017.

[233] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *In Proceedings of IEEE Symposium on Computers and Communication (ISCC)*. IEEE, 2015, pp. 180–187.

[234] A. Amies, *Developing and hosting applications on the cloud*. IBM Press, 2012.

[235] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the internet of things," in *2012 32nd International Conference on Distributed Computing Systems Workshops*. IEEE, 2012, pp. 588–592.

[236] A. Shamir, "Identity-based cryptosystem based on the discrete logarithm problem," in *Proc. CRYPTO'84*, 1985, pp. 47–53.

[237] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89–98.

[238] ISO. (2017) ISO 27001 Risk Assessments, IT Governance U.K. [Online]. Available: https://www.itgovernance.co.uk/iso27001/iso27001-risk-assessment

[239] NIST. (2012) Guide for Conducting Risk Assessment. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[240] AT&T. (2016) The CEO's Guide to Data Security. Protect your data through innovation - AT&T Cybersecurity Insights (Vol 5). [Online]. Available: https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf

[241] B. Greenstein, "IoT devices used in DDoS Attacks," *IBM Internet of Things Blogs*, 2016. [Online]. Available: https://www.ibm.com/blogs/internet-of-things/ddos-iot-platform-security/

[242] IBM. (2016) IoT Security: An IBM Position Paper. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12379USEN\&

[243] TCG. (2015) Guidance for Securing IoT using TCG Technology, Version 1, Revision 21 . [Online]. Available: https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf

[244] ——. (2015) TCG Infrastructure WG TPM Keys for Platform Identity for TPM 1.2. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/TPM_Keys_for_Platform_Identity_v1_0_r3_Final.pdf

[245] V. Benjumea, S. G. Choi, J. Lopez, and M. Yung, "Anonymity 2.0–X. 509 extensions supporting privacy-friendly authentication," in *International Conference on Cryptology and Network Security*. Springer, 2007, pp. 265–281.

[246] S. Chen, M. Ma, and Z. Luo, "An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems," *Security and Communication Networks*, vol. 9, no. 10, pp. 1146–1157, 2016.

[247] Y. Qiu and M. Ma, "A mutual authentication and key establishment scheme for M2M communication in 6LowPAN networks," *IEEE transactions on industrial informatics*, vol. 12, no. 6, pp. 2074–2085, 2016.

[248] Y. Qiu, M. Ma, and S. Chen, "An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems," *Computer Networks*, vol. 129, pp. 306–318, 2017.

[249] P. Soon-Shiong, H. Kupwade-Patil, R. Seshadri, and N. J. Witchey, "Homomorphic encryption in a healthcare network environment, system and methods," Feb. 5 2019, uS Patent 10,200,347.

[250] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Whitepaper*, 2008.

[251] HLF. (2017) Hyperledger Business Blockchain Technologies, The Linux Foundation. [Online]. Available: https://www.hyperledger.org/projects

[252] P. Foxhoven, J. A. Chanak, W. Fehring, D. Wessels, P. Desai, M. Apte, and S. P. Herle, "Cloud-based virtual private access systems and methods," Aug. 6 2019, uS Patent 10,375,024.

[253] DoD. (2012) Information Security Advice: Network Segmentation and Segregation, Australian Government Department of Defence. [Online]. Available: https://www.asd.gov.au/publications/protect/network_segmentation_segregation.htm

[254] O. Flauzac, C. González, A. Hachani, and F. Nolot, "Sdn based architecture for iot and improvement of the security," in *Proc. 29th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2015, pp. 688–693.

[255] F. Jazib, C. Pignataro, A. Jeff, and M. Monique, "Securing the Internet of Things: A Proposed Framework," *Cisco Security Research & Operations*, 2015. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

[256] I. Indre and C. Lemnaru, "Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things," in *Proc. 12th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, Sept 2016, pp. 175–182.

[257] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proc. 14th ACM Workshop on Hot Topics in Networks*, 2015, pp. 1–7.

[258] IBM. (2015) IBM Point of View: Internet of Things Security. [Online]. Available: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN

[259] F. Ünlü, L. Wawrla, and A. Dìaz, "Energy harvesting technologies for IoT edge devices," *4E, Int. Energy Agency, Paris, France*, 2018.

