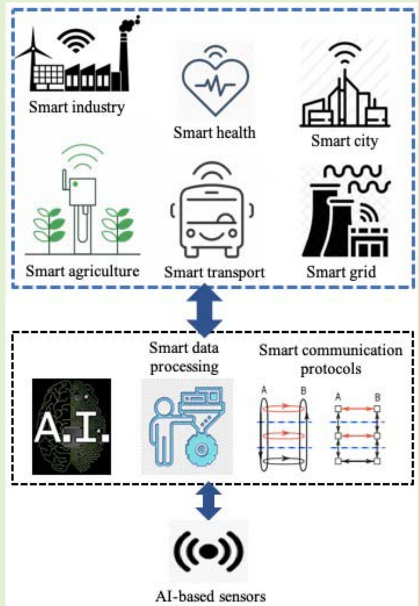
Artificial Intelligence-Based Sensors for Next Generation IoT Applications: A Review

Subhas Chandra Mukhopadhyay, *Fellow, IEEE*, Sumarga Kumar Sah Tyagi, *Member, IEEE*, Nagender Kumar Suryadevara, *Senior Member, IEEE*, Vincenzo Piuri, *Fellow, IEEE*, Fabio Scotti, *Senior Member, IEEE*, and Sherali Zeadally, *Senior Member, IEEE*

***Abstract*—Sensors play a vital role in our daily lives and are an essential component for Internet of Things (IoT) based systems as they enable the IoT to collect data to take smart and intelligent decisions. Recent advances in IoT systems, applications, and technologies, including industrial Cyber-Physical Systems (CPSs), are being supported by a wide range of different types of sensors based on artificial intelligence (AI). These smart AI-based sensors are typically characterized by onboard intelligence and have the ability to communicate collaboratively or through the Internet. To achieve the high level of automation required in today's smart IoT applications, sensors incorporated into nodes must be efficient, intelligent, context-aware, reliable, accurate, and connected. Such sensors must also be robust, safety- and privacy-aware for users interacting with them. Sensors leveraging advanced AI technologies, new capabilities have recently emerged which have the potential to detect, identify, and avoid performance degradation and discover new patterns. Along with knowledge from complex sensor datasets, they can promote product innovation, improve operation level, and open up novel business models. We review sensors, smart data processing, communication protocol, and artificial intelligence which will enable the deployment of AI-based sensors for next-generation IoT applications.**



AI-based sensors used for various IoT applications.

***Index Terms*— Artificial intelligence, Internet of Things, sensors, smart sensors, wireless sensor networks, network, protocol.**

I. Introduction

A SENSOR is a device that responds to a physical stimulus (such as heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse (such as for measurement or operating a control system). Sensors are used in almost every system today. They are in our homes and workplaces, shopping centers, hospitals, and are embedded in smartphones. Sensors have become an integral part of the Internet of Things (IoT) ecosystem. According to Lord Kevin, "If you cannot measure it, you cannot improve it". The sensor is a fundamental element for measuring any parameters of interest. The IoT and its counterpart, the Industrial Internet of Things (IIoT), bring sensor usage to a new level.

Background: Sensors are crucial to the operation of many businesses today. They are instrumental in warning us of any potential problems which could affect operations, allowing businesses to perform predictive maintenance and avoid costly downtime. The emergence of big data analytics technology is enabling sensors' data to be analyzed to detect trends that may allow business owners to gain insight into crucial trends and ultimately help them to make informed, evidence-based decisions.

There are many types of sensors used in diverse IoT applications and these types of sensors are referred to as IoT sensors. These IoT sensors have become critical in improving operational efficiency, reducing the cost of production, enhanc-

Manuscript received December 22, 2020; accepted January 24, 2021. Date of publication January 29, 2021; date of current version November 12, 2021. The associate editor coordinating the review of this article and approving it for publication was Dr. Qammer H. Abbasi.
(Corresponding author: Sumarga Kumar Sah Tyagi.)

Subhas Chandra Mukhopadhyay is with Macquarie University, Sydney, NSW, Australia (e-mail: subhas.mukhopadhyay@mq.edu.au).

Sumarga Kumar Sah Tyagi is with the Zhongyuan University of Technology, Zhengzhou, China (e-mail: sumarga@zut.edu.cn).

Nagender Kumar Suryadevara is with the University of Hyderabad, Hyderabad, India (e-mail: nks@uohyd.ac.in).

Vincenzo Piuri and Fabio Scotti are with the Università degli Studi di Milano, Milan, Italy (e-mail: vincenzo.piuri@unimi.it; fabio.scotti@unimi.it).

Sherali Zeadally is with the University of Kentucky, Lexington, KY 40506 USA (e-mail: szeadally@uky.edu).
Digital Object Identifier 10.1109/JSEN.2021.3055618

ing workers' safety, providing early warning to prevent system breakdown, and so on. Advancements in (1) electronic technology [23], (2) biology/healthcare [17], [20], [34], and (3) data/machine learning can provide insights into personalized healthcare and potentially improve the quality of life.

Motivation: New technologies and advances in heterogeneous integration tools, materials, and processes that provide differentiating electronics for future healthcare diagnostic tools and sensors have been described in [1], [16]. The authors of [2] described a system which takes in depersonalized data collected by a patient medication management system, carries out reformatting and necessary calculations on the data, stores the resulting information into a database for retrieval, visualization, and further analysis. The authors of [11], [14], [48] described a practical implementation for Internet of Things that uses low-cost ubiquitous sensing systems which monitor regular domestic conditions such as energy usage and occupancy of homes. In [46], the authors developed a system that uses AI to predict attendance of students and performs optimal allocation of rooms to courses to minimize space wastage [46].

In [12], the authors proposed a sensor-based system that monitors (in real-time) complex behavioral changes in daily activities for reliable wellness operations' measurements. The sensor status of household objects used for the elderly, combined with the time-series data processing algorithm's prediction process, was presented in [19]. New sensor technologies are being applied to achieve targeted healthcare diagnostics with cost-effectiveness [1]. Data streams can leverage AI to provide smart, personalized healthcare guidance or solutions that complement existing technology and data to healthcare professionals, patients, and clients.

Challenges: Trust, reliability, and data validation of data collected in distributed edge sensor systems are becoming an increasingly relevant issue. Given the need for dependable autonomy and reliability in IoT systems, in [3], the authors present a sensor validation method to increase robustness, resilience, and dependability of sensed data by detecting false positives and negatives using sensory substitution. Sometimes, sensor data is trusted without ongoing validation. With the rise of cyber-physical attacks on cloud, fog, and edge computing systems, validation of sensor data becomes increasingly important.

In [8], [15], the authors propose an enhanced architecture and implementation for 128-bit Schmidt-Samoa cryptosystem (SSC) to protect the data communication for wireless sensor networks (WSN) against external attacks. The security features of integrity in smart vehicles were identified and discussed, emphasizing the potential impact of integrity on future vehicular applications [9].

Failures of sensors and actuators are not uncommon in many applications but detection of failures or even prevention at an early stage is sometimes challenging. In [4], [21], the authors propose a low computational cost method for detecting actuator/sensor faults. A typical model-based Fault Detection (FD) unit for multiple sensor faults requires a bank of estimators (i.e., conventional Kalman estimators or Artificial Intelligence (AI)-based ones). The proposed FD scheme reported in [4] has used an AI approach to develop a low computational power FD unit (abbreviated as IFD). In contrast to the bank-of-estimators approach, the proposed IFD unit employs a single estimator for multiple actuators/sensors FD. The efficacy of the proposed FD scheme has been illustrated through a rigorous analysis of the results for several sensor fault scenarios on an electromagnetic suspension system. Optimization of network resource utilization and to protect the network against failures has been discussed in [50].

LoRa integrated with AI learning models for IoT servers and clouds could serve intelligent tasks in the home environment. The authors of [5] have proposed a dataflow design for the LoRa-based home monitoring using AI. A multi-purpose integrated sensor-based system which consists of networked sensors for different purposes, and applications have been described in [6], [18]. The sensors can be health sensors to measure patients' pulse and blood pressure [36], or the sensors can measure the temperature to indicate a fire accident [31]. The networked sensors transfer the sensed data through wireless technologies to a cloud for processing and notify the listed users to take an appropriate action [42], [44]. Coverage, discovery, connection times, and mobility in the deployment of a sensor node in a smart city environment has been discussed in [7]. The authors of [7] have proposed an automated fire alert detection system which comprises smoke sensors and fire sensors [10]. These sensors detect the change in a measurable physical quantity such as sudden high temperature and help to detect a forest fire.

Objective: IoT enables device-to-device communications due to limited energy capabilities which present a significant challenge [47]. The design and development of low-energy electronics [45] and energy harvesting devices are of tremendous importance [49]. An energy-efficient routing protocol based on AI techniques such as particle swarm optimization and genetic algorithm, for large scale I-IoT networks for SDN and cloud architectures has been reported in [40], [50]. 5G Intelligent Internet of Things (5G I-IoT) architectures are under development to process big data intelligently and optimize communication channels, including big data mining, deep learning, reinforcement learning [41] and novel techniques such as cloudlet-based cyber foraging (i.e., edge/fog computing) [43], [139].

A new computation paradigm for wireless sensor networks, the sensor cloud, which decouples the network owner and the user and allows multiple WSNs to interoperate simultaneously for a single or multiple applications transparent to the users, has been discussed in [13]. A sensor cloud is a heterogeneous computing environment spread in a wide geographical area that brings together multiple WSNs consisting of different sensors [35]. Each WSN can have a different owner [39]. The sensor cloud then virtualizes the wireless sensors and provides sensing as a service to users [32]. Since users buy sensing services on demand from the sensor cloud, use of large-scale sensor networks becomes affordable with ease [22], [38].

Contribution: AI-based sensors significantly empower new architectures in IoT and IoT-like applications, wherein local intelligence and distributed data disclosure cycles replace centralized control and data processing. The design and development of AI-based sensing systems, the intricacies of

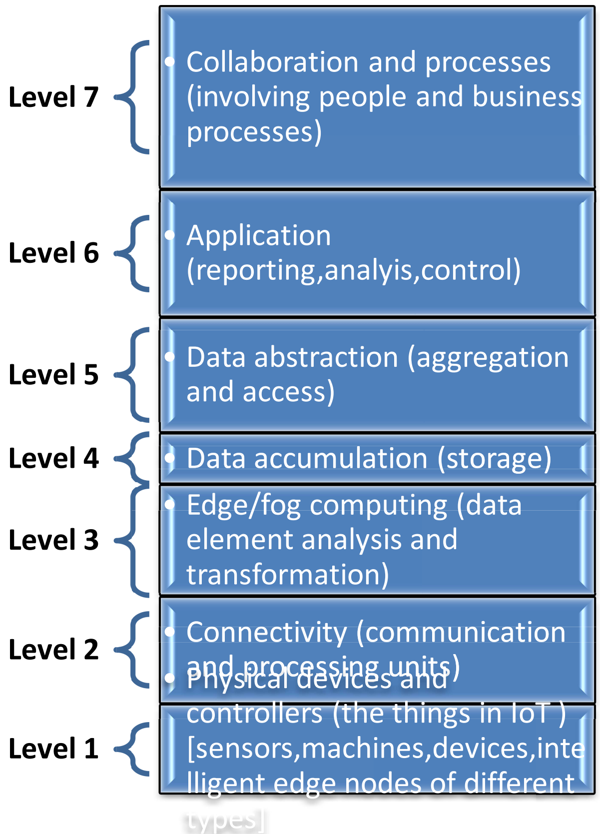


Fig. 1. Conceptual framework as reference model of an IoT system proposed by CISCO [117].

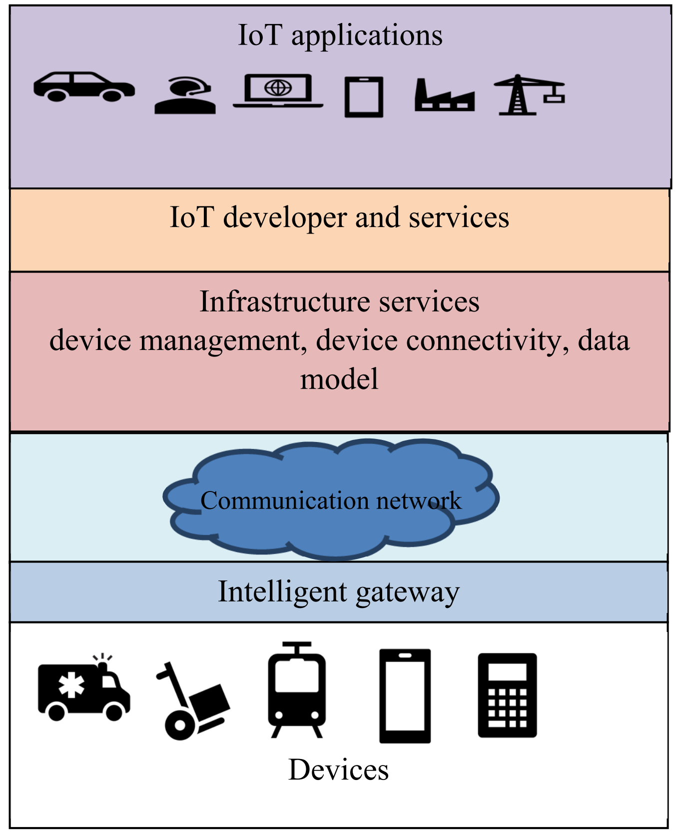


Fig. 2. IoT architecture as proposed by Oracle [121].

embedding AI techniques can be best achieved through a better understanding of the role of embedded smart sensing systems in Industry 4.0, IoT architectures and technologies.

The rest of this paper is organized as follows. Section 1 presents the latest technological developments on the integration of AI and IoT in embedded smart sensing systems in Industry 4.0. Section 2 describes various IoT architectures proposed by various organizations and scientific bodies. Section 3 presents a comprehensive review of the types of sensor data processing at the edge/fog and cloud computing levels. Section 4 describes the framework for the communication technologies that support the AI-IoT enabled smart data communications. Section 5 describes the motivations behind enabling intelligence for the sensors in the IoT environment. Section 6 highlights the significance of AI in IoT applications. Section 7 discusses open issues and key innovative solutions. Finally, section 8 concludes the paper.

II. IoT Architecture

Various IoT architectures have been defined each with the required system functionalities based on the problem being addressed. In general, different scientific organizations have proposed IoT architectures based on hierarchical layers for specific application domains [118]–[122].

These layers are also known as "tiers". A reference model can be considered to show various functional blocks, interactions and integration. CISCO's representation of a reference model consists of seven layers [117] as Figure 1 shows.

Fig.2 depicts the IoT architecture proposed by Oracle [121]. The architectural design has the following characteristics:

- The design fills in as a kind of perspective in IoT in administrations and business measures.
- Smart sensors collect the information, analyze vital components, change it according to the gadget's application system, and interface it directly to a communication device.
- A set of sensor circuits is associated with an entryway having separate information.
- The communication gateway sub-framework comprises of convention overseers, switches, and message reserve.
- The executive's sub-framework has functionalities for supporting the gadget's character information base, characteristics, and access to the board.
- Data travels securely from the entryway through the web and server farm to the application worker or venture worker.
- Organization and examination sub frameworks empower the administrations, business measures, venture joining, and complex cycle.

Various models have been proposed at SWG during Dec 2014, through online mode. The principles for a compositional system for the IoT have been created under IEEE standards architectural P2413 [120]. IEEE SA recommended P2413 standard for the design of IoT. Its design is built upon the reference model, as Fig. 3 shows. The reference architecture describes the meaning of essential compositional structure blocks and their ability to support a multi-tiered framework.

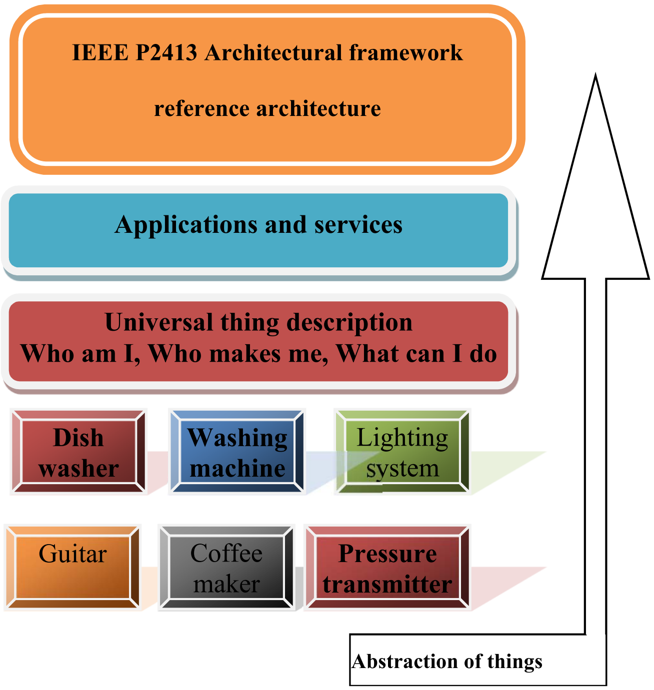


Fig. 3. Abstraction of "Things" proposed by IEEE P2413.

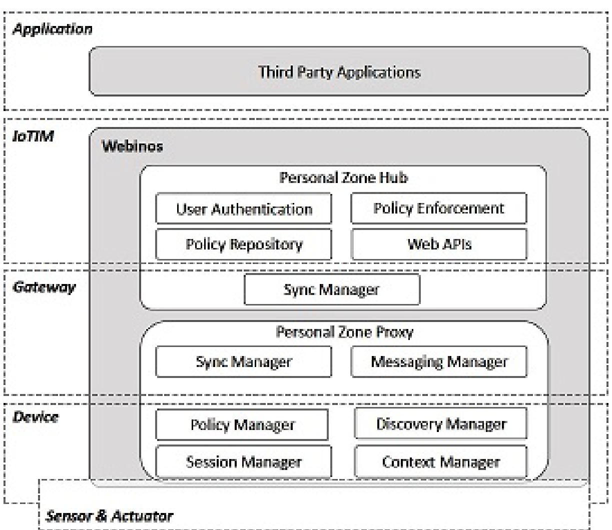


Fig. 4. Webinos IoT Architecture for smart things [123].

The IEEE P4213 standard [120], developed by the IEEE P2413 IoT working group, describes a reference architecture for IoT as shown in Figure 3. The reference architecture describes the basic building blocks of a multi-tiered framework that abstracts "Things" using a top down approach. This blueprint covers different functional areas of the IoT domain and recommends quality 'quadruple' belief that incorporates assurance, security, protection, and well-being.

Fig. 3 depicts the "Things" levels of abstraction as proposed by the IEEE P2413 [120].

Webinos [123], which is an IoT architecture for smart things that focuses on empowering web applications deployed on Personal Computers (PCs), in-vehicle units, and home media. Fig. 4 depicts the Webinos IoT architecture that supports both IoT and Machine to Machine (M2M) applications.

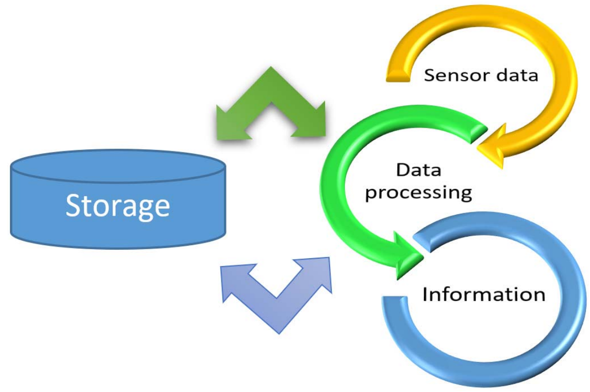


Fig. 5. Sensor data processing cyclic process.

Specifically, Webinos provides explicit API support to enable the development of applications that use sensors and actuators in the client's space. Most IoT architectures proposed in the literature [124]–[127] address heterogeneity issues.