[260] Y.-k. Wang, G.-p. Sheng, B.-j. Shi, W.-w. Li, and H.-q. Yu, "A novel electrochemical membrane bioreactor as a potential net energy producer for sustainable wastewater treatment," *Scientific Reports (Nature Publisher Group)*, vol. 3, p. 1864, May 2013, copyright - Copyright Nature Publishing Group May 2013; Last updated - 2017-08-18.

[261] V. Kuhn, C. Lahuec, F. Seguin, and C. Person, "A multi-band stacked RF energy harvester with RF-to-DC efficiency up to 84%," *IEEE Transactions on Microwave Theory and Techniques*, vol. 63, no. 5, pp. 1768–1778, May 2015.

[262] N. Shariati, W. S. Rowe, J. R. Scott, and K. Ghorbani, "Multi-service highly sensitive rectifier for enhanced RF energy scavenging," *Scientific reports*, vol. 5, p. 9655, May 2015.

[263] S. B. Inayat, K. R. Rader, and M. M. Hussain, "Nano-materials enabled thermoelectricity from window glasses," *Scientific reports*, vol. 2, p. 841, Nov. 2012.

[264] R. J. Vyas, B. B. Cook, Y. Kawahara, and M. M. Tentzeris, "E-WEHP: A batteryless embedded sensor-platform wirelessly powered from ambient digital-TV signals," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 6, pp. 2491–2505, Jun. 2013.

[265] J. A. Paradiso and T. Starner, "Energy scavenging for mobile and wireless electronics," *IEEE Pervasive Computing*, vol. 4, no. 1, pp. 18–27, Mar. 2005.

[266] X. Tang, X. Wang, R. Cattley, F. Gu, and A. D. Ball, "Energy harvesting technologies for achieving self-powered wireless sensor networks in machine condition monitoring: A review," *Sensors*, vol. 18, no. 12, p. 4113, Nov. 2018.

[267] N. Shariati, W. S. T. Rowe, and K. Ghorbani, "Highly sensitive FM frequency scavenger integrated in building materials," in *2015 European Microwave Conference (EuMC)*, Paris, France, Sep. 2015, pp. 68–71.

[268] ——, "Highly sensitive rectifier for efficient rf energy harvesting," in *2014 44th European Microwave Conference*, Rome, Italy, Oct. 2014, pp. 1190–1193.

[269] R. Vullers, R. [van Schaijk], I. Doms, C. V. Hoof], and R. Mertens, "Micropower energy harvesting," *Solid-State Electronics*, vol. 53, no. 7, pp. 684 – 693, Jul. 2009.

[270] X. Yue, J. Kiely, D. Gibson, and E. M. Drakakis, "Charge-based supercapacitor storage estimation for indoor sub-mw photovoltaic energy harvesting powered wireless sensor nodes," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 3, pp. 2411–2421, Mar. 2020.

[271] H. Yang, "A review of supercapacitor-based energy storage systems for microgrid applications," in *2018 IEEE Power Energy Society General Meeting (PESGM)*, Portland, OR, USA, 2018, pp. 1–5.

[272] Analog Devices. (2020) Supercapacitor chargers. Analog Devices. [Accessed: September 16, 2020]. [Online]. Available: https://www.analog.com/en/products/power-management/supercapacitor-chargers.html

[273] Texas Instruments. (2020) Battery management IC. Texas Instruments. [Accessed: September 16, 2020]. [Online]. Available: https://www.ti.com/power-management/battery-management/overview.html

[274] Murata. (2020) DMF4B5R5G105M3DTA0. Murata. [Accessed: September 16, 2020]. [Online]. Available: https://www.murata.com/en-us/products/productdetail?partno=DMF4B5R5G105M3DTA0

[275] ICT International. (2020) Products. ICT International. [Accessed: September 16, 2020]. [Online]. Available: http://www.ictinternational.com/products

[276] Z. Stevic, *Supercapacitor Design and Applications*. IntechOpen, 2016.

[277] A. Lahyani, P. Venet, A. Guermazi, and A. Troudi, "Battery/supercapacitors combination in uninterruptible power supply (ups)," *IEEE Transactions on Power Electronics*, vol. 28, no. 4, pp. 1509–1522, Apr. 2013.