III. Sensors Data Processing for IoT

Data collected from sensors (including IoT sensors) needs to be processed and analyzed in order to make timely, intelligent decisions [77]. Sensors data processing for IoT is viewed as the assortment and control of things to generate vital information [78], [79]. Meaningful information is extracted from the raw data and this information is then presented to the end entity (user or machine) so that the latter can provide the appropriate response. The procedure to convert raw data into meaningful information to generate smarter decisions follows a cyclic process comprising three phases: input, processing, and output [80]. Fig. 5 depicts the cyclic process of sensors data processing. Input is the principal phase of the data processing cyclic process. In this phase, sensors' fusion data is changed into a machine-comprehensible structure so that a machine can process it. In the processing phase, a program running on the machine transforms the raw data into information by following various data manipulation methods depending on the application requirements. AI data manipulation methods for information processing include classification, calculation, and sorting techniques. The next phase is the output wherein the data is changed over into a comprehensible structure and introduced to the end-user or machine as valuable data [80], [81].

A. Sensor Data Processing Levels for Various IoT Application Domains

Some IoT application domains, such as real-time applications, demand low latency, and high data transfer rates. Hence, sensor data processing can be performed at two different levels depending on the application requirements:1) near to the sensor data origin (node level) or 2) at the cloud level. Further, node-level sensor data processing is categorized into a) Edge computing, and b) Fog computing.

1) Data Processing at/Near the Sensor Node:

a) Edge Computing: The edge computing permits the data to be handled close to its cause (the sensor devices/gadgets).

The information is moved from sensor gadgets to a neighborhood edge computing framework, which procedures, stores the information, and processes the data locally. Additionally, the framework could assemble the handled information and send it to the Cloud at regular intervals of time. The beneficial thing about edge processing is that only the significant data is sent over the network. This requires less data transmission from the sensor system and spares the sensor batteries. Likewise, the information can be processed faster when done close to the sensor gadget [82], [83].

b) Fog Computing: Fog Computing, otherwise called fogging, is engineering that utilizes edge gadgets (sensor devices) to complete a considerable measure of calculation, storage, and communication locally before being transmitted over the web [84]. In 2014, the need to expand distributed computing with fog computing rose, and the idea was given by Cisco. Fog computing includes carrying knowledge to the local network of computing devices and processes the data in a fog node. As indicated by Cisco, fog computing is a standard that characterizes how edge computing should work, and it empowers the activity of process, storage, and systems administration between end gadgets/devices and distributed computing systems [85], [86]. Fog computing underpins the IoT idea, in which a large portion of the devices utilized by people consistently will be associated with one another. Models incorporate telephones, wearable well-being checking gadgets, associated vehicles, and wearable devices (e.g., Google Glass). IEEE received the Fog Computing norms proposed by OpenFog Consortium for standardization [87].

2) Sensor Data Processing at the Cloud: Numerous IoT frameworks utilize vast sensors to gather information and make smart decisions [88]. Utilizing the cloud, is significant for data aggregation, subsequently inferring intelligent decisions from the information. For example, an agribusiness organization would have the option to look at soil moisture from the sensors located at different places after planting similar seeds. Without the Cloud, looking at information across more extensive zones is substantially more troublesome.

Utilizing the cloud computing features for IoT takes into account high versatility. When a massive number of sensors is utilized, putting a high computational burden on every sensor would be very costly. Instead, information can be passed to the Cloud from every sensor and prepared there in total [89], [90]. For quite a bit of IoT, sensors and gadgets gather information and perform activities, yet the handling/ordering/investigation ordinarily occurs in the Cloud. Sensor data is continuously streamed to the Cloud. IoT applications that do not concern much on the latency and bandwidth do prefer cloud computing scenario.

AI for sensors is getting simpler than any time in the recent past: equipment costs are decreasing, and sensors are getting less expensive, making IoT gadgets broadly accessible for an assortment of utilizations running for smarter decisions. Fig.6 depicts the generic sensor data processing at various levels.

IV. Communication Protocols in IoT

The IoT ecosystem is a highly heterogeneous environment with a mix of devices running various types of communication protocols and using different types of communication models. Tschofenig *et al.* [91], [95] defined four communication models: device to device, device to the cloud, device to the gateway, and back-end data sharing. In device-to-device communications, protocol design issues that address interoperability need to be investigated and innovative solutions developed.

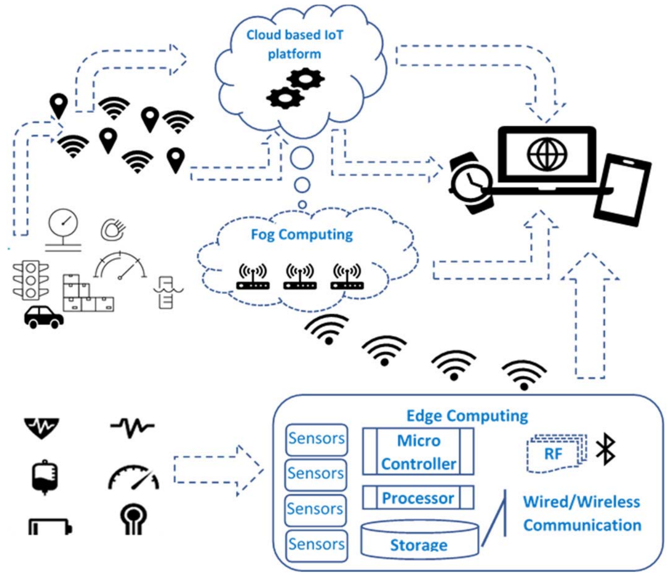


Fig. 6. Sensor data processing levels node (Edge/Fog), Cloud level.

From the device to cloud communications (e.g., interactions between a humidity sensor and an application service provider wherein sensor data may be uploaded to an application service provider), interoperability is much less of an issue. This is because the most of the communications occur within the provider [91]. In the device to gateway communication architecture, communications between two IoT devices (e.g., one equipped with a temperature sensor and the other equipped with a humidity sensor) take place through an Internet-connected gateway (which can be a generic one or a specific type that translates application-layer protocols) that connects them.

In the case of back-end data sharing, an application service provider shares its sensor data (e.g., data from a temperature sensor) with other application service providers. Figure 7 presents some of the most popular protocols and communication standards that are being deployed at the various layers of the communication stack in the IoT environment today. It is worth pointing out that many of these protocols have been specifically designed to be lightweight in terms of their usage of resources (processing power, memory, bandwidth, and so on) mainly because they are expected to work in environments with a high number of resource-constrained devices and networks. Although the lightweight characteristic of many of these IoT communication protocols help to achieve an energy-efficient IoT ecosystem, the security and privacy of the data exchanged among IoT devices are becoming increasingly important [83], [92], [94].

To improve security, several enhancements have been proposed in the literature to several application layer protocols shown in Figure 7. Some of the security protocols

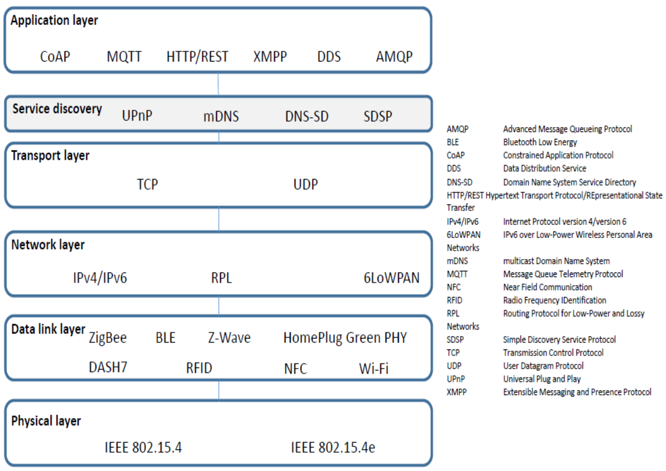


Fig. 7. Popular communication protocols used in Internet of Things [Adapted from [91], [93]].

and techniques used include: Secure Sockets Layer/Transport Layer Security (SSL/TLS), Datagram Transport Layer Security (DTLS), Blockchain, Elliptic Curve Cryptography (ECC), and so on. However, it remains a significant challenge for IoT researchers to develop robust, reliable, scalable optimized solutions that can achieve optimal trade-offs for lightweight operations and communications, energy-efficiency, security and privacy in the IoT environment.

V. AI - A Brief Introduction and the Need for a Smart Sensor

Artificial intelligence (AI) envelops different advancements including Machine Learning, Deep Learning, and Natural Language Processing. We expect that AI procedures and strategies will continue to be integrated into a few IoT compositional layers paving the way for the development of Artificial Intelligence of Things (AIoT) applications. Current AI is being used in IoT environments mostly for: i) boosting operational effciciency. For example, Google brings the power of AI into IoT to reduce its data center cooling costs, ii) providing better risks management (for example, Fujitsu ensures worker safety by using AI for analyzing data sourced from connected wearable devices), iii) triggering new and enhanced products/services (e.g., Rolls Royce leverages AI techniques in the implementation of IoT-enabled airplane engine maintenance amenities), and iv) increasing the scalability of IoT. In the future, we expect AI to be used for designing data reduction approaches for AIoT on embedded edge node, and mimicking human-like personality in designing smart-objects [129]–[131]. AI can be applied to IoT to enhance security, and protect resources, and lessen vulnerabilities. Thus, AI will be utilized to make self-governing activities.

The mix of AI-based techniques at various IoT compositional layers to deal with IoT information for self-management tasks improves the designs of interconnected IoT systems. Innovations (AI, bots, mechanization, AR/VR) make intelligent decisions through combined IoT knowledge thereby expanding human capabilities and increasing abilities of machines/things to better handle and manage the edge/fog computing areas [132]–[134].

A smart sensor is an AI thing of what is known as a sense in science. With a smart sensor, a machine monitors the environment and data can be gathered. A sensor quantifies a physical amount and converts it into a sign. Sensors interpret estimations from this present reality into information for the computerized area. A practically unbounded variety of boundaries can be estimated. Examples include area, uprooting, development, sound recurrence, temperature, pressure, dampness, electrical voltage level, camera pictures, shading, synthetic creation, and so on. The objective is to identify functions or changes in the environment.

Different sensors are commonly used in different gadgets. Advances in chip designs and implementation makes it possible to develop small, cost-effective, and energy-efficient sensors. The quantity of sensors around us is expanding quickly and as IoT grows further in coming years, the number and types of sensors that will be deployed in the IoT environment will continue to rise.

A smart sensor alludes to the incredible significance of completing estimations to make concrete and verifiable data accessible. Measurement (estimation) of data through smart sensors is very much needed. Estimating gives an understanding of things that work out in the right way.

The gadgets, which together structure the IoT, are equipped with sensors. With these sensors, the gadgets gather information about how they are utilized and their environment. The gathered information can be as straightforward as estimating the temperature or as unpredictable as a total video feed. In addition, consider sensor information as area, sound or stickiness, and various estimations of machines or our bodies. These gadgets have an implicit (remote) network to be associated with the Internet and can trade information. Billions of associated gadgets are essential for IoT.

IoT gadgets produce a large amount of data (big data) [135]–[139]. IoT makes data collected from a wide range of different gadgets and sensor types easier to analyze and detect specific information of interest or trends.

The desire is that IoT can offer answers for significant social issues identifying with energy and the environment. After some time, utilizing IoT, for instance, we will utilize less energy, squander fewer items and go through less cost. The individuals who realize how to utilize such data can function considerably more effectively.

Big data from the IoT sensors:

IoT is growing exponentially: there is an ever-increasing number of gadgets that gather, store, and communicate information. The amount of information being generated is also rising rapidly resulting in big data sets that makes it difficult to store on common information base administration frameworks.

Increasingly more, we hear that big data portrays a turn of events. It contains two parts. Above all else, PC innovation: the inexorably complex equipment and programming that makes it conceivable to gather, cycle, and store more information. The next part is the analysis part that makes it conceivable to discover significant information in an assortment of isolated information. Big data analysis in this definition refers to our

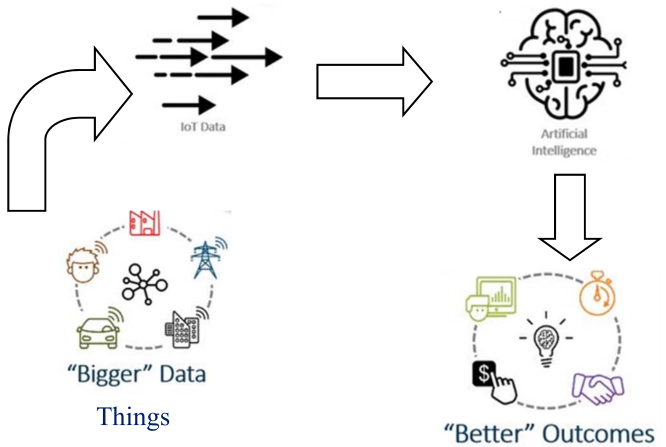


Fig. 8. "Things" enabled AI in the IoT theme will result into "Smart Things" for better outcomes.

likelihood in examining and utilizing the increasing amount of data being produced by the IoT systems and devices.

Smart things: The additional estimation of big data: To utilize the vast amount of information, efficient AI investigation of the information is essential. Enormous Data investigation is the way toward exploring Big Data – to find smart designs, discreet relationships, market patterns, client inclinations, and other valuable data – to settle on more educated choices. The upside of information investigation is that choices can be founded on information picked up from realities and subsequently turn out to be less reliant on instinct and abstract encounters.

IoT gadgets, in some cases, run on their own installed programming or firmware. However, they can likewise utilize the Cloud for further analysis of the information. When the information arrives at the Cloud, the product measures the information. This can be straightforward, for example, checking whether the temperature esteem is within an adequate reach. Alternatively, then again unpredictable, for example, the utilization of PC vision on record to distinguish objects, (for example, interlopers in our home).

It is commonly acknowledged that IoT and AI are essential to one another's future. Simulated intelligence will make IoT practical on a scale, and through AIoT, the lives of a great many people will be impacted day by day. The AioT potential for profoundly individualized administrations is unending and will radically change how individuals live. Fig. 8 depicts augmenting AI with the "Things" so that smart sensing can enable better outcomes for humanity's benefit.

VI. AI in IoT Applications

Artificial intelligence techniques are enabling technologies for hundreds of different applications in a wide range of IoT scenarios. AI are used for consumer and industrial IoT, industry 4.0, smart cities, smart buildings, smart homes, smart transportations, healthcare, environmental monitoring, agriculture and smart grids. In particular, AI has been shown to be effective in many aspects by supporting application design and implementation, as well as infrastructure and application management.

AI techniques are mainly applied to analyze server-side data collected from IoT sensors, but the increasing availability of computational resources in IoT devices frequently allow to locally process multidimensional signals using AI-based methods. The research community is particularly active in designing novel AI paradigms optimized for devices used in most of the IoT applications [96]. The main AI technologies currently adopted in IoT applications are artificial neural networks (e.g., feed-forward networks and deep learning techniques), fuzzy logic and evolutionary computation, which are applied for heterogeneous purposes, such as: regression, classification, multidimensional signal processing, sensor calibration, measurement, data fusion, prediction, decision support, security, and data transmission.

Nowadays, IoT applications are generating paramount quantities of data. Consequently, it is important to design and apply robust AI techniques for preprocessing and preparing data by reducing the amount of noise, decreasing their dimensionality, and removing possible redundancies [97]. Furthermore, it is frequently needed to design and apply AI methods able to deal with unstructured input samples [98].

In some cases, it is not possible to adopt AI methods based on supervised learning techniques since it is not possible to obtain a sufficient amount of manually labeled data collected from IoT devices. Hence unsupervised (or semi-supervised) AI techniques capable of creating or tuning models without output or ground truth information play a relevant role in IoT AI-based applications [99].

In the IoT context, application environments can evolve after the deployment and it is also possible to take advantage of the data obtained during time to automatically update the knowledge base of AI-based methods by using reinforcement learning strategies [100].

Every IoT application uses specific communication technologies and can adopt strategies for privacy and security protection. AI techniques play an important role also for these aspects of IoT. Considering the communication technologies, a great number of IoT applications is based on compact, mobile, and energy-constrained devices. In these cases, traditional approaches used to optimize the communication procedures may not be suitable because it could not be possible to know in advance the model of the environment. Furthermore, traditional optimization approaches may require an excessive amount of computational resources for the specific IoT device. Therefore, AI techniques are frequently used to perform fast and accurate optimizations in IoT applications For example, deep capsule neural networks can solve energy optimization problems [101] and evolutionary algorithms can also obtain accurate results for offline optimizations of network settings [102].

Considering strategies for privacy and security protection, AI techniques permit the automatic learning of discriminative patterns of possible malicious actions from the communication streams. Taking advantage of their learning capabilities, different deep learning strategies and artificial neural networks are frequently used to realize intrusion detection systems and methods to detect malicious attacks [103].

In the following, some specific applications in different scenarios where the AI techniques gave a relevant contribution to the solution are reviewed. In smart environments like in smart buildings, smart homes and smart cities, the IoT paradigm realizes a communication network between measurement sensors, embedded devices, and human-computer interfaces. In these environments, AI can be considered as a new enabling technology for processing the acquired data and taking decisions automatically. Within this context, AI is widely applied for heterogeneous applications, encompassing local processing of sensor data by monitoring, forecasting, and extracting information from the collected data [104].

Furthermore, applications include human-machine interaction based on voice signals or videos, and methods to analyze the actions of the people interacting with the environment. Considering the wide amount of information obtainable from the environment and the intrinsic complexity of processing acoustic signals and videos, many recent AI-based applications adopt deep learning techniques. As an example, commercial systems from different companies use artificial neural networks to manage illumination systems of smart buildings. Moreover, in smart homes, the use of vocal assistants, based on deep learning strategies, is constantly growing. Artificial neural networks are also used to monitor and manage critical infrastructures, such as pipelines and overhead power lines. Other methods for the analysis of IoT data acquired in smart environments different than artificial neural networks are mainly based on fuzzy logic and evolutionary algorithms.

In smart transportations, IoT applications need to process huge amounts of multidimensional signals and heterogeneous kinds of data collected from a wide variety of sensors also managing noisy and missing data. Therefore, AI methods represent enabling technologies to fuse the collected data and infer information from them. AI methods are used for a wide set of applications, as destination prediction, demand prediction, traffic flow prediction, travel time estimation, predicting traffic accident severity, predicting the mode of transportation, trajectory clustering, navigation, traffic signal control, and pollution monitoring [105]. Furthermore, transportation infrastructures can be monitored and controlled using the IoT paradigm and AI techniques, like artificial neural networks, for monitoring and analyzing the conditions of motor highways, airports and railways [106]. In this scenario, deep learning approaches are showing particularly promising results.

In Industry 4.0 and Industrial IoT applications, AI methods are applied to optimize image and sensor processing, transmission and decisions. These applications typically require high-speed data streams, low-latency communications, fast processing and time-sensitive actions on small-scale platforms, often directly on the IoT devices. In some applications, large and general-purpose deep neural networks are not applicable, and AI techniques based on the concept of knowledge transfer and fine-tuning methods are used to improve the accuracy of specific neural networks. Possible applications can range from image classification to ultra-reliable low-latency communication, for instance by exploiting reinforcement learning models capable of working in the compact memory space typical of IoT devices [99]. A different processing approach in industrial IoT applications considers the fog/edge computing paradigm by adopting edge computing-based deep learning models, hence avoiding slow and unreliable transmission from the cloud service, thus mitigating problems related to the possible congestion in the industrial IoT network and avoiding the limits of insufficient local computational power [107].

The fast execution time of deep neural networks, like convolutional neural networks, enables their use for quality assessment of the products, online monitoring and control of the manufacturing production [108], as well as their use on indoor autonomous robots in productions sites and warehouses [109]. AI techniques like artificial neural networks and deep neural networks are also relevant tools in logistics for managing, optimizing and monitoring the goods in the complete supply chain [110]. In this scenario, neural networks, deep learning, fuzzy logic, and evolutionary algorithms are the mostly used AI techniques.

In healthcare applications, the pervasive diffusion of technologies like fitness trackers, wearable devices, and body sensor networks made available a huge amount of information that can be processed in real time. Starting from that data, AI techniques are used to learn and produce effective reasoning, thus enabling systems to monitor in real time the health conditions of the user For instance, methods based on deep neural networks can be used to predict diseases from signals collected using IoT sensors [111]. In environmental monitoring, AI techniques are particularly important for processing heterogeneous noisy signals collected in uncontrolled environments. As an instance, artificial neural networks are used to process data collected by IoT sensors for monitoring the quality of the air quality, water pollution, and radiation pollution [112]. Neural networks and deep learning are the mostly used AI techniques in this scenario.