[278] O. Elsayed, M. Abouzied, and E. Sánchez-Sinencio, "A 540 μw rf wireless receiver assisted by rf blocker energy harvesting for iot applications with +18 dBm OB-IIP3," in *2016 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, San Francisco, CA, USA, May 2016, pp. 230–233.

[279] E. Alliance. (2019) Kieback&peter en:key room thermostat. EnOcean Alliance. [Accessed: May 28, 2019]. [Online]. Available: https://www.enocean-alliance.org/product/kieback-peter-en-key-room-thermostat/

[280] EnOcean. (2017) STM 250J OEM - radio magnet contact. EnOcean. [Accessed: May 28, 2019]. [Online]. Available: https://www.enocean.com/en/products/enocean_modules_928mhz/stm-250j-oem/user-manual-pdf/

[281] ——. (2014) Rocker pad (single, double). EnOcean. [Accessed: May 28, 2019]. [Online]. Available: https://www.enocean.com/en/products/enocean_modules_902mhz/wireless-switch-esrp-edrp-oem/user-manual-pdf/

[282] ——. (2014) Key card switch. EnOcean. [Accessed: May 28, 2019]. [Online]. Available: https://www.enocean.com/en/products/enocean_modules_902mhz/key-card-switch-ekcs-oem/user-manual-pdf/

[283] ——. (2017) Occupancy sensor - ceiling mounted. EnOcean. [Accessed: May 28, 2019]. [Online]. Available: https://www.enocean.com/en/products/enocean_modules_902mhz/ceiling-mounted-occupancy-sensor-eosc-oem/user-manual-pdf/

[284] E. Alliance. (2019) Enocean easyclickpro room temperature sensor nova, pure white. EnOcean Alliance. [Accessed: May 28, 2019]. [Online]. Available: https://www.enocean-alliance.org/product/peha_easyclick-room-thermostat/

[285] R. Das. (2009) Batteryless infrared remote control from Arveni. IDTechEx. [Accessed: May 28, 2019]. [Online]. Available: https://www.offgridenergyindependence.com/articles/1842/batteryless-infrared-remote-control-from-arveni

[286] Energous. (2019) Da4100 wattup wireless power transmitter. Energous. [Accessed: April 30, 2020]. [Online]. Available: https://www.energous.com/wp-content/uploads/DA4100-Product-Brief-2019.pdf

[287] Perpetuum. (2020) Da4100 wattup wireless power transmitter. Perpetuum. [Accessed: April 30, 2020]. [Online]. Available: https://perpetuum.com/rail-applications/

[288] Pavegen. (2019) Oxford street, london. Pavegen. [Accessed: April 30, 2020]. [Online]. Available: https://pavegen.com/case-studies/oxford-street/

[289] EnGoplanet. (2020) Smart solar street lights. EnGoplanet. [Accessed: April 30, 2020]. [Online]. Available: https://www.engoplanet.com/engoplanet-smart-solar-street-light/

[290] Thermokon. (2020) SR65 wireless outdoor temperature sensor. Thermokon. [Accessed: April 30, 2020]. [Online]. Available: https://www.thermokon.de/download-archive/EasySens-Sender/Temperatur/SR65/ProduktblÃd'tter/SR65_EasySens_Datasheet_en.pdf

[291] Perpetua. (2020) Use cases thermoelectric delivers power for all industries. Perpetua. [Accessed: April 30, 2020]. [Online]. Available: https://perpetuapower.com/use-cases/

[292] K. Takeuchi, "Developing energy harvesting technologies for IoT applications - activities of public and private sectors in japan," 2016, in Energy Harvesting Consortium.