In agriculture applications, AI methods are applied in IoT devices to control harvests, green house parameters, parasite forecast, smart irrigation, and to create IoT devices capable of prompt reactions to changes in plants and environmental conditions. For example, convolutional neural networks can be adopted to forecast and detect possible rice blast diseases in large scale applications by using data acquired with IoT sensors, which describe the soil humidity and weather conditions [113]. Support vector machines and convolutional neural networks can also be used to detect the grow stages of vegetables in greenhouse monitoring applications [114]. AI approaches able to learn from data, as artificial neural networks are frequently adopted in this application context.

In smart grids, AI techniques allow to improve the energy efficiency and management of power systems by performing analyses and forecasts from large-scale data collected from heterogeneous distributed devices [115], [116]. Examples of applications for which researchers studied methods based on AI techniques are the prediction of energy production, integration of renewable energy sources, integration of energy storage systems, analysis of the demand and response of energy management systems and management of local and private small grids. Artificial neural networks and fuzzy logic are widely used in this scenario.

VII. Open Issues and Innovative Key Solutions

As described in sections II, III, IV, V, and VI, a progression of experiences can be determined concerning AI-based sensor systems' innovation restrictions and their ease of use in a wide range of application domains. AIoT is being embraced in many fields and business areas thereby providing unprecedented opportunities for improvements and novel capabilities.

However, as with other emerging technologies there are challenges that must be addressed with AIoT innovations. Next, we discuss some of these challenges below.

AIoT adoption and interoperability: The number of AI-based sensor applications is growing at a fast pace, creating a large number of heterogeneous solutions. The wide diversity of implementations and features open up interoperability issues, hindering standardization. As discussed in section III, most APIs provided by Edge/Fog computations are far from being considered easy to use. Therefore, several authors have proposed their solutions towards interoperable architectures as described in the IoT architecture section.

Latency and scalability: Most IoT applications require low latency (delay) rates. The data storage optimization (as discussed in section III) and the architectural aspects provide IoT networks distributed intelligence. But to enable distributed and federated intelligence, complex challenges in the setup and configuration for smart sensing systems in the AIoT framework must be addressed.

Quantum resilience: One challenge is how to monitor and ensure quality services from all the connected devices. Responsiveness, scalability, processes, and efficiency are needed to provide the best service when it comes to any new technology especially across trillions of sensors [140], [141]. Quantum technology with AI-based sensor systems can be helpful in addressing network latency, interoperability, AI, real-time analytics, predictive analytics, increased storage and data memory, secure cloud computing and the emerging 5G telecommunications infrastructure.

VIII. Conclusion

IoT theme of applications are helping in collecting voluminous of sensor fusion data from multiple sources. Though, the multitude of data generated from limitless IoT devices makes complicated process for collection, processing and analysing data in real-time, convergence of AI and IoT as AIoT can rethink the way data can be handled for enterprises, business, and economies to act smartly. Man-made intelligence empowered IoT devices makes machines produce smart behaviour devices.

Consolidating these two (AI and IoT) streams to manage smart sensing systems, benefits the basic individual day to day needs. While IoT manages gadgets collaborating utilizing the web, AI causes the gadgets to gain from their information and experience. While, IoT gives information, man-made reasoning procures the ability to open reactions, offering both imagination and setting to drive smart activities. As the information conveyed from the sensor can be broke down with AI, organizations can settle on smartchoices. The man-made brainpower IoT prevails with regards to accomplishing the smart sensing systems.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions which helped them improve the organization, quality, and presentation of this work.

References

[1] J. U. Knickerbocker *et al.*, "Heterogeneous integration technology demonstrations for future healthcare, IoT, and AI computing solutions," in *Proc. IEEE 68th Electron. Compon. Technol. Conf. (ECTC)*, Jun. 2018, pp. 1519–1528, doi: 10.1109/ECTC.2018.00231.

[2] K. Mbuthia, J. Dai, S. Zavrakas, and J. Yan, "Patient-centric healthcare data processing using streams and asynchronous technology," *Int. J. Smart Sens. Intell. Syst.*, vol. 11, no. 1, pp. 1–18, 2018, doi: 10.21307/ijssis-2018-003.

[3] L. Russel, R. Goubran, and F. Kwamena, "Towards reliable IoT: Fog-based AI sensor validation," in *Proc. IEEE Cloud Summit*, Washington, DC, USA, Aug. 2019, pp. 37–44, doi: 10.1109/CloudSummit47114.2019.00013.

[4] K. Michail, K. M. Deliparaschos, S. G. Tzafestas, and A. C. Zolotas, "AI-based actuator/sensor fault detection with low computational cost for industrial applications," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 1, pp. 293–301, Jan. 2016.

[5] M. Shahjalal, M. K. Hasan, M. M. Islam, M. M. Alam, M. F. Ahmed, and Y. M. Jang, "An overview of AI-enabled remote smart-home monitoring system using LoRa," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Fukuoka, Japan, Feb. 2020, pp. 510–513, doi: 10.1109/ICAIIC48513.2020.9065199.

[6] M. AlOtaibi, L. A. Tawalbeh, and Y. Jararweh, "Integrated sensors system based on IoT and mobile cloud computing," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov./Dec. 2016, pp. 1–5, doi: 10.1109/AICCSA.2016.7945812.

[7] J. Gomez-Rojas, L. Camargo, and R. Montero, "Mobile wireless sensor networks in a smart city," *Int. J. Smart Sens. Intell. Syst.*, vol. 11, no. 1, pp. 1–8, 2018, doi: 10.21307/ijssis-2018-009.

[8] Q. A. Al-Haija, I. Marouf, M. M. Asad, and K. A. Nasr, "Implementing a lightweight Schmidt-Samoa cryptosystem (SSC) for sensory communications," *Int. J. Smart Sens. Intell. Syst.*, vol. 12, no. 1, pp. 1–9, 2019, doi: 10.21307/ijssis-2019-006.

[9] G. Kim and I. Y. Jung, "Integrity assurance of OTA software update in smart vehicles," *Int. J. Smart Sens. Intell. Syst.*, vol. 12, no. 1, pp. 1–8, 2019, doi: 10.21307/ijssis-2019-011.

[10] P. Dasari, G. K. J. Reddy, and A. Gudipalli, "Forest fire detection using wireless sensor networks," *Int. J. Smart Sens. Intell. Syst.*, vol. 13, no. 1, pp. 1–8, 2020, doi: 10.21307/ijssis-2020-006.

[11] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the implementation of IoT for environmental condition monitoring in homes," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3846–3853, Oct. 2013.

[12] N. K. Suryadevara, S. C. Mukhopadhyay, R. Wang, R. K. Rayudu, and Y. M. Huang, "Reliable measurement of wireless sensor network data for forecasting wellness of elderly at smart home," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. (IMTC)*, Minneapolis, MN, USA, May 2013, pp. 16–21.

[13] S. Madria, V. Kumar, and R. Dalvi, "Sensor cloud: A cloud of virtual sensors," *IEEE Softw.*, vol. 31, no. 2, pp. 70–77, Mar./Apr. 2014.

[14] N. K. Suryadevara, S. C. Mukhopadhyay, S. D. T. Kelly, and S. P. S. Gill, "WSN-based smart sensors and actuator for power management in intelligent buildings," *IEEE/ASME Trans. Mechatronics*, vol. 20, no. 2, pp. 564–571, Apr. 2015.

[15] J. Duan, D. Gao, D. Yang, C. H. Foh, and H.-H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 58–69, Feb. 2014.

[16] N. K. Suryadevara and S. C. Mukhopadhyay, "Determining wellness through an ambient assisted living environment," *IEEE Intell. Syst.*, vol. 29, no. 3, pp. 30–37, May 2014.

[17] V. Goverdovsky, D. Looney, P. Kidmose, C. Papavassiliou, and D. P. Mandic, "Co-located multimodal sensing: A next generation solution for wearable health," *IEEE Sensors J.*, vol. 15, no. 1, pp. 138–145, Jan. 2015.

[18] Y. Wang, C. Li, Y. Duan, J. Yang, and X. Cheng, "An energy-efficient and swarm intelligence-based routing protocol for next-generation sensor networks," *IEEE Intell. Syst.*, vol. 29, no. 5, pp. 74–77, Sep/Oct. 2014.

[19] H. Ghayvat, J. Liu, S. C. Mukhopadhyay, and X. Gui, "Wellness sensor networks: A proposal and implementation for smart home for assisted living," *IEEE Sensors J.*, vol. 15, no. 12, pp. 7341–7348, Dec. 2015.

[20] W. Wu, H. Zhang, S. Pirbhulal, S. C. Mukhopadhyay, and Y.-T. Zhang, "Assessment of biofeedback training for emotion management through wearable textile physiological monitoring system," *IEEE Sensors J.*, vol. 15, no. 12, pp. 7087–7095, Dec. 2015.

[21] H. Ghayvat, S. C. Mukhopadhyay, and X. Gui, "Issues and mitigation of interference, attenuation and direction of arrival in IEEE 802.15.4/ZigBee to wireless sensors and networks based smart building," *Measurement*, vol. 86, pp. 209–226, May 2016, doi: 10.1016/j.measurement.2016.01.045.

[22] S. Thavalengal, T. Nedelcu, P. Bigioi, and P. Corcoran, "Iris liveness detection for next generation smartphones," *IEEE Trans. Consum. Electron.*, vol. 62, no. 2, pp. 95–102, May 2016.

[23] R. Thakur, "Scanning LIDAR in advanced driver assistance systems and beyond: Building a road map for next-generation LIDAR technology," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 48–54, Jul. 2016.

[24] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," in *Proc. Int. Conf. Innov. Challenges Cyber Secur. (ICICCS-INBUSH)*. Noida, India: Amity Univ., Feb. 2016, pp. 315–318.

[25] S. Borkar and H. Pande, "Application of 5G next generation network to Internet of Things," in *Proc. Int. Conf. Internet Things Appl. (IOTA)*, Pune, India, Jan. 2016, pp. 443–447.

[26] T. Islam, S. C. Mukhopadhyay, and N. K. Suryadevara, "Smart sensors and Internet of Things: A postgraduate paper," *IEEE Sensors J.*, vol. 17, no. 3, pp. 577–584, Feb. 2017.

[27] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn, "Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 54–61, Jan. 2017.

[28] R. Morello, S. C. Mukhopadhyay, Z. Liu, D. Slomovitz, and S. R. Samantaray, "Advances on sensing technologies for smart cities and power grids: A review," *IEEE Sensors J.*, vol. 17, no. 23, pp. 7596–7610, Dec. 2017.

[29] C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, "Big-sensing-data curation for the cloud is coming: A promise of scalable cloud-data-center mitigation for next-generation IoT and wireless sensor networks," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 48–56, Oct. 2017.

[30] R. Morello, C. De Capua, G. Fulco, and S. C. Mukhopadhyay, "A smart power meter to monitor energy flow in smart grids: The role of advanced sensing and IoT in the electric grid of the future," *IEEE Sensors J.*, vol. 17, no. 23, pp. 7828–7837, Dec. 2017.

[31] J. Cabra, D. Castro, J. Colorado, D. Mendez, and L. Trujillo, "An IoT approach for wireless sensor networks applied to E-health environmental monitoring," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Exeter, U.K., Jun. 2017, pp. 578–583.

[32] R. Ferrero, E. Beattie, and J. Phoenix, "Sensor city—A global innovation hub for sensor technology," *IEEE Instrum. Meas. Mag.*, vol. 21, no. 1, pp. 4–16, Feb. 2018.

[33] M. E. E. Alahi, N. Pereira-Ishak, S. C. Mukhopadhyay, and L. Burkitt, "An Internet-of-Things enabled smart sensing system for nitrate monitoring," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4409–4417, Dec. 2018.

[34] N. Afsarimanesh, M. E. E. Alahi, S. C. Mukhopadhyay, and M. Kruger, "Development of IoT-based impedometric biosensor for point-of-care monitoring of bone loss," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 8, no. 2, pp. 211–220, Jun. 2018.

[35] A. Kumar, A. Singh, A. Kumar, M. K. Singh, P. Mahanta, and S. C. Mukhopadhyay, "Sensing technologies for monitoring intelligent buildings: A review," *IEEE Sensors J.*, vol. 18, no. 12, pp. 4847–4860, Jun. 2018.

[36] F. Wu, C. Rudiger, J.-M. Redoute, and M. R. Yuce, "WE-Safe: A wearable IoT sensor node for safety applications via LoRa," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018, pp. 144–148.

[37] K. Shafique *et al.*, "Energy harvesting using a low-cost rectenna for Internet of Things (IoT) applications," *IEEE Access*, vol. 6, pp. 30932–30941, 2018.

[38] A. Aijaz and P. Kulkarni, "On performance evaluation of dynamic sensitivity control techniques in next-generation WLANs," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1324–1327, Jun. 2019.

[39] M. S. Murty and R. Shrestha, "Hardware implementation and VLSI design of spectrum sensor for next-generation LTE-A cognitive-radio wireless network," *IET Circuits, Devices Syst.*, vol. 12, no. 5, pp. 542–550, Sep. 2018.

[40] T. A. Al-Janabi and H. S. Al-Raweshidy, "A centralized routing protocol with a scheduled mobile sink-based AI for large scale I-IoT," *IEEE Sensors J.*, vol. 18, no. 24, pp. 10248–10261, Dec. 2018.

[41] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 114–120, Oct. 2018.

[42] S. Pirbhulal, W. Wu, S. C. Mukhopadhyay, and G. Li, "A medical-IoT based framework for eHealth care," in *Proc. Int. Symp. Sens. Instrum. IoT Era (ISSI)*, Shanghai, China, Sep. 2018, pp. 6–7.

[43] S. M. A. Oteafy and H. S. Hassanein, "Leveraging tactile Internet cognizance and operation via IoT and edge technologies," *Proc. IEEE*, vol. 107, no. 2, pp. 364–375, Feb. 2019.

[44] S. Pirbhulal, W. Wu, S. C. Mukhopadhyay, and G. Li, "Adaptive energy optimization algorithm for Internet of medical things," in *Proc. 12th Int. Conf. Sens. Technol. (ICST)*, Limerick, Ireland, Dec. 2018, pp. 269–272.

[45] S. Zeadally, F. K. Shaikh, A. Talpur, and Q. Z. Sheng, "Design architectures for energy harvesting in the Internet of Things," *Renew. Sustain. Energy Rev.*, vol. 128, Aug. 2020, Art. no. 109901.

[46] T. Sutjarittham, H. H. Gharakheili, S. S. Kanhere, and V. Sivaraman, "Experiences with IoT and AI in a smart campus for optimizing classroom usage," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7595–7607, Oct. 2019.

[47] I. Ahmad and K. Chang, "Effective SNR mapping and link adaptation strategy for next-generation underwater acoustic communications networks: A cross-layer approach," *IEEE Access*, vol. 7, pp. 44150–44164, 2019.

[48] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: A review," *IEEE Sensors J.*, vol. 19, no. 15, pp. 5952–5967, Aug. 2019.

[49] A. Rauniyar, P. E. Engelstad, and O. N. Osterbo, "Performance analysis of RF energy harvesting and information transmission based on NOMA with interfering signal for IoT relay systems," *IEEE Sensors J.*, vol. 19, no. 17, pp. 7668–7682, Sep. 2019.

[50] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G," *Proc. IEEE*, vol. 107, no. 6, pp. 944–961, Jun. 2019.

[51] B. S. Awoyemi, A. S. Alfa, and B. T. Maharaj, "Network restoration in wireless sensor networks for next-generation applications," *IEEE Sensors J.*, vol. 19, no. 18, pp. 8352–8363, Sep. 2019.

[52] A. Verma, S. Prakash, V. Srivastava, A. Kumar, and S. C. Mukhopadhyay, "Sensing, controlling, and IoT infrastructure in smart building: A review," *IEEE Sensors J.*, vol. 19, no. 20, pp. 9036–9046, Oct. 2019.

[53] A. Zappone, M. Di Renzo, and M. Debbah, "Wireless networks design in the era of deep learning: Model-based, AI-based, or both?" *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7331–7376, Oct. 2019.

[54] J. Wan, P. Zheng, H. Si, N. N. Xiong, W. Zhang, and A. V. Vasilakos, "An artificial intelligence driven multi-feature extraction scheme for big data detection," *IEEE Access*, vol. 7, pp. 80122–80132, 2019.

[55] S. Savazzi, S. Sigg, F. Vicentini, S. Kianoush, and R. Findling, "On the use of stray wireless signals for sensing: A look beyond 5G for the next generation of industry," *Computer*, vol. 52, no. 7, pp. 25–36, Jul. 2019.

[56] F. Wu, T. Wu, and M. R. Yuce, "Design and implementation of a wearable sensor network system for IoT-connected safety and health applications," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 87–90.

[57] H. Nguyen *et al.*, "The next generation architecture of low power wide area network for energy platform," in *Proc. 11th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Zagreb, Croatia, Jul. 2019, pp. 2–5.

[58] Q.-Y. Yu, H.-C. Lin, and H.-H. Chen, "Intelligent radio for next generation wireless communications: An overview," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 94–101, Aug. 2019.

[59] I. Garcia-Magarino, R. Muttukrishnan, and J. Lloret, "Human-centric AI for trustworthy IoT systems with explainable multilayer perceptrons," *IEEE Access*, vol. 7, pp. 125562–125574, 2019.

[60] M. A. Azad, S. Bag, C. Perera, M. Barhamgi, and F. Hao, "Authentic caller: Self-enforcing authentication in a next-generation network," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3606–3615, May 2020.

[61] D. Sehrawat and N. S. Gill, "Smart sensors: Analysis of different types of IoT sensors," in *Proc. 3rd Int. Conf. Trends Electron. Inform. (ICOEI)*, Apr. 2019, pp. 523–528.

[62] A. M. Alberti *et al.*, "Platforms for smart environments and future Internet design: A survey," *IEEE Access*, vol. 7, pp. 165748–165778, 2019.

[63] Y.-W. Lin, Y.-B. Lin, C.-Y. Liu, J.-Y. Lin, and Y.-L. Shih, "Implementing AI as cyber IoT devices: The house valuation example," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2612–2620, Apr. 2020.

[64] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.

[65] P. Lakkamraju, M. Anumukonda, and S. R. Chowdhury, "Improvements in accurate detection of cardiac abnormalities and prognostic health diagnosis using artificial intelligence in medical systems," *IEEE Access*, vol. 8, pp. 32776–32782, 2020.

[66] M. Youssef, M. Hassan, and G. Kortuem, "Next generation IoT: Toward ubiquitous autonomous cost-efficient IoT devices," *IEEE Pervas. Comput.*, vol. 18, no. 4, pp. 8–11, Oct. 2019.

[67] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020.

[68] K.-L. Tsai, F.-Y. Leu, L.-L. Hung, and C.-Y. Ko, "Secure session key generation method for LoRaWAN servers," *IEEE Access*, vol. 8, pp. 54631–54640, 2020.

[69] Q. Xu, B. Wang, F. Zhang, D. S. Regani, F. Wang, and K. J. R. Liu, "Wireless AI in smart car: How smart a car can be?" *IEEE Access*, vol. 8, pp. 55091–55112, 2020.

[70] F. Akhter, S. Khadivizand, J. Lodyga, H. R. Siddiquei, M. E. E. Alahi, and S. C. Mukhopadhyay, "Design and development of an IoT enabled pedestrian counting and environmental monitoring system for a smart city," in *Proc. 13th Int. Conf. Sens. Technol. (ICST)*, Sydney, NSW, Australia, Dec. 2019, pp. 1–6.

[71] X. Chen *et al.*, "Artificial intelligence-empowered path selection: A survey of ant colony optimization for static and mobile sensor networks," *IEEE Access*, vol. 8, pp. 71497–71511, 2020.

[72] S. Veeralingam, S. Khandelwal, and S. Badhulika, "AI/ML-enabled 2-D–RuS2 nanomaterial-based multifunctional, low cost, wearable sensor platform for non-invasive point of care diagnostics," *IEEE Sensors J.*, vol. 20, no. 15, pp. 8437–8444, Aug. 2020.