[293] Matrix. (2020) Powerwatch. Matrix. [Accessed: April 30, 2020]. [Online]. Available: https://www.powerwatch.com

[294] L. Ningbo Yongjiang Shenzhou Photovoltaic Co. (2020) Solar lamp. Ningbo Yongjiang Shenzhou Photovoltaic Co., Ltd. [Accessed: April 30, 2020]. [Online]. Available: http://www.nbszgd.com/en/product/class/82.html

[295] K. Technologies. (2017) Solar harvester. KCF Technologies. [Accessed: April 30, 2020]. [Online]. Available: https://www.kcftech.com/smartdiagnostics/products/harvesters/solar-harvester.html

[296] Libelium. (2020) Product overview. Libelium. [Accessed: April 30, 2020]. [Online]. Available: http://www.libelium.com/products/plug-sense/technical-overview/

[297] Perpetuum. (2013) Vibration energy harvesters. Perpetuum. [Accessed: April 30, 2020]. [Online]. Available: https://perpetuum.com/download/veh-vibration-energy-harvester-datasheet/?wpdmdl=913

[298] Powercast. (2016) P2110B 915 MHz RF powerharvester receiver. Powercast. [Accessed: April 30, 2020]. [Online]. Available: https://www.powercastco.com/wp-content/uploads/2016/12/P2110B-Datasheet-Rev-3.pdf

[299] STMicroelectronics. (2018) Ultralow power energy harvester and battery charger. STMicroelectronics. [Accessed: April 30, 2020]. [Online]. Available: https://www.st.com/resource/en/datasheet/spv1050.pdf

[300] Marlow. (2020) Technical data sheet preliminary. Marlow. [Accessed: April 30, 2020]. [Online]. Available: https://cdn2.hubspot.net/hubfs/547732/Data_Sheets/EHA-LXXLXX-R01-L1.pdf

[301] M. Piñuela, P. D. Mitcheson, and S. Lucyszyn, "Ambient RF energy harvesting in urban and semi-urban environments," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 7, pp. 2715–2726, Jul. 2013.

[302] N. Shariati, W. S. T. Rowe, and K. Ghorbani, "RF field investigation and maximum available power analysis for enhanced rf energy scavenging," in *2012 42nd European Microwave Conference*, Amsterdam, Netherlands, Oct. 2012, pp. 329–332.

[303] S. Keshavarz, A. Abdipour, A. Mohammadi, and R. Keshavarz, "Design and implementation of low loss and compact microstrip triplexer using CSRR loaded coupled lines," *AEU - International Journal of Electronics and Communications*, vol. 111, p. 152913, Nov. 2019.

[304] R. Keshavarz, A. Mohammadi, and A. Abdipour, "A quad-band distributed amplifier with E-CRLH transmission line," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 12, pp. 4188–4194, Dec. 2013.

[305] Z. Chen, B. Guo, Y. Yang, and C. Cheng, "Metamaterials-based enhanced energy harvesting: A review," *Physica B: Condensed Matter*, vol. 438, pp. 1 – 8, Apr. 2014.

[306] K. Chaudhary and D. Kumar, "Satellite solar wireless power transfer for baseload ground supply: clean energy for the future," *European Journal of Futures Research*, vol. 6, no. 1, p. 9, Jun. 2018.

[307] J. C. Lin, "Space solar-power stations, wireless power transmissions, and biological implications," *IEEE Microwave Magazine*, vol. 3, no. 1, pp. 36–42, Mar. 2002.

[308] R. Morsi, V. Jamali, A. Hagelauer, D. W. K. Ng, and R. Schober, "Conditional capacity and transmit signal design for SWIPT systems with multiple nonlinear energy harvesting receivers," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 582–601, Jan. 2020.

[309] T. D. Ponnimbaduge Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 264–302, Firstquarter 2018.

[310] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, Jun. 2015.

[311] D. Pires, D. Belo, M. Jordão, P. Pinho, and N. B. d. Carvalho, "3d antenna array for swipt sensing with wpt capabilities," in *14th European Conference on Antennas and Propagation (EuCAP)*, 2020, pp. 1–4.

[312] A. Cidronali, S. Maddio, G. Giorgetti, and G. Manes, "Analysis and performance of a smart antenna for 2.45-ghz single-anchor indoor positioning," *IEEE Transactions on Microwave Theory and Techniques*, vol. 58, no. 1, pp. 21–31, Jan. 2010.

[313] V. Marian, C. Menudier, M. Thevenot, C. Vollaire, J. Verdier, and B. Allard, "Efficient design of rectifying antennas for low power detection," in *2011 IEEE MTT-S International Microwave Symposium*, 2011, pp. 1–4.

[314] M. ur Rehman, W. Ahmad, and W. T. Khan, "Highly efficient dual band 2.45/5.85 ghz rectifier for rf energy harvesting applications in ism band," in *2017 IEEE Asia Pacific Microwave Conference (APMC)*, 2017, pp. 150–153.

[315] P. S. Yedavalli, T. Riihonen, X. Wang, and J. M. Rabaey, "Far-field rf wireless power transfer with blind adaptive beamforming for internet of things devices," *IEEE Access*, vol. 5, pp. 1743–1752, 2017.

[316] S. Gupta, S. Abielmona, and C. Caloz, "Microwave analog real-time spectrum analyzer (rtsa) based on the spectral–spatial decomposition property of leaky-wave structures," *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 12, pp. 2989–2999, 2009.

[317] M. K. Emara and S. Gupta, "Multi-port leaky-wave antennas as real-time analog spectral decomposers," in *14th European Conference on Antennas and Propagation (EuCAP)*, 2020, pp. 1–4.

[318] S. Gupta and C. Caloz, "Real-time 2-d spectral-decomposition using a leaky-wave antenna array with dispersive feeding network," in *2015 IEEE International Symposium on Antennas and Propagation USNC/URSI National Radio Science Meeting*, 2015, pp. 29–30.

[319] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, Apr. 2015.

[320] S. Ziegler, C. Crettaz, L. Ladid, S. Krco, B. Pokric, A. F. Skarmeta, A. Jara, W. Kastner, and M. Jung, "IoT6 – moving to an IPv6-based future IoT," in *The Future Internet*, A. Galis and A. Gavras, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 161–172.

[321] K. Dickerson, R. García-Castro, P. Kostelnik, and M. Paralič, "Standards for the IoT," in *IoT Platforms, Use Cases, Privacy, and Business Models: With Hands-on Examples Based on the VICINITY Platform*, C. Zivkovic, Y. Guan, and C. Grimm, Eds. Cham: Springer International Publishing, 2021, pp. 125–147.

[322] S. Patidar, D. Rane, and P. Jain, "A survey paper on cloud computing," in *Proc. 2012 Second International Conference on Advanced Computing Communication Technologies*, Jan. 2012, pp. 394–398.

[323] D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: A big picture," in *Proc. 2015 International Conference on Computational Intelligence and Networks*, Odisha, India, Jan. 2015, pp. 116–123.

[324] X. Zhang, R. Adhikari, M. Pipattanasomporn, M. Kuzlu, and S. Rahman, "Deploying iot devices to make buildings smart: Performance evaluation and deployment experience," in *Proc. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, VA, Dec. 2016, pp. 530–535.

[325] E. G. Petrakis, S. Sotiriadis, T. Soultanopoulos, P. T. Renta, R. Buyya, and N. Bessis, "Internet of things as a service (iTaaS): Challenges and solutions for management of sensor data on the cloud and the fog," *Internet of Things*, vol. 3-4, pp. 156 – 174, Oct. 2018.

[326] N. Ramohalli and T. Adegbija, "Modular electronics for broadening non-expert participation in STEM innovation: An IoT perspective," in *Proc. 2018 IEEE Integrated STEM Education Conference (ISEC)*, Princeton, NJ, Mar. 2018, pp. 167–174.

[327] A. P. Athreya and P. Tague, "Network self-organization in the internet of things," in *Proc. 2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*, New Orleans, LA, Jun. 2013, pp. 25–33.

[328] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, and R. Ande, "IoT standardisation: Challenges, perspectives and solution," in *Proceedings of the 2Nd International Conference on Future Networks and Distributed Systems*, Amman, Jordan, Jun. 2018, pp. 1:1–1:9.

[329] M. Alaa, A. Zaidan, B. Zaidan, M. Talal, and M. Kiah, "A review of smart home applications based on internet of things," *Journal of Network and Computer Applications*, vol. 97, pp. 48 – 65, Nov. 2017.

[330] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454 – 1464, Jan. 2017.

[331] S. H. Shah and I. Yaqoob, "A survey: Internet of things (IoT) technologies, applications and challenges," in *Proc. 2016 IEEE Smart Energy Grid Engineering (SEGE)*, Ontario, Canada, Aug. 2016, pp. 381–385.