[73] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of deep learning to real-time Web intrusion detection," *IEEE Access*, vol. 8, pp. 70245–70261, 2020.

[74] K. Huang *et al.*, "Photovoltaic agricultural Internet of Things towards realizing the next generation of smart farming," *IEEE Access*, vol. 8, pp. 76300–76312, 2020.

[75] L. Kirschbaum, D. Roman, G. Singh, J. Bruns, V. Robu, and D. Flynn, "AI-driven maintenance support for downhole tools and electronics operated in dynamic drilling environments," *IEEE Access*, vol. 8, pp. 78683–78701, 2020.

[76] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020.

[77] S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "GDPR interference with next generation 5G and IoT networks," *IEEE Access*, vol. 8, pp. 108052–108061, 2020.

[78] I. Anagnostopoulos, S. Zeadally, and E. Exposito, "Handling big data: Research challenges and future directions," *J. Supercomput.*, vol. 72, no. 4, pp. 1494–1516, Apr. 2016.

[79] A. Sahani, R. Kumar, S. Chinara, A. Kumari, and B. Patro, "Data management for the Internet of Things," in *Internet of Things (IoT)*, M. Alam, K. Shakil, and S. Khan, Eds. Cham, Switzerland: Springer, 2020, doi: 10.1007/978-3-030-37468-6_5.

[80] D. Gil, A. Ferrández, H. Mora-Mora, and J. Peral, "Internet of Things: A review of surveys based on context aware intelligent services," *Sensors*, vol. 16, no. 7, p. 1069, Jul. 2016.

[81] *Google Cloud Solutions*. Accessed: Jul. 30, 2020. [Online]. Available: https://cloud.google.com/solutions/iot-overview

[82] D.-J. Shin, J.-H. Park, J.-H. Kim, K.-J. Kwak, J.-M. Park, and J.-J. Kim, "Big data-based sensor data processing and analysis for IoT environment," *J. Inst. Internet, Broadcast. Commun.*, vol. 19, no. 1, pp. 117–126, Feb. 2019.

[83] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015, doi: 10.1109/COMST.2015.2444095.

[84] M. Merenda, C. Porcaro, and D. Iero, "Edge machine learning for AI-enabled IoT devices: A review," *Sensors*, vol. 20, no. 9, p. 2533, Apr. 2020, doi: 10.3390/s20092533.

[85] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[86] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016, doi: 10.1109/jiot.2016.2584538.

[87] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of Internet of Things," *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 46–59, Jan. 2018, doi: 10.1109/TCC.2015.2485206.

[88] S. Sarkar, R. Wankar, S. N. Srirama, and N. K. Suryadevara, "Serverless management of sensing systems for fog computing framework," *IEEE Sensors J.*, vol. 20, no. 3, pp. 1564–1572, Feb. 2020, doi: 10.1109/JSEN.2019.2939182.

[89] *IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing*, IEEE Standard 1934-2018.

[90] A. P. Plageras and K. E. Psannis, "Algorithms for big data delivery over the Internet of Things," in *Proc. IEEE 19th Conf. Bus. Informat. (CBI)*, Thessaloniki, Greece, Jul. 2017, pp. 202–206, doi: 10.1109/CBI.2017.27.

[91] M. Aazam, S. Zeadally, and K. A. Harras, "Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities," *Future Gener. Comput. Syst.*, vol. 87, pp. 278–289, Oct. 2018.

[92] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, *Architectural Considerations in Smart Object Networking*, document RFC 7452, Mar. 2015.

[93] C. Sharma and N. K. Gondhi, "Communication protocol stack for constrained IoT systems," in *Proc. 3rd Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Feb. 2018, pp. 1–6.

[94] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[95] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for Internet of Things (IoT)," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3440–3450, Sep. 2020.

[96] F. Siddiqui, J. Beley, S. Zeadally, and G. Braught, "Secure and lightweight communication in heterogeneous IoT environments," *Internet Things, Eng. Cyber Phys. Hum. Syst.*, Sep. 2019, Art. no. 100093, doi: 10.1016/j.iot.2019.100093.

[97] F. Tao, Y. Cheng, L. Da Xu, L. Zhang, and B. H. Li, "CCIoT-CMfg: Cloud computing and Internet of Things-based cloud manufacturing service system," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1435–1442, May 2014, doi: 10.1109/TII.2014.2306383.

[98] J. Tang, D. Sun, S. Liu, and J.-L. Gaudiot, "Enabling deep learning on IoT devices," *Computer*, vol. 50, no. 10, pp. 92–96, 2017.

[99] Y. Ma, J. Jin, Q. Huang, and F. F. Dan, "Data preprocessing of agricultural IoT based on time series analysis," in *Intelligent Computing Theories and Application* (Lecture Notes in Computer Science), vol. 10954. Cham, Switzerland: Springer, 2018, doi: 10.1007/978-3-319-95930-6_21.

[100] R. Hou, Y. Kong, B. Cai, and H. Liu, "Unstructured big data analysis algorithm and simulation of Internet of Things based on machine learning," *Neural Comput. Appl.*, vol. 32, no. 10, pp. 5399–5407, May 2020.

[101] M. Mohammadi, A. Al-Fuqaha, M. Guizani, and J.-S. Oh, "Semi-supervised deep reinforcement learning in support of IoT and smart city services," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 624–635, Apr. 2018.

[102] H. Yang, A. Alphones, W.-D. Zhong, C. Chen, and X. Xie, "Learning-based energy-efficient resource management by heterogeneous RF/VLC for ultra-reliable low-latency industrial IoT networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5565–5576, Aug. 2020.

[103] S. Govindaraj and S. N. Deepa, "Network energy optimization of IOTs in wireless sensor networks using capsule neural network learning model," *Wireless Pers. Commun.*, vol. 115, no. 3, pp. 2415–2436, Dec. 2020.

[104] Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, "A survey of multi-objective optimization in wireless sensor networks: Metrics, algorithms, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 550–586, 1st Quart., 2017.

[105] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2716–2725, Apr. 2020.

[106] C. Kirwan and F. Zhiyong, *Smart Cities and Artificial Intelligence*. Amsterdam, The Netherlands: Elsevier, 2020.

[107] M. Veres and M. Moussa, "Deep learning for intelligent transportation systems: A survey of emerging trends," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 8, pp. 3152–3168, Aug. 2020.
[108] P. Fraga-Lamas, T. Fernández-Caramés, and L. Castedo, "Towards the Internet of smart trains: A review on industrial IoT-connected railways," *Sensors*, vol. 17, no. 6, p. 1457, Jun. 2017.
[109] M. Saravanan, P. S. Kumar, and A. Sharma, "IoT enabled indoor autonomous mobile robot using CNN and Q-learning," in *Proc. IEEE Int. Conf. Ind. 4.0, Artif. Intell., Commun. Technol. (IAICT)*, Jul. 2019, pp. 7–13.
[110] J. Villalba-Diez, D. Schmidt, R. Gevers, J. Ordieres-Meré, M. Buchwitz, and W. Wellbrock, "Deep learning for industrial computer vision quality control in the printing industry 4.0," *Sensors*, vol. 19, no. 18, p. 3987, Sep. 2019.
[111] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, "Toward edge-based deep learning in industrial Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4329–4341, May 2020.
[112] G. Kousiouris *et al.*, "A microservice-based framework for integrating IoT management platforms, semantic and AI services for supply chain management," *ICT Exp.*, vol. 5, no. 2, pp. 141–145, Jun. 2019.
[113] M. A. Khan, "An IoT framework for heart disease prediction based on MDCNN classifier," *IEEE Access*, vol. 8, pp. 34717–34727, 2020.
[114] S. L. Ullo and G. R. Sinha, "Advances in smart environment monitoring systems using IoT and sensors," *Sensors*, vol. 20, no. 11, p. 3113, May 2020.
[115] W.-L. Chen, Y.-B. Lin, F.-L. Ng, C.-Y. Liu, and Y.-W. Lin, "RiceTalk: Rice blast detection using Internet of Things and artificial intelligence technologies," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1001–1010, Feb. 2020.
[116] N. Kitpo, Y. Kugai, M. Inoue, T. Yokemura, and S. Satomura, "Internet of Things for greenhouse monitoring system using deep learning and bot notification services," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–4.
[117] S. S. Ali and B. J. Choi, "State-of-the-art artificial intelligence techniques for distributed smart grids: A review," *Electronics*, vol. 9, no. 6, p. 1030, Jun. 2020.
[118] Accessed: Oct. 18, 2020. [Online]. Available: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf
[119] [Online]. Available: https://www.ibm.com/cloud/architecture/architectures/iotArchitecture
[120] [Online]. Available: http://d885pvmm0z6oe.cloudfront.net/hubs/intel_80616/assets/downloads/general/Architecture_Specification_Of_An_IOT_Platform.pdf
[121] [Online]. Available: https://www.iajapan.org/iot/event/2015/pdf/05_kraemer.pdf
[122] Accessed: Oct. 18, 2020. [Online]. Available: https://iot5.net/iot-platforms/oracle-iot-architecture-platform/
[123] C. Fuhrhop, J. Lyle, and S. Faily, "The Webinos project," in *Proc. 21st Int. Conf. World Wide Web*, 2012, pp. 259–262.
[124] "Webinos project: Webinos project deliverable-phase II architecture and components," Tech. Rep., 2012.
[125] N. K. Suryadevara and G. R. Biswal, "Smart plugs: Paradigms and applications in the smart city-and-smart grid," *Energies*, vol. 12, no. 10, p. 1957, 2019.
[126] J. Guth *et al.*, "A detailed analysis of IoT platform architectures: Concepts, similarities, and differences," in *Internet of Everything*. Singapore: Springer, 2018, pp. 81–101.
[127] S. R. Sahith, S. R. Rudraraju, A. Negi, and N. K. Suryadevara, "Mesh WSN data aggregation and face identification in fog computing framework," in *Proc. 13th Int. Conf. Sens. Technol. (ICST)*, Sydney, NSW, Australia, Dec. 2019, pp. 1–6.
[128] N. K. Survadevara, S. C. Mukhopadhyay, and R. K. Rayudu, "Applying SARIMA time series to forecast sleeping activity for wellness model of elderly monitoring in smart home," in *Proc. 6th Int. Conf. Sens. Technol. (ICST)*, Kolkata, India, Dec. 2012, pp. 157–162.
[129] K.-H.-L. Loh, "1.2 fertilizing AIoT from roots to leaves," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2020, pp. 15–21.
[130] K.-C. Chang and M.-H. Chiang, "Design of data reduction approach for AIoT on embedded edge node," in *Proc. IEEE 8th Global Conf. Consum. Electron. (GCCE)*, Osaka, Japan, Oct. 2019, pp. 899–900, doi: 10.1109/GCCE46687.2019.9015421.
[131] M. Pieroni, L. Rizzello, N. Rosini, G. Fantoni, D. De Rossi, and D. Mazzei, "Affective Internet of Things: Mimicking human-like personality in designing smart-objects," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Milan, Italy, Dec. 2015, pp. 400–405, doi: 10.1109/WF-IoT.2015.7389088.
[132] D. Mazzei, G. Montelisciani, G. Baldi, and G. Fantoni, "Changing the programming paradigm for the embedded in the IoT domain," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 293–297.
[133] D. Mazzei, G. Fantoni, G. Montelisciani, and G. Baldi, "Internet of Things for designing smart objects," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 293–297.
[134] Y.-H. Lai, S.-Y. Chen, C.-F. Lai, Y.-C. Chang, and Y.-S. Su, "Study on enhancing AIoT computational thinking skills by plot image-based VR," *Interact. Learn. Environ.*, pp. 1–14, Feb. 2019, doi: 10.1080/10494820.2019.1580750.
[135] Y.-H. Lai, T.-C. Wu, C.-F. Lai, L. T. Yang, and X. Zhou, "Cognitive optimal-setting control of AIoT industrial applications with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 2116–2123, Mar. 2021, doi: 10.1109/TII.2020.2986501.
[136] C.-J. Chen, Y.-Y. Huang, Y.-S. Li, C.-Y. Chang, and Y.-M. Huang, "An AIoT based smart agricultural system for pests detection," *IEEE Access*, vol. 8, pp. 180750–180761, 2020.
[137] *AIoT: Thoughts on Artificial Intelligence and the Internet of Things*. Accessed: Oct. 20, 2020. [Online]. Available: https://iot.ieee.org/conferences-events/wf-iot-2014-videos/56-newsletter/july-2019.html
[138] G. Mylonas, D. Amaxilatis, I. Chatzigiannakis, A. Anagnostopoulos, and F. Paganelli, "Enabling sustainability and energy awareness in schools based on IoT and real-world data," *IEEE Pervas. Comput.*, vol. 17, no. 4, pp. 53–63, Oct. 2018.
[139] M. Alvarez-Campana, G. López, E. Vázquez, V. Villagrá, and J. Berrocal, "Smart CEI moncloa: An IoT-based platform for people flow and environmental monitoring on a Smart University Campus," *Sensors*, vol. 17, no. 12, p. 2856, Dec. 2017.
[140] M. Aazam, K. A. Harras, and S. Zeadally, "Fog computing for 5G tactile industrial Internet of Things: QoE-aware resource allocation model," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 3085–3092, May 2019.
[141] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, and E. Bartocci, "A roadmap toward the resilient Internet of Things for cyber-physical systems," *IEEE Access*, vol. 7, pp. 13260–13283, 2019, doi: 10.1109/ACCESS.2019.2891969.
[142] Accessed: Dec. 2, 2020. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2019/12/05/quantum-trends-and-the-internet-of-things/?sh=46ae846b3eb0;