[332] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "Iot-based smart cities: A survey," in *Proc. 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, Florence, Italy, Jun. 2016, pp. 1–6.

[333] Darshan K R and Anandakumar K R, "A comprehensive review on usage of Internet of Things (IoT) in healthcare system," in *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, 2015, pp. 132–136.

[334] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of internet of things in healthcare: a systematic literature review and classification," *Universal Access in the Information Society*, pp. 1–33, 2019.

[335] S. Nazir, Y. Ali, N. Ullah, and I. García-Magariño, "Internet of things for healthcare using effects of mobile computing: A systematic literature review," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[336] P. A. Laplante and N. Laplante, "The internet of things in healthcare: Potential applications and challenges," *IT Professional*, vol. 18, no. 3, pp. 2–4, May-June 2016.

[337] M. S. Mekala and P. Viswanathan, "A survey: Smart agriculture IoT with cloud computing," in *Proc. 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, Vellore, India, Aug. 2017, pp. 1–7.

[338] K. G. Liakos, P. Busato, D. Moshou, S. Pearson, and D. Bochtis, "Machine learning in agriculture: A review," *Sensors*, vol. 18, no. 8, Aug. 2018.

[339] M. H. Memon, W. Kumar, A. Memon, B. S. Chowdhry, M. Aamir, and P. Kumar, "Internet of things (IoT) enabled smart animal farm," in *Proc. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, Mar. 2016, pp. 2067–2072.

[340] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial internet of things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78 238–78 259, 2018.

[341] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, "The 5G-enabled tactile internet: Applications, requirements, and architecture," in *Proc. 2016 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Doha, Qatar, Apr. 2016, pp. 61–66.

[342] A. Aijaz, M. Dohler, A. H. Aghvami, V. Friderikos, and M. Frodigh, "Realizing the tactile internet: Haptic communications over next generation 5G cellular networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 82–89, Apr. 2017.

[343] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Network*, vol. 33, no. 4, pp. 70–75, July–August 2019.

[344] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[345] Myriota. (2019) Myriota product brief. Myriota. [Accessed: September 16, 2020]. [Online]. Available: https://myriota.com/wp-content/uploads/2019/04/Myriota-Product-Brief-Final.pdf

[346] M. Parr. (2019) IoT + geosatellites... a perfect match. Satnews. [Accessed: September 16, 2020]. [Online]. Available: http://www.satmagazine.com/story.php?number=1830210392

[347] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security and intelligence," *IEEE Wireless Communications*, p. Early Access, 2020.

[348] B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, and J. Wang, "6G technologies: Key drivers, core requirements, system architectures, and enabling technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 18–27, Sep. 2019.

[349] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electronics*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[350] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[351] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. C. Zhang, "Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 212–217, Apr. 2020.

[352] I. Tomkos, D. Klonidis, E. Pikasis, and S. Theodoridis, "Toward the 6G network era: Opportunities and challenges," *IT Professional*, vol. 22, no. 1, pp. 34–38, Jan.-Feb. 2020.

[353] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, 2020.

[354] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017.

[355] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[356] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2019.

[357] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[358] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, p. 102630, 2020.

[359] H. Ning, *Unit and ubiquitous internet of things*. CRC press, 2013.
[360] M. Youssef and M. Hassan, "Next generation IoT: Toward ubiquitous autonomous cost-efficient IoT devices," *IEEE Pervasive Computing*, vol. 18, no. 4, pp. 8–11, 2019.
[361] F. Alam, R. Mehmood, I. Katib, N. N. Albogami, and A. Albeshri, "Data fusion and IoT for smart ubiquitous environments: A survey," *IEEE Access*, vol. 5, pp. 9533–9554, 2017.
[362] H. E. Erdem and V. C. Gungor, "Analyzing lifetime of energy harvesting underwater wireless sensor nodes," *International Journal of Communication Systems*, vol. 33, no. 3, p. e4214, Nov. 2020.
[363] H. Erdem and V. Gungor, "On the lifetime analysis of energy harvesting sensor nodes in smart grid environments," *Ad Hoc Networks*, vol. 75-76, pp. 98 – 105, Jun. 2018.
[364] N. Shariati, J. R. Scott, D. Schreurs, and K. Ghorbani, "Multitone excitation analysis in RF energy harvesters–considerations and limitations," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2804–2816, Aug. 2018.
[365] S. Gupta and C. Caloz, "Dispersion and nonlinearity engineered metamaterial devices," in *Proc. Metamaterials*, Rome, Oct. 2007, pp. 627–630.
[366] ——, "Analog signal processing in transmission line metamaterial structures." *Radioengineering*, vol. 18, no. 2, Jun. 2009.
[367] C. Caloz, S. Gupta, B. Nikfal, and Q. Zhang, "Analog signal processing (asp) for high-speed microwave and millimeter-wave systems," in *2012 Asia Pacific Microwave Conference Proceedings*, 2012, pp. 691–692.
[368] Q. Zhang and F. H. P. Fitzek, "Mission critical IoT communication in 5G," in *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, V. Atanasovski and A. Leon-Garcia, Eds. Cham: Springer International Publishing, 2015, pp. 35–41.
[369] A. Sharma and M. Salim, "Polar code appropriateness for ultra-reliable and low-latency use cases of 5g systems," *International Journal of Networked and Distributed Computing*, vol. 7, no. 3, pp. 93–99, Jul. 2019.
[370] A. Roy and R. Roy, "Reliability benefit of network coding and cooperative communication," *Physical Communication*, vol. 29, pp. 217 – 229, 2018.
[371] J. Park, S. Samarakoon, M. Bennis, and M. Debbah, "Wireless network intelligence at the edge," *Proceedings of the IEEE*, vol. 107, no. 11, pp. 2204–2239, 2019.
[372] L. Zhang, Y. Liang, and D. Niyato, "6G visions: Mobile ultra-broadband, super internet-of-things, and artificial intelligence," *China Communications*, vol. 16, no. 8, pp. 1–14, Aug. 2019.

IAN ZHOU (S'20) received the B.S. degree in computer science from the University of Sydney, Australia, in 2016. He also received the MBA degree from the University of Technology Sydney in 2019. His research interest includes AI, IoT, cyber-physical system, and blockchain. Currently, he is pursuing a Ph.D. degree at the University of Technology Sydney researching on machine learning-based frost monitoring systems.

IMRAN MAKHDOOM (S'18–M'21) is a postdoc researcher at the University of Technology Sydney. He completed his Ph.D. from the University of Technology Sydney in 2020. His research interests include blockchain, the Internet of Things, distributed consensus, network, and computer security. Imran has published numerous papers in some of the prestigious journals and conferences. He has also been a Food Agility Scholar from 2019-2020 and has made a valuable contribution to data security and privacy in the Food Tech/Agri Tech. Before this, he secured a masters degree in information security from the National University of Sciences and Technology, Pakistan, in 2015.

NEGIN SHARIATI is a Senior Lecturer in the School of Electrical and Data Engineering, Faculty of Engineering and IT, University of Technology Sydney (UTS), Australia. She established the state of the art RF and Communication Technologies (RFCT) research laboratory at UTS in 2018, where she is currently the Deputy Director and leads research and development in RF-Electronics, Sustainable Sensing, Low-power Internet of Things, and Energy Harvesting. She also is the Sensing Innovations Constellation Leader at Food Agility CRC (Corporative Research Centre). Since 2018, she has held a joint appointment as a Senior Lecturer at Hokkaido University, externally engaging with research and teaching activities in Japan.

She completed her PhD in Electrical-Electronic and Communication Technologies at Royal Melbourne Institute of Technology (RMIT), Australia, in 2016. She worked in industry as an Electrical-Electronic Engineer from 2009-2012. Her research interests are in Microwave Circuits and Systems, RF Energy Harvesting, low-power IoT, Simultaneous Wireless Information and Power Transfer, AgTech, and Renewable Energy Systems.

MUHAMMAD AHMAD RAZA received the Bachelor of Science (Telecommunication Engineering) and the Master of Science (Electrical Engineering) degrees from the National University of Computer and Emerging Sciences, Lahore, Pakistan, in 2008 and 2013, respectively. Currently, he is doing PhD with the Faculty of Engineering and Information Technology at the University of Technology Sydney, NSW, Australia. His research interests include adaptive networking, wireless and mobile communications, and signals estimation and detection theory.