Subhas Chandra Mukhopadhyay (Fellow, IEEE) is working as a Professor of Mechanical/Electronics Engineering at Macquarie University, Australia, and is the Discipline Leader of the Mechatronics Engineering Degree Programme. He is also the Director of International Engagement for the School of Engineering. His fields of interests include smart sensors and sensing technology, instrumentation techniques, wireless sensors and network, and the Internet of Things. He has supervised over 40 postgraduate students and over 100 Honours students. He has examined over 60 postgraduate theses. He has published over 400 papers in different international journals and conference proceedings, written nine books and 42 two book chapters, and edited 18 conference proceedings. He has also edited 35 books with Springer-Verlag and 30 journal special issues. He has organized over 20 international conferences as either General Chair/Co-Chair or Technical Programme Chair. He has delivered 365 presentations, including keynote, invited, tutorial, and special lectures. He is a Fellow of the IET (U.K.), a Fellow of the IETE (India), a Topical Editor of the IEEE SENSORS JOURNAL, an Associate Editor of the IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENTS, the IEEE SYSTEMS JOURNAL, and the IEEE REVIEW OF BIOMEDICAL ENGINEERING. He is a Distinguished Lecturer of the IEEE Sensors Council from 2017 to 2022. He is the Founding Chair of the IEEE Sensors Council NSW Chapter.

Sumarga Kumar Sah Tyagi (Member, IEEE) received the M.Sc. degree in computer science and the Ph.D. degree in wireless communication from the South Asian University (established by SAARC countries), New Delhi, India, and the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, respectively. He is working as an Assistant Professor at the Zhongyuan University of Technology, Zhengzhou, China. He has published two books and over 15 SCI publications. His research interests focus on cutting-edge AI enabled communications and computing technology. He was a recipient of several prestigious scholarships/awards from different governments, including "CAS-TWAS President's Fellowship-2014" for the duration of Ph.D. from the Government of China and Italy, and "SAARC Silver-Jubilee Scholarship" (2012–2014) from Indian Government for the duration of studying master's degree. Besides, he is also serving as the Lead Guest Editor for several peer-reviewed journals from the IEEE, ACM, Elsevier, and Springer.

Nagender Kumar Suryadevara (Senior Member, IEEE) received the Ph.D. degree from the School of Engineering and Advanced Technology, Massey University, New Zealand, in 2014. He is an Associate Professor at the School of Computer and Information Sciences, University of Hyderabad, India. He has authored/coauthored two books, edited two books, and has published over 50 papers in various international journals, conferences, and book chapters. He has supervised over 100 graduate and postgraduate students. He has examined over 30 postgraduate theses. He has delivered 36 presentations, including keynote, tutorial, and special lectures. His research interests include wireless sensor networks, the Internet of Things, and time-series data mining.

Vincenzo Piuri (Fellow, IEEE) received the Ph.D. degree in computer engineering from the Politecnico di Milano, Italy, in 1989.

He has been a Full Professor of Computer Engineering with the Universitàdegli Studi di Milano, Italy, since 2000. He has been an Associate Professor with the Politecnico di Milano, Italy, and a Visiting Professor at the University of Texas at Austin and at George Mason University, Fairfax, VA, USA. He is an Honorary Professor at Obuda University, Hungary; Guangdong University of Petrochemical Technology, China; Northeastern University, China; Muroran Institute of Technology, Japan; and the Amity University, India. His main research interests are artificial intelligence, computational intelligence, intelligent systems, machine learning, pattern analysis and recognition, signal and image processing, biometrics, intelligent measurement systems, industrial applications, digital processing architectures, fault tolerance, cloud computing infrastructures, and the Internet-of-Things. Original results have been published in over 400 papers in international journals, proceedings of international conferences, books, and book chapters.

Dr. Piuri is a Fellow of the Distinguished Scientist of ACM, and a Senior Member of the INNS. He received the IEEE Instrumentation and Measurement Society Technical Award (2002) and the IEEE TAB Hall of Honor (2019). He is the President of the IEEE Systems Council (2020–2021), and has been the IEEE Vice President for Technical Activities (2015), the IEEE Director, the President of the IEEE Computational Intelligence Society, the Vice President for Education of the IEEE Biometrics Council, the Vice President for Publications of the IEEE Instrumentation and Measurement Society and the IEEE Systems Council, and the Vice President for Membership of the IEEE Computational Intelligence Society. He has been the Editor-in-Chief of the IEEE Systems Journal (2013-2019). He is Associate Editor of the IEEE Transactions on Cloud Computing and has been an Associate Editor of the IEEE Transactions on Computers, the IEEE Transactions on Neural Networks, the IEEE Transactions on Instrumentation and Measurement, and the IEEE Access.

Fabio Scotti (Senior Member, IEEE) received the Ph.D. degree in computer engineering from the Politecnico di Milano, Italy, in 2003.

He has been an Associate Professor at the Department of Computer Science, Universitàdegli Studi di Milano, Italy, since 2015. He was the Director of the Biometric Systems Laboratory of the Department of Computer Science, Universitàdegli Studi di Milano. He has been the Deputy Director of the Industrial, Environmental and Biometric Informatics Laboratory, Department of Computer Science, Universitàdegli Studi di Milano, since 2015. His research interests include biometric systems, contactless biometrics, multimodal biometric systems, biometric encryption and privacy-compliant biometric templates, signal and image processing, high-level system design, computational intelligence algorithms and related technologies for industrial applications, theoretical, architectural, and application aspects of artificial neural networks. He has published over 130 papers in international journals, books, and conference proceedings. He is serving as an Associate Editor of the IEEE Open Journal of Signal Processing (since 2020) and as an Associate Editor of the IEEE Transactions on Human-machine Systems (since 2015). He is serving as a Book Editor (Area Editor, section Less-constrained Biometrics) of the *Encyclopedia of Cryptography, Security, and Privacy (3rd Edition)*, (Springer, since 2019). He has served as an Associate Editor of the *Springer Soft Computing* (2013-2020) and as an Associate Editor of the IEEE Transactions on Information Forensics and Security (2010–2013).

Sherali Zeadally (Senior Member, IEEE) earned the bachelor's degree in computer science from the University of Cambridge, U.K. He also received a doctoral degree in computer science from the University of Buckingham, U.K., followed by post-doctoral research at the University of Southern California, Los Angeles, CA. He is currently an Associate Professor in the College of Communication and Information, University of Kentucky. His research interests include cybersecurity, privacy, the Internet of Things, computer networks, and energy-efficient networking. He has received numerous awards and honors for his research and teaching. He is a Fellow of the British Computer Society and the Institution of Engineering Technology, U.K.