RASOOL KESHAVARZ was born in Shiraz, Iran in 1986. He received the B.Sc. degree in Electrical Engineering from the University of Shiraz, Shiraz, Iran, in 2008, the M.Sc. degree in Telecommunications Engineering from Shahid Bahonar University of Kerman, Kerman, Iran, in 2011, and Ph.D. degree in Telecommunications Engineering from the Amirkabir University of Technology, Tehran, Iran in 2017. He is currently working toward an Honorary Appointment position as Visiting Fellow in RFCT Lab at the University of Technology, Sydney, Australia. His main research interests are RF and microwave circuit and system design, antenna design, agriculture sensors, biomedical sensors, wireless power transfer (WPT), and RF energy harvesting (EH).

JUSTIN LIPMAN (S'94–M'04–SM'12) is an Industry Associate Professor at the University of Technology Sydney and Director of the RF Communications Technologies (RFCT) Lab, where he leads industry engagement and research in RF technologies, Internet of Things, Tactile Internet and Software Defined Communication. He serves as a committee member in Standards Australia contributing to International IoT standards and is the Deputy Chief Scientist and Research Program Lead for the Food Agility Cooperative Research Centre. Since 2018, he has held a visiting appointment as an Associate Professor at Hokkaido University's Graduate School of Engineering. He received his PhD Telecommunications and BE Computer Engineering from the University of Wollongong, Australia in 2003 and 1999 respectively. From 2004 to 2017, Dr. Lipman was based in Shanghai, China and held a number of senior management and technical leadership roles at Intel and Alcatel leading research and innovation, product architecture and IP generation. He is an IEEE Senior Member. His research interests are in all "things" adaptive, connected, distributed and ubiquitous.

MEHRAN ABOLHASAN (S'01–M'03–SM'11) is an Associate Professor and Deputy head of School for Research in School of Electrical and Data Engineering, University of Technology Sydney. A/Prof. Abolhasan has over 20 years of experience in R&D and serving in research leadership roles. Some of these previous roles includes: serving as the Director of Research programs for the Faculty of Engineering and IT and Lab Director for Telecommunication and IT Research Institute at University of Wollongong. He has authored over 140 international publications and has won over four million dollars in research funding. He won a number of major research project grants including ARC Discovery Project and a number of CRC and other government and industry-based grants. His Current research Interests are in Software Defined Networking, IoT, Wireless Mesh, Wireless Body Area Networks, Cooperative Networks, 5G Networks and Beyond and Sensor networks.

ABBAS JAMALIPOUR received the Ph.D. degree in electrical engineering from Nagoya University. He is currently a Professor of ubiquitous mobile networking with The University of Sydney. He is also the President of the IEEE Vehicular Technology Society. He has authored nine technical books, eleven book chapters, over 550 technical articles, and five patents, all in the area of wireless communications. He is a Fellow of the Institute of Electrical, Information, and Communication Engineers (IEICE) and the Institution of Engineers Australia, an ACM Professional Member, and an IEEE Distinguished Speaker. Since 2014, he has been an Elected Member of the Board of Governors of the IEEE Vehicular Technology Society. He was a recipient of a number of prestigious awards, such as the 2019 IEEE ComSoc Distinguished Technical Achievement Award in Green Communications, the 2016 IEEE ComSoc Distinguished Technical Achievement Award in Communications Switching and Routing, the 2010 IEEE ComSoc Harold Sobol Award, the 2006 IEEE ComSoc Best Tutorial Paper Award, as well as 15 Best Paper Awards. He has been a General Chair or Technical Program Chair for a number of conferences, including the IEEE ICC, GLOBECOM, WCNC, and PIMRC. He was an Executive Vice-President and the Editor-in-Chief of VTS Mobile World. He was the Editor-in-Chief of the IEEE Wireless Communications, Vice President-Conferences, and a member of Board of Governors of the IEEE Communications Society. He serves as an Editor for IEEE Access, the IEEE Transactions on Vehicular Technology, and several other journals